

# Application, Network and Storage Controls

K-12 hardening playbook · ThreatLocker and AppLocker

Jim Tyler, K-12 Director of Technology · MAEDS 2026

© 2026 Jim Tyler. All rights reserved. The latest version of this guide is at [jimtyler.org/guides](https://jimtyler.org/guides).

A plain-language playbook for the controls that decide what runs, what it can touch, and where it can talk: application control, ringfencing, network control and storage control, for every tier of a K-12 Windows environment. It is one ordered list that covers domain controllers, member servers, workstations and operational technology, with the egress and command-and-control side included.

Each control shows how to implement it in **ThreatLocker (TL)**, the nearest **AppLocker (AL)** or free Microsoft equivalent (**WDAC**, **ASR**, **FW** = Windows Firewall GPO, **GPO**), and how to verify it. Where AppLocker has no equivalent, the row says so: AppLocker blocks launches; it cannot ringfence, control network per process, or restrict storage.

---

## CONTENTS

- |                                                                         |                                                    |
|-------------------------------------------------------------------------|----------------------------------------------------|
| 1. Jim's 10 Quick Hits                                                  | 10. C5 · Workstation-specific                      |
| 2. How to read this guide                                               | 11. C6 · Servers by role                           |
| 3. Phased rollout                                                       | 12. C7 · Network Control and Windows Firewall GPO  |
| 4. Mechanics: ThreatLocker behavior that decides whether a policy works | 13. C8 · Egress and command-and-control            |
| 5. Mechanics: AppLocker behavior and limits                             | 14. C9 · Identity and protocol                     |
| 6. C1 · Tier-0 LOLBin denies                                            | 15. C11 · ThreatLocker portal and agent protection |
| 7. C2 · LOLBAS additions                                                | 16. C12 · Verification and troubleshooting         |
| 8. C3 · Ringfences                                                      | 17. C13 · Detect: alert rules                      |
| 9. C4 · Fixes to an inherited policy set                                | 18. C14 · Deception                                |

# Jim's 10 Quick Hits

The first ten, in order. Every deny goes through Monitor first; every GPO goes through its audit event first. Then the rest of the phased rollout in order.

## 1. Confirm every group's Default policy is Deny and the group is Secured

|         |                                                                                                                                                                                                                     |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DO THIS | Open each computer group (DCs, Tier 0 Hypervisors, Tier 1 Infrastructure, OT, Workstations, PAWs). Confirm the Default policy is <b>Deny</b> , not Monitor, and the group mode is <b>Secured</b> . Screenshot each. |
| WHY     | An empty "Last Match" on an existing deny can mean the group was still in Learning or Monitor. Nothing else in this guide matters until this is true.                                                               |
| WHERE   | ThreatLocker portal > Computer Groups > each group > Default policy and mode                                                                                                                                        |
| EFFORT  | 30 minutes                                                                                                                                                                                                          |

## 2. Add the tier-0 deny block to the top of the DC policy list, Monitor Only

|         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DO THIS | Create the C1 denies ( <code>ntdsutil</code> , <code>dsdbutil</code> , <code>esentutl</code> , <code>vssadmin</code> / <code>diskshadow</code> / <code>wbadmin</code> , <code>ldifde</code> / <code>csvde</code> / <code>dsquery</code> , <code>wmic</code> , <code>dnscmd</code> , WinRM hosts, <code>mshta</code> / <code>certutil</code> / <code>bcdedit</code> , download proxies, .NET compilers, <code>mmc</code> ) as <b>Add to top</b> , policy status <b>Monitor Only</b> . The low-risk set ( <code>msdt</code> , <code>powershell_ise</code> / <code>pwsh</code> , <code>taskmgr</code> , <code>cmstp</code> , <code>at</code> , <code>finger</code> , <code>tftp</code> ) can go straight to Secured; see Phase 2. |
| WHY     | Windows Core Files sits at order 999,995 and permits every signed Microsoft binary. A deny below it never matches. Monitor first so the backup agent and RMM reveal themselves before anything is enforced.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| WHERE   | Policies > DC group > New policy > Add to top                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| EFFORT  | Half a day; two to four weeks of monitoring                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## 3. Fix any "Ringfenced" policy with empty ringfence tabs; remove browsers and Office from DCs and servers

|         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DO THIS | A policy whose name says Ringfenced but whose Applications, Internet, Files and Registry tabs are empty is a plain permit; WMI, Office, Office Installer and RunDLL are the usual ones. Configure the tabs (C3) or remove the application from the DC and server groups. Uninstall browsers, Office, OneDrive, Google Updater, Windows Phone and Communication App from DCs and servers; delete their policies; any Office or browser match on a DC in Unified Audit is an incident to explain, not noise. |
| WHY     | A policy named "Ringfenced" with nothing in the ringfence tabs is a plain permit. Nothing on a DC needs a browser.                                                                                                                                                                                                                                                                                                                                                                                         |
| WHERE   | Policies > filter by name; Applications on each DC                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| EFFORT  | Half a day                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

## 4. Deny `wsmprovhost` , `winrshost` and `winrs` everywhere; disable WinRM by GPO where unused

|         |                                                                                                                                                                                                                                                                           |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DO THIS | Deny the WinRM host and client binaries on DCs, Tier 1, OT and workstations. Ringfenced permit on Hyper-V hosts only if Windows Admin Center or PowerShell remoting is used there. GPO: WinRM service Disabled on workstations and on any server nobody manages remotely. |
| WHY     | PowerShell remoting rides WinRM. An agent signed in as an admin can run commands on every server that answers.                                                                                                                                                            |
| WHERE   | Policies (deny, Secured after the monitor period); Computer Configuration > Policies > Windows Settings > Security Settings > System Services > Windows Remote Management                                                                                                 |
| EFFORT  | One day; the monitor period finds the one host that needs it                                                                                                                                                                                                              |

## 5. Network Control: workstation to DC on AD-client ports only; workstation to workstation deny; management from the jump host only

|         |                                                                                                                                                                                                                                                                                                                                                                              |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DO THIS | Workstation > DC: allow 53, 88, 123/udp (time), 389/636 plus 389/udp (CLDAP locator), 445, 464, 3268/3269, 135 + RPC dynamic; deny 5985/5986, 3389, 139. Workstation > workstation: deny inbound 445, 135, 3389, 5985, 5900. Jump host or PAW > DCs and servers: allow 3389, 5985/5986 (where kept), 135/445 from the jump host object only. Monitor two weeks, enforce one. |
| WHY     | A credential is only as dangerous as what it can reach. 445 to DCs stays open; SYSVOL and NETLOGON need it or Group Policy stops applying.                                                                                                                                                                                                                                   |
| WHERE   | ThreatLocker > Network Control policies per group; free: Windows Firewall GPO inbound rules on the DC and workstation OUs scoped to source subnets                                                                                                                                                                                                                           |
| EFFORT  | Two weeks monitor, one enforce                                                                                                                                                                                                                                                                                                                                               |

## 6. Server VLANs outbound default-deny with per-role allowlists; alert on LLM hostnames

|         |                                                                                                                                                                                                                                                   |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DO THIS | Server and management VLANs: outbound denied except WSUS/Windows Update, Defender, NTP, KMS, CA CRL, ThreatLocker, RMM, backup cloud and named vendor FQDNs. DNS query logging from server VLANs to the SIEM; alert on any LLM-provider hostname. |
| WHY     | A domain controller has no business reaching the internet. An agent on a compromised server phones home to a legitimate AI API that every filter allows.                                                                                          |
| WHERE   | Perimeter firewall per VLAN; ThreatLocker Network Control outbound; Windows Firewall outbound default block on the server OU                                                                                                                      |
| EFFORT  | Two weeks monitor, one enforce                                                                                                                                                                                                                    |

## 7. Explicit denies for every RMM you don't use, plus outbound denies to their relays

|         |                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DO THIS | Permit one RMM by certificate and path. Explicit deny for AnyDesk, ScreenConnect, Atera, Splashtop, TeamViewer, NetSupport, Level, RustDesk, Syncro, Action1, Supremo, LogMeIn, GoTo, Zoho, VNC, Ammyy and DWAgent. Deny <a href="#">quickassist.exe</a> and <a href="#">msra.exe</a> for non-IT. Outbound denies to the other vendors' relays and ports (5938, 6568/7070, 8040/8041, 5900-5910, 7000). |
| WHY     | A second RMM is the most common persistence tool in ransomware incidents, and it is signed, so default-deny alone is not enough once a permit for "Microsoft Corporation" or a broad certificate exists.                                                                                                                                                                                                |
| WHERE   | Policies > deny by publisher; Network Control outbound; free: AppLocker publisher deny per vendor plus Windows Firewall outbound block                                                                                                                                                                                                                                                                  |
| EFFORT  | Half a day                                                                                                                                                                                                                                                                                                                                                                                              |

## 8. DCSync rights audit and 4662 alert; [dnscmd](#) deny and DnsAdmins audit; Locksmith against the CA

|         |                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DO THIS | Only DCs, Administrators and one sync account hold Replicating Directory Changes All; delete stale MSOL_ ADsync and Exchange ACEs; alert on 4662 with GUID <a href="#">1131f6ad-9c07-11d1-f79f-00c04fc2dcd2</a> from a non-DC. Deny <a href="#">dnscmd.exe</a> (temporary permit on the DNS server); treat DnsAdmins as Domain Admins on any DNS server missing the October 2021 update, and audit membership everywhere. Run Locksmith monthly. |
| WHY     | Each is a one-step path from a foothold to every password in the domain.                                                                                                                                                                                                                                                                                                                                                                         |
| WHERE   | ADSI Edit > domain root > Security; ThreatLocker policies; <a href="#">Invoke-Locksmith -Mode 1</a>                                                                                                                                                                                                                                                                                                                                              |
| EFFORT  | Half a day                                                                                                                                                                                                                                                                                                                                                                                                                                       |

## 9. Hyper-V hosts into Tier 0: PAW-only access, vTPM on DC VMs, export and checkpoint alerting, Storage Control on VHDX paths

|         |                                                                                                                                                                                                                                                                                                                                                                                    |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DO THIS | Hyper-V Administrators = Domain Admins only; management from the PAW; BitLocker on CSVs; vTPM on DC, backup and sync VMs; Storage Control deny on <a href="#">*.vhdx</a> <a href="#">*.vhd</a> <a href="#">*.vmdk</a> outside the VM paths; alert on the Hyper-V-VMMS Admin log events for a DC export or checkpoint (confirm the IDs on a test export before you trust the rule). |
| WHY     | Whoever can export a DC's disk has every password without touching the DC.                                                                                                                                                                                                                                                                                                         |
| WHERE   | Hyper-V Manager; ThreatLocker Storage Control; a SIEM rule on the VMMS log                                                                                                                                                                                                                                                                                                         |
| EFFORT  | One day                                                                                                                                                                                                                                                                                                                                                                            |

## 10. Honeytokens and the five never-legitimate rules with active response

|         |                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DO THIS | A decoy SPN account, a <a href="#">creds.csv</a> with a SACL in the script share, a canary document and API key, a decoy computer object. Active response (disable account, isolate host, page) on: DCSync from a non-DC; Kerberoast of the decoy SPN; any match on a Secured tripwire deny on a DC; a computer moved out of Secured mode or a Tier 0 policy edited; a privileged-group add outside a change window. |
| WHY     | An agent enumerates everything at machine speed. Each decoy fires on exactly that, and an alert with no action at 2 AM is an audit log.                                                                                                                                                                                                                                                                              |
| WHERE   | ThreatLocker Detect; SIEM active response; canarytokens.org                                                                                                                                                                                                                                                                                                                                                          |
| EFFORT  | One afternoon                                                                                                                                                                                                                                                                                                                                                                                                        |

---

## How to read this guide

| TAG         | MEANING                                                                                                                                                                                                         |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>TL</b>   | ThreatLocker: application control, ringfencing, Network Control, Storage Control, Elevation Control, Detect.                                                                                                    |
| <b>AL</b>   | AppLocker: launch allow and deny rules by publisher, path or hash. Built into every supported Windows edition, Pro included since the October 2022 updates; enforcement needs the Application Identity service. |
| <b>WDAC</b> | Windows Defender Application Control / App Control for Business: kernel-enforced, stronger than AppLocker, harder to author.                                                                                    |
| <b>ASR</b>  | Defender Attack Surface Reduction rules: the behavioral half AppLocker lacks.                                                                                                                                   |
| <b>FW</b>   | Windows Firewall, pushed by GPO.                                                                                                                                                                                |
| <b>GPO</b>  | Group Policy, nothing else needed.                                                                                                                                                                              |

★ marks the items to fix first.

**Tiers used throughout.** Tier 0 = domain controllers, hypervisors, the backup server, sync servers, AD CS, PAWs. Tier 1 = member servers. Tier 2 = workstations. OT = HVAC, cameras, access control.

**The AppLocker ceiling.** AppLocker or WDAC (launch denies) + ASR (behaviors) + Windows Firewall GPO (ports) + Defender for Endpoint if licensed (command-line detections) covers about 70% of this playbook. The missing 30% is ringfencing and per-process network control. Where a row says "no AL equivalent," that is the 30%.

# Phased rollout

| PHASE                                  | SCOPE                                                                                                                                                                                                                                                                                                                                                                                                                              | DURATION                        | EXIT CRITERIA                                                                                              |
|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|------------------------------------------------------------------------------------------------------------|
| <b>0 — Audit</b>                       | Unified Audit (or AppLocker 8003 events) for 30–60 days: filter by the backup agent, RMM and vendor process paths, and by every binary in the controls catalog. Identify who holds DCSync rights, DnsAdmins, Hyper-V Administrators, Protected Users. Run Locksmith and PingCastle.                                                                                                                                                | 2 weeks of reading              | Written list of legitimate matches per binary                                                              |
| <b>1 — Groups and defaults</b>         | Build computer groups (Mechanics). Confirm Default = Deny and Secured per group. Remove browsers, Office, OneDrive and Google Updater from DC and server groups. Fix any "Ringfenced" policy with empty ringfence tabs. Move existing denies above any permit that could shadow them.                                                                                                                                              | 1 week                          | Every group's Default policy verified by screenshot                                                        |
| <b>2 — Low-risk denies, enforced</b>   | <code>msdt</code> , <code>powershell_ise</code> , <code>pwsh</code> , Task Manager, <code>cmstp</code> , <code>at</code> , <code>finger</code> , <code>tftp</code> , tunnelers, every RMM you don't use, interpreters on servers. Secured Mode.                                                                                                                                                                                    | Same week                       | No matches during Phase 0                                                                                  |
| <b>3 — Tripwires, Monitor Only</b>     | <code>ntdsutil</code> , <code>dsdbutil</code> , <code>esentutil</code> , <code>vssadmin</code> / <code>diskshadow</code> / <code>wbadmin</code> , <code>ldifde</code> / <code>csvde</code> / <code>dsquery</code> , <code>wmic</code> , <code>dnscmd</code> , <code>reg.exe</code> , <code>netsh</code> , LSASS dumpers, PowerShell bypasses, rundll32 DLL blocklist, <code>wmi</code> / <code>dllhost</code> no-child ringfences. | 2–4 weeks (4–6 on workstations) | Backup jobs succeed with guest processing; RMM and monitoring still work                                   |
| <b>4 — Tripwires, enforced</b>         | Flip Phase 3 to Secured (or Inherit for backup-adjacent). Carve permits by parent process or certificate for backup and RMM.                                                                                                                                                                                                                                                                                                       | 1 week                          | 24 h clean on DCs, then servers, then workstations                                                         |
| <b>5 — Network Control</b>             | Inbound per role from the jump host; workstation > DC on AD-client ports only; workstation > workstation deny; server VLAN outbound default-deny; DNS egress lockdown. Monitor first.                                                                                                                                                                                                                                              | 2 weeks monitor + 1 enforce     | WSUS, KMS, NTP, CRL and vendor FQDNs allowlisted; GPO still applies; the backup server still reaches hosts |
| <b>6 — Identity and protocol GPOs</b>  | One at a time, each with its audit event enabled first: NTLM audit (8004) > <code>LmCompatibilityLevel 5</code> ; LDAP 2889 audit > signing + channel binding required; SMB signing; Protected Users one admin per day; deny-logon GPOs on the correct OUs; krbtgt rotation; DSRM.                                                                                                                                                 | 1 control per week              | Zero audit hits for 2 weeks before each enforce                                                            |
| <b>7 — Detect, deception, response</b> | Alert rules, honeytokens, active response on the never-legitimate rules, IR runbook, restore rehearsal.                                                                                                                                                                                                                                                                                                                            | Ongoing                         | Each rule has an owner and a documented response                                                           |

# Mechanics: ThreatLocker behavior that decides whether a policy works

| MECHANIC                          | RULE                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Evaluation order                  | Lowest order number first; first match wins. Windows Core Files sits at 999,995 and permits every signed Microsoft binary. <b>A deny below it never matches.</b>                                                                                                                                                                                                                                                                                                                                                                                    |
| Add to top vs bottom              | Denies > <b>Add to top</b> . Ringfence permits > add to top. Temporary permits > top (above the matching deny), with an expiry.                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Policy status                     | <b>Inherit Status From Computer</b> = follows the computer's mode. <b>Secured Mode</b> = enforced regardless of computer mode. <b>Monitor Only Mode</b> = logs regardless.                                                                                                                                                                                                                                                                                                                                                                          |
| Which status for what             | Tripwire denies ( <code>ntdsutil</code> , WinRM hosts, <code>mshta</code> , <code>certutil</code> , <code>dnscmd</code> , LSASS dumpers) > Secured after the monitor period, so Learning mode on a box cannot reope them. Backup-adjacent denies ( <code>vssadmin</code> , <code>wbadmin</code> , <code>esentutl</code> , <code>reg.exe</code> ) > Inherit. Everything new > Monitor Only first.                                                                                                                                                    |
| Kill Running Processes            | On for deny policies. Off for ringfence permits.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Show Notification / Allow Request | Off on servers and DCs. On for workstations (the request workflow is the user experience).                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Selected Users & Groups           | One deny for everyone, a permit scoped to the IT group above it. Shrink the IT group's workstation footprint to a PAW over time.                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Custom applications               | Binaries not in the built-in catalog ( <code>wsmprovhost</code> , <code>ntdsutil</code> , <code>esentutl</code> , <code>diskshadow</code> , <code>ldifde</code> , <code>csvde</code> , <code>dsquery</code> , <code>cmstp</code> , <code>at</code> , <code>finger</code> , <code>tftp</code> , <code>dsdbutil</code> , <code>tttracer</code> ...) > Applications > New Application > <b>Path + Certificate</b> (Microsoft Windows publisher), both <code>System32</code> and <code>SysWow64</code> paths. Never hash-only; updates brea hash rules. |
| Ringfence tabs                    | <b>APPLICATIONS</b> (what it can launch or interact with; empty exception list = no child processes), <b>INTERNET</b> , <b>FILES</b> , <b>REGISTRY</b> . Each has its own Monitor Only togg!                                                                                                                                                                                                                                                                                                                                                        |
| Parent process restrictions       | Agent 10.6.2+. Use to permit a binary only under a backup agent or RMM parent instead of permitting it broadly.                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| DLL and script control            | Confirm DLL tracking is on for the DC and server groups; confirm script control is on so unknown <code>.ps1</code> , <code>.vbs</code> and <code>.bat</code> are denied even where the interpreter is permitted.                                                                                                                                                                                                                                                                                                                                    |
| Computer groups                   | DCs · Tier 0 Hypervisors · Tier 1 Infrastructure · OT · Workstations · PAWs. Policies are per group; confirm each group's Default policy is Deny and the group is Secured.                                                                                                                                                                                                                                                                                                                                                                          |
| Unified Audit                     | The ground truth. Filter by group, action, date, process path. Use it before every enforce decision and first in every incident.                                                                                                                                                                                                                                                                                                                                                                                                                    |

# Mechanics: AppLocker behavior and limits

| MECHANIC           | RULE                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Rule collections   | Executable, Windows Installer, Script, Packaged app, <b>DLL</b> (off by default; turning it on is noisy but required to stop sideloading).                                                                                                                                                                                                                                                                                                                                                                                               |
| Rule types         | Publisher (preferred; survives updates), Path (bypassable via user-writable paths), Hash (brittle).                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Enforcement        | Requires the <b>Application Identity</b> service running; an admin can stop it. Set the service to Automatic via GPO and alert on it stopping (Event 7036).                                                                                                                                                                                                                                                                                                                                                                              |
| Audit mode         | Enforcement = Audit only per collection. Event log <a href="#">AppLocker/EXE and DLL</a> : <b>8003</b> = would have blocked, <b>8004</b> = blocked; <a href="#">AppLocker/MSI and Script</a> : <b>8006</b> / <b>8007</b> ; <a href="#">AppLocker/Packaged app-Execution</a> : <b>8022</b> / <b>8025</b> .                                                                                                                                                                                                                                |
| Default rules      | Create default rules first (allow <a href="#">C:\Windows\*</a> and <a href="#">C:\Program Files\*</a> for Everyone, allow all for Administrators), then layer <b>deny</b> rules above. Deny always wins over allow in AppLocker.                                                                                                                                                                                                                                                                                                         |
| Known gaps         | Path rules allow user-writable folders under <a href="#">C:\Windows</a> ( <a href="#">Tasks</a> , <a href="#">Temp</a> , <a href="#">tracing</a> , <a href="#">System32\spool\drivers\color</a> , others): add explicit deny path rules. LOLBins that execute code without a new EXE ( <a href="#">msbuild</a> , <a href="#">installutil</a> , <a href="#">regasm</a> , <a href="#">mshta</a> , <a href="#">rundll32</a> , <a href="#">regsvr32</a> ) need their own deny rules. No ringfencing, no network control, no storage control. |
| WDAC instead       | For servers and DCs, <b>WDAC / App Control for Business</b> with the <b>Microsoft Recommended Block Rules</b> XML is stronger: kernel-enforced, covers most LOLBAS binaries and the vulnerable-driver blocklist. Harder to author; deploy via Intune or <a href="#">ConvertFrom-CIPolicy</a> + GPO; run in audit first.                                                                                                                                                                                                                  |
| ASR rules          | Defender Attack Surface Reduction gives the behavioral half AppLocker lacks: Office child processes, LSASS credential theft, PsExec/WMI process creation, script-launched downloaded content, USB unsigned executables. Enable in audit, then block.                                                                                                                                                                                                                                                                                     |
| Minimum free stack | AppLocker or WDAC (launch denies) + ASR (behaviors) + Windows Firewall GPO (ports) + Defender for Endpoint if licensed (command-line detections). Covers about 70% of this playbook; the missing 30% is ringfencing and per-process network control.                                                                                                                                                                                                                                                                                     |

**AppLocker quick deny set (PowerShell).** Build publisher deny rules for the tier-0

LOLBin set from reference files on a DC:

```
$bins = 'ntdsutil','esentutil','vssadmin','diskshadow','wbadmin','ldifde','csvde','dsquery',
        'wmic','dnscmd','mshta','certutil','bcdedit','msdt','bitsadmin','cmstp','wsmprovhost','winrshost','winrs'
$files = $bins | % { Get-ChildItem "C:\Windows\System32\$_exe","C:\Windows\SysWOW64\$_exe" -ErrorAction SilentlyContinue }
$info = $files | Get-AppLockerFileInformation
$pol = New-AppLockerPolicy -FileInformation $info -RuleType Publisher -User Everyone -RuleNamePrefix 'Deny-LOLBin'
# No -Optimize: every file shares one publisher and product, so -Optimize collapses them into a
# single BinaryName="" rule, which as a Deny would block every Windows binary.
# Edit the XML: set Action="Deny" (New-AppLockerPolicy creates Allow rules), confirm each rule keeps its
# BinaryName, and set BinaryVersionRange LowSection="" so older file versions are denied too. Then:
# Set-AppLockerPolicy -XmlPolicy .\deny-lolbins.xml -Merge -Ldap "LDAP://CN={GPO-GUID},CN=Policies,CN=System,DC=domain,DC=local"
```

# C1 · Tier-0 LOLBin denies

Apply to DCs, servers and workstations unless the row says otherwise.

| BINARY                                                                                                                                                                                                                                                                                                                                                               | WHAT IT DOES FOR AN ATTACKER                                                                                                                                                                                | THREATLOCKER                                                                                                | APPOCKER / FREE                                            |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|------------------------------------------------------------|
| <a href="#">ntdsutil.exe</a>                                                                                                                                                                                                                                                                                                                                         | Dumps NTDS.dit + SYSTEM via IFM                                                                                                                                                                             | Deny, Secured; pre-built temporary permit for recovery                                                      | AL publisher deny; WDAC block rule                         |
| <a href="#">dsdbutil.exe</a>                                                                                                                                                                                                                                                                                                                                         | AD LDS twin of ntdsutil                                                                                                                                                                                     | Deny, Secured                                                                                               | AL deny                                                    |
| <a href="#">esentutil.exe</a>                                                                                                                                                                                                                                                                                                                                        | Copies locked files (NTDS.dit, SAM)                                                                                                                                                                         | Deny, Monitor > Secured                                                                                     | AL deny                                                    |
| <a href="#">vssadmin.exe</a> <a href="#">diskshadow.exe</a> <a href="#">wbadmin.exe</a>                                                                                                                                                                                                                                                                              | Shadow-copy NTDS.dit; delete recovery points                                                                                                                                                                | Deny, Monitor > Inherit; permit the backup agent by parent or certificate                                   | AL deny for Everyone, allow for the backup service account |
| <a href="#">ldifde.exe</a> <a href="#">csvde.exe</a> <a href="#">dsquery.exe</a> <a href="#">dsget.exe</a><br><a href="#">dsacis.exe</a> <a href="#">adfind.exe</a>                                                                                                                                                                                                  | Bulk AD export and recon                                                                                                                                                                                    | Deny; temporary permit for schema work                                                                      | AL deny                                                    |
| <a href="#">wmic.exe</a>                                                                                                                                                                                                                                                                                                                                             | Remote process creation, AV enumeration, XSL bypass                                                                                                                                                         | Deny (Monitor first for old RMM)                                                                            | AL deny; ASR "Block process creations from PsExec and WMI" |
| <a href="#">dnscmd.exe</a>                                                                                                                                                                                                                                                                                                                                           | <a href="#">serverlevelplugindll</a> = SYSTEM code execution on DNS for any DnsAdmins member on servers missing the October 2021 fix (CVE-2021-40469); still the tool for remote zone and forwarder changes | Deny; temporary permit on the DNS server                                                                    | AL deny                                                    |
| <a href="#">wsmprovhost.exe</a> <a href="#">winrshost.exe</a> <a href="#">winrs.exe</a> <a href="#">winrm.cmd</a><br><a href="#">winrm.vbs</a>                                                                                                                                                                                                                       | WinRM / PSRemoting host and client                                                                                                                                                                          | Deny on DCs, Tier 1, OT, workstations; ringfenced permit on Hyper-V hosts only if WAC or PowerShell is used | AL deny; GPO disable the WinRM service                     |
| <a href="#">mshta.exe</a> <a href="#">certutil.exe</a> <a href="#">bcdedit.exe</a> <a href="#">signtool.exe</a>                                                                                                                                                                                                                                                      | HTA execution, download and decode, boot tamper                                                                                                                                                             | Deny; keep it in the top deny block, above every permit                                                     | AL deny; WDAC block rules                                  |
| <a href="#">msdt.exe</a>                                                                                                                                                                                                                                                                                                                                             | Follina                                                                                                                                                                                                     | Deny (change from ringfence)                                                                                | AL deny                                                    |
| <a href="#">powershell_ise.exe</a> <a href="#">pwsh.exe</a>                                                                                                                                                                                                                                                                                                          | Alternate PowerShell hosts                                                                                                                                                                                  | Deny                                                                                                        | AL deny                                                    |
| <a href="#">taskmgr.exe</a>                                                                                                                                                                                                                                                                                                                                          | One-click LSASS dump                                                                                                                                                                                        | Deny; permit the IT group on workstations                                                                   | AL deny for non-admins; ASR LSASS rule                     |
| <a href="#">bitsadmin.exe</a> <a href="#">cmstp.exe</a> <a href="#">ftp.exe</a> <a href="#">tftp.exe</a><br><a href="#">finger.exe</a> <a href="#">at.exe</a>                                                                                                                                                                                                        | Download and execution proxies                                                                                                                                                                              | Deny                                                                                                        | AL deny                                                    |
| <a href="#">msbuild.exe</a> <a href="#">installutil.exe</a> <a href="#">regasm.exe</a><br><a href="#">regsvcs.exe</a> <a href="#">csc.exe</a> <a href="#">vbc.exe</a> <a href="#">aspnet_compiler.exe</a><br><a href="#">ilasm.exe</a> <a href="#">jsc.exe</a> <a href="#">microsoft.workflow.compiler.exe</a><br><a href="#">wfc.exe</a> <a href="#">dotnet.exe</a> | .NET compile and execute allowlist bypass                                                                                                                                                                   | Deny ( <a href="#">dotnet.exe</a> deny on servers; workstations only if no app needs it)                    | AL deny; WDAC block rules                                  |
| <a href="#">mmc.exe</a>                                                                                                                                                                                                                                                                                                                                              | UAC bypass, snap-in access                                                                                                                                                                                  | Deny on DCs, OT, Hyper-V; ringfence on Tier 1; deny for users on workstations                               | AL deny for non-admins                                     |
| <a href="#">regsvr32.exe</a> ★                                                                                                                                                                                                                                                                                                                                       | Squiblydoo: <a href="#">/i:http://... scrobj.dll</a> runs a scriptlet; it works offline too, so blocking the DLL alone is not enough.                                                                       | Deny for users; permit by parent ( <a href="#">msiexec</a> , your installers)                               | AL deny; WDAC block rule                                   |
| <a href="#">wevtutil.exe</a> <a href="#">auditpol.exe</a> ★                                                                                                                                                                                                                                                                                                          | Log clearing and audit disable, the first step of the standard pre-encryption script                                                                                                                        | Deny, Secured on DCs; never legitimate from a non-admin host                                                | AL deny                                                    |
| <a href="#">manage-bde.exe</a> <a href="#">repair-bde.exe</a> ★                                                                                                                                                                                                                                                                                                      | BitLocker as ransomware, used repeatedly in 2024–25. The <a href="#">.wsf</a> is in the scripts row; the EXE needs its own deny                                                                             | Deny; permit the IT group where BitLocker is managed                                                        | AL deny                                                    |
| <a href="#">diskpart.exe</a> <a href="#">format.com</a> <a href="#">reagentc.exe</a> <a href="#">vshadow.exe</a>                                                                                                                                                                                                                                                     | Wipe, format, disable WinRE; <a href="#">vshadow</a> is a Microsoft-signed SDK shadow-copy tool that bypasses the <a href="#">vssadmin</a> deny                                                             | Deny                                                                                                        | AL deny                                                    |
| <a href="#">icacls.exe</a> <a href="#">takeown.exe</a> <a href="#">cacls.exe</a> <a href="#">attrib.exe</a><br><a href="#">taskkill.exe</a>                                                                                                                                                                                                                          | Permission and attribute tampering and process killing ahead of encryption                                                                                                                                  | Ringfence no-child; deny for users on workstations; Monitor first (login scripts)                           | AL deny for users                                          |

## C2 · LOLBAS additions

| GROUP                                        | BINARIES                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | THREATLOCKER                                                                                                                                                                                                      | APPLOCKER                                                                                                                                  |
|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| LSASS / NTDS dump                            | <a href="#">tttracer.exe</a> <a href="#">ttdinject.exe</a> <a href="#">rdrleakdiag.exe</a> <a href="#">createdump.exe</a><br><a href="#">sqldumper.exe</a> <a href="#">dump64.exe</a> <a href="#">adplus.exe</a> <a href="#">cdb.exe</a> <a href="#">ntsd.exe</a><br><a href="#">procdump.exe</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Deny, Secured                                                                                                                                                                                                     | AL deny; ASR LSASS                                                                                                                         |
| PowerShell bypasses                          | <a href="#">runscripthelper.exe</a> <a href="#">syncappvpublishingserver.exe</a><br><a href="#">syncappvpublishingserver.vbs</a> <a href="#">sqlps.exe</a> <a href="#">sqltoolsps.exe</a> <a href="#">wt.exe</a><br><a href="#">openconsole.exe</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Deny (permit <a href="#">wt.exe</a> for IT on workstations)                                                                                                                                                       | AL deny                                                                                                                                    |
| Forced auth / sniffing / screen capture      | <a href="#">rpcping.exe</a> <a href="#">pktmon.exe</a> <a href="#">nmcap.exe</a> <a href="#">psr.exe</a> (Steps Recorder: silent screenshots, not sniffing)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Deny                                                                                                                                                                                                              | AL deny                                                                                                                                    |
| Remote exec / transfer                       | <a href="#">ssh.exe</a> <a href="#">scp.exe</a> <a href="#">sftp.exe</a> <a href="#">bash.exe</a> <a href="#">wsl.exe</a> <a href="#">wbemtest.exe</a><br><a href="#">devtunnel.exe</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Deny (permit <a href="#">ssh</a> for IT)                                                                                                                                                                          | AL deny                                                                                                                                    |
| Execution proxies                            | <a href="#">atbroker</a> <a href="#">change</a> <a href="#">query</a> <a href="#">reset</a> <a href="#">customshellhost</a> <a href="#">runexehelper</a><br><a href="#">provlaunch</a> <a href="#">setres</a> <a href="#">stordiag</a> <a href="#">sigverif</a> <a href="#">unregmp2</a> <a href="#">wlrmdr</a><br><a href="#">workfolders</a> <a href="#">write</a> <a href="#">setupugc</a> <a href="#">ie4uinit</a> <a href="#">iediagcmd</a> <a href="#">ieexec</a><br><a href="#">infdefaultinstall</a> <a href="#">register-cimprovider</a> <a href="#">rasautou</a> <a href="#">extexport</a> <a href="#">wab</a><br><a href="#">verclsid</a> <a href="#">pcwrun</a> <a href="#">presentationhost</a> <a href="#">applaunch</a> <a href="#">dfsvc</a> <a href="#">addinutil</a><br><a href="#">appinstaller</a> <a href="#">cmdl32</a> <a href="#">replace</a> <a href="#">diantz</a> <a href="#">print</a> <a href="#">hh</a> <a href="#">forfiles</a><br><a href="#">pcaua</a> <a href="#">scriptrunner</a> <a href="#">odbconf</a> <a href="#">mavinject</a> <a href="#">msxsl</a> <a href="#">xwizard</a> <a href="#">certoc</a><br><a href="#">desktopimgdownldr</a> <a href="#">winget</a> | Deny ( <a href="#">dfsvc</a> and <a href="#">applaunch</a> break ClickOnce; <a href="#">customshellhost</a> breaks kiosk mode; check)                                                                             | AL deny                                                                                                                                    |
| Staging / compression                        | <a href="#">makecab</a> <a href="#">expand</a> <a href="#">extrac32</a> <a href="#">tar</a> <a href="#">compact</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Deny on servers; ringfence on workstations                                                                                                                                                                        | AL deny                                                                                                                                    |
| UAC bypass (workstations)                    | <a href="#">computerdefaults</a> <a href="#">eudcedit</a> <a href="#">iscsicpl</a> <a href="#">wsreset</a> <a href="#">odbcad32</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Deny                                                                                                                                                                                                              | AL deny                                                                                                                                    |
| Tamper                                       | <a href="#">fltmc.exe</a> <a href="#">cipher.exe</a> <a href="#">pnputil.exe</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Deny ( <a href="#">pnputil</a> permit IT)                                                                                                                                                                         | AL deny                                                                                                                                    |
| Print                                        | <a href="#">printbrm.exe</a> <a href="#">pubprn.vbs</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Deny except print-server IT during migrations                                                                                                                                                                     | AL deny                                                                                                                                    |
| Scripts                                      | <a href="#">cl_loadassembly.ps1</a> <a href="#">cl_mutexverifiers.ps1</a> <a href="#">cl_invocation.ps1</a><br><a href="#">utilityfunctions.ps1</a> <a href="#">pester.bat</a> <a href="#">launch-vsdevshell.ps1</a> <a href="#">manage-bde.wsf</a> (ringfence if BitLocker)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Deny by hash (script control on)                                                                                                                                                                                  | AL Script collection deny                                                                                                                  |
| Only if installed                            | VS, SQL and debugger tools ( <a href="#">csi</a> <a href="#">rcsi</a> <a href="#">tracker</a> <a href="#">vstest.console</a><br><a href="#">dbgsvr</a> <a href="#">windbg</a> <a href="#">remote</a> <a href="#">bginfo</a> <a href="#">msdeploy</a> <a href="#">te</a> <a href="#">coregen</a><br><a href="#">acccheckconsole</a> )                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Default deny covers; audit for any bare "Microsoft Corporation" certificate permit                                                                                                                                | —                                                                                                                                          |
| UAC bypass (most used)                       | <a href="#">fodhelper</a> <a href="#">eventvwr</a> <a href="#">sdclt</a> <a href="#">slui</a> <a href="#">dccw</a> <a href="#">perfmon</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Ringfence "no child processes" rather than deny                                                                                                                                                                   | No AL equivalent for no-child; a deny breaks the tools                                                                                     |
| Accessibility backdoors                      | <a href="#">sethc</a> <a href="#">utilman</a> <a href="#">osk</a> <a href="#">narrator</a> <a href="#">magnify</a> <a href="#">displayswitch</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Ringfence <a href="#">winlogon.exe</a> to its normal children (see C3) plus those tools, nothing else; Registry ringfence on <a href="#">Image File Execution Options</a>                                         | FIM on IFEO; no AL equivalent                                                                                                              |
| Persistence and execution                    | <a href="#">sdbinst.exe</a> (shim persistence) <a href="#">runonce.exe</a> <a href="#">gpscript.exe</a> <a href="#">wuauclt.exe</a><br>( /UpdateDeploymentProvider DLL load) <a href="#">conhost.exe</a> --headless<br><a href="#">sdiaghost.exe</a> (diagcab packages run PowerShell even with <a href="#">msdt</a> denied)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Deny <a href="#">sdbinst</a> and <a href="#">sdiaghost</a> ; ringfence no-child on <a href="#">runonce</a> <a href="#">gpscript</a> <a href="#">wuauclt</a> <a href="#">conhost</a>                               | AL deny; WDAC block rules                                                                                                                  |
| Signed downloaders and execution proxies     | Downloaders: <a href="#">ConfigSecurityPolicy.exe</a> (Defender; <a href="#">MpCmdRun - DownloadFile</a> was removed in 2020) <a href="#">OneDriveStandaloneUpdater.exe</a><br><a href="#">GfxDownloadWrapper.exe</a> (Intel) <a href="#">MsOhtmed.exe</a> <a href="#">ProtocolHandler.exe</a><br><a href="#">AppVLP.exe</a> (Office). Execution proxies: <a href="#">fsi.exe</a> <a href="#">mfttrace.exe</a><br><a href="#">OfflineScannerShell.exe</a> <a href="#">vsdiagnostics.exe</a> <a href="#">dxcapi.exe</a> (if VS or SDKs exist)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Downloaders: ringfence Internet blocked except the vendor's update FQDNs; no child processes. Proxies: deny unless the SDK is in use. All are Microsoft- or OEM-signed, so a certificate-based permit passes them | AL deny where unused; no network equivalent                                                                                                |
| AD recon and lateral movement (workstations) | <a href="#">setspn.exe</a> <a href="#">klist.exe</a> <a href="#">repadmin.exe</a> <a href="#">dcdiag.exe</a> <a href="#">ldp.exe</a><br><a href="#">adsiedit.msc</a> <a href="#">tasklist</a> <a href="#">systeminfo</a> <a href="#">tscon.exe</a> (RDP session hijack as SYSTEM) <a href="#">mstsc.exe</a> (non-IT) <a href="#">telnet.exe</a> <a href="#">sshd.exe</a> <a href="#">ssh-agent.exe</a><br>(OpenSSH Server enabled as a backdoor)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Deny for users on workstations alongside <a href="#">dsquery</a> ; <a href="#">tscon</a> deny everywhere; permit <a href="#">mstsc</a> for IT                                                                     | AL deny for users                                                                                                                          |
| Sandboxes and control escape                 | <a href="#">WindowsSandbox.exe</a> and <a href="#">.wsb</a> files, Docker Desktop, WSL ( <a href="#">wsl.exe</a> plus <a href="#">dism.exe</a> <a href="#">dismhost.exe</a> enabling the features)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Deny; code running inside these is outside the agent                                                                                                                                                              | AL deny; GPO Windows features                                                                                                              |
| VS Code tunnels ★                            | <a href="#">code.exe</a> <a href="#">tunnel</a> <a href="#">code-tunnel.exe</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Deny <a href="#">code-tunnel.exe</a> ; ringfence <a href="#">code.exe</a> Internet to the Marketplace; outbound deny <a href="#">*.tunnels.api.visualstudio.com</a> <a href="#">*.devtunnels.ms</a>               | AL deny <a href="#">code-tunnel.exe</a> ; hostname block on the DNS filter or perimeter firewall (Windows Firewall cannot match hostnames) |
| AI coding agents on servers                  | Claude Code, Codex, Gemini CLI, Cursor, Copilot CLI                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Deny on Tier 0 and Tier 1: these are shells with outbound network, the LLM-hostname concern in process form                                                                                                       | AL deny by publisher                                                                                                                       |
| Sysinternals                                 | <a href="#">livekd</a> (dumps kernel memory including LSASS) <a href="#">procexp</a> and its driver (kills EDR via BYOVD; the driver is Microsoft-signed and not on the vulnerable-driver blacklist, so the deny has to come from policy) <a href="#">sdelete</a> <a href="#">psloggedon</a> <a href="#">pskill</a><br><a href="#">psservice</a> <a href="#">adexplorer</a> <a href="#">handle</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Deny for all but the IT PAW. The Store-packaged Sysinternals Suite installs under <a href="#">WindowsApps</a>                                                                                                     | AL: add a Packaged-app deny; the default Packaged-app rule allows it                                                                       |
| Archivers and sync tools                     | <a href="#">rclone</a> <a href="#">7z.exe</a> <a href="#">rar.exe</a> WinSCP MEGASync                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Unsigned or third-party, so default deny catches them. If 7-Zip is permitted org-wide, ringfence it: no internet, no reads of <a href="#">Documents</a> or shares                                                 | AL deny                                                                                                                                    |
| Scripts, addition                            | <a href="#">slmgr.vbs</a> (the same scrobj COM hijack as <a href="#">winrm.vbs</a> )                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Deny by hash                                                                                                                                                                                                      | AL Script collection deny                                                                                                                  |

## C3 · Ringfences

ThreatLocker only. AppLocker has no equivalent; ASR is noted where it overlaps. Each ringfence tab has its own Monitor Only toggle.

### ☐ rundll32.exe

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| APPLICATIONS         | No child processes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| INTERNET             | Blocked                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| FILES / REGISTRY     | Files: deny reads of <code>comsvcs.dll</code> <code>advpack.dll</code> <code>ieadvpack.dll</code> <code>syssetup.dll</code> <code>setupapi.dll</code> <code>url.dll</code> <code>mshtml.dll</code> <code>scrobj.dll</code> <code>zipfldr.dll</code> <code>pcwutl.dll</code> <code>shdocvw.dll</code> <code>ieframe.dll</code> <code>desk.cpl</code> <code>dfshim.dll</code> <code>davclnt.dll</code> (WebDAV <code>DavSetCookie</code> )<br><code>keymgr.dll</code> ; leave <code>shell32.dll</code> |
| NOTES / FREE OVERLAP | A RunDLL policy with no ringfence configured is a plain permit; configure all three tabs. ASR LSASS rule covers the <code>comsvcs</code> case.                                                                                                                                                                                                                                                                                                                                                       |

### ☐ wmioprse.exe

|                      |                                                                                                       |
|----------------------|-------------------------------------------------------------------------------------------------------|
| APPLICATIONS         | No child processes                                                                                    |
| INTERNET             | Blocked                                                                                               |
| FILES / REGISTRY     | Off                                                                                                   |
| NOTES / FREE OVERLAP | Monitor: virtualization management, RMM and backup-agent steps use it. ASR "PsExec and WMI" overlaps. |

### ☐ dllhost.exe

|                      |                    |
|----------------------|--------------------|
| APPLICATIONS         | No child processes |
| INTERNET             | Blocked            |
| FILES / REGISTRY     | Off                |
| NOTES / FREE OVERLAP | —                  |

### ☐ reg.exe

|                      |                                                                                                                                                                  |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| APPLICATIONS         | No child processes                                                                                                                                               |
| INTERNET             | Blocked                                                                                                                                                          |
| FILES / REGISTRY     | Deny reads of <code>HKLM\SAM</code> , <code>HKLM\SECURITY</code> , <code>HKLM\SYSTEM</code> (the attack is <code>reg save</code> , not <code>reg export</code> ) |
| NOTES / FREE OVERLAP | Logon scripts and RMM use it; Monitor first.                                                                                                                     |

### ☐ net.exe net1.exe nltest.exe

|                      |                                        |
|----------------------|----------------------------------------|
| APPLICATIONS         | No child processes                     |
| INTERNET             | Blocked                                |
| FILES / REGISTRY     | —                                      |
| NOTES / FREE OVERLAP | <code>net use</code> in logon scripts. |

### ☐ sc.exe schtasks.exe

|                      |                                                                                                                                                                    |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| APPLICATIONS         | No child processes                                                                                                                                                 |
| INTERNET             | Blocked                                                                                                                                                            |
| FILES / REGISTRY     | —                                                                                                                                                                  |
| NOTES / FREE OVERLAP | Ringfencing <code>schtasks.exe</code> does not stop task execution: tasks run under <code>svchost</code> ( <code>Schedule</code> ) . Pair with 4698/4702 alerting. |

### ☐ netsh.exe

|                      |                                                              |
|----------------------|--------------------------------------------------------------|
| APPLICATIONS         | No child processes                                           |
| INTERNET             | Blocked                                                      |
| FILES / REGISTRY     | —                                                            |
| NOTES / FREE OVERLAP | Permit on the DHCP server and Hyper-V hosts; deny elsewhere. |

### ☐ **msiexec.exe**

|                      |                                             |
|----------------------|---------------------------------------------|
| APPLICATIONS         | Child processes limited to known installers |
| INTERNET             | Blocked                                     |
| FILES / REGISTRY     | —                                           |
| NOTES / FREE OVERLAP | Pair with Elevation Control.                |

### ☐ **mofcomp.exe** **fsutil.exe** **regedit.exe** **regini.exe** **certreq.exe** **control.exe** **msconfig.exe** **colorcp**

|                      |                                                                       |
|----------------------|-----------------------------------------------------------------------|
| APPLICATIONS         | No child processes                                                    |
| INTERNET             | Blocked ( <a href="#">certreq</a> : CA only)                          |
| FILES / REGISTRY     | —                                                                     |
| NOTES / FREE OVERLAP | Deny for non-admin users on workstations via Selected Users & Groups. |

### ☐ **cmd.exe** **wscript.exe** **cscript.exe**

|                      |                                                                                                            |
|----------------------|------------------------------------------------------------------------------------------------------------|
| APPLICATIONS         | No child processes except the interpreters a script legitimately calls; permit by parent for logon scripts |
| INTERNET             | Blocked                                                                                                    |
| FILES / REGISTRY     | —                                                                                                          |
| NOTES / FREE OVERLAP | Consider denying Windows Script Host for non-admins.                                                       |

### ☐ **PowerShell**

|                      |                                                                                                                                                                                                      |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| APPLICATIONS         | Constrained Mode; child processes per script need                                                                                                                                                    |
| INTERNET             | Blocked                                                                                                                                                                                              |
| FILES / REGISTRY     | —                                                                                                                                                                                                    |
| NOTES / FREE OVERLAP | Remove the PowerShell 2.0 engine. Module, script-block and transcript logging where permitted. Review any Add-Type or Windows Assembly .NET permit; with Constrained Mode it is usually unnecessary. |

### ☐ **curl.exe** **certreq.exe**

|                      |                                   |
|----------------------|-----------------------------------|
| APPLICATIONS         | No child processes                |
| INTERNET             | Approved domains only, or blocked |
| FILES / REGISTRY     | —                                 |
| NOTES / FREE OVERLAP | —                                 |

### ☐ **Microsoft Office (workstations)**

|                      |                                                                                                                                                                                                    |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| APPLICATIONS         | No <a href="#">cmd</a> <a href="#">powershell</a> <a href="#">wscript</a> <a href="#">cscript</a> <a href="#">mshta</a> <a href="#">regsvr32</a> <a href="#">certutil</a> <a href="#">rundll32</a> |
| INTERNET             | Update and authentication endpoints only                                                                                                                                                           |
| FILES / REGISTRY     | No writes to the Startup folder                                                                                                                                                                    |
| NOTES / FREE OVERLAP | ASR "Block Office child processes", "Block Office from creating executable content"; MOTW macro block GPO.                                                                                         |

### ☐ **Browsers**

|                      |                                                                  |
|----------------------|------------------------------------------------------------------|
| APPLICATIONS         | Own helpers only                                                 |
| INTERNET             | —                                                                |
| FILES / REGISTRY     | No reads of other browsers' profile directories                  |
| NOTES / FREE OVERLAP | Extension allowlist by GPO (ThreatLocker cannot see extensions). |

### ☐ **PDF readers, Teams, Zoom, Outlook,** [msedgewebview2](#) [msedge\\_proxy](#) [squirrel.exe](#) [update.exe](#)

|                      |                                                   |
|----------------------|---------------------------------------------------|
| APPLICATIONS         | No child processes                                |
| INTERNET             | —                                                 |
| FILES / REGISTRY     | —                                                 |
| NOTES / FREE OVERLAP | ASR "Block executable content from email client". |

## ☐ `explorer.exe`

|                      |                                                              |
|----------------------|--------------------------------------------------------------|
| APPLICATIONS         | —                                                            |
| INTERNET             | —                                                            |
| FILES / REGISTRY     | Block launches from <code>%TEMP%</code> , Downloads, AppData |
| NOTES / FREE OVERLAP | Storage Control plus ringfence.                              |

## ☐ `spoolsv.exe` (print server only)

|                      |                                                                                                                         |
|----------------------|-------------------------------------------------------------------------------------------------------------------------|
| APPLICATIONS         | <code>PrintIsolationHost</code> , <code>splwow64</code> , <code>printfilterpipelinesvc</code> and the print vendor only |
| INTERNET             | Blocked                                                                                                                 |
| FILES / REGISTRY     | Deny writes to <code>spool\drivers</code> by anything else                                                              |
| NOTES / FREE OVERLAP | Disable the service everywhere else.                                                                                    |

## ☐ `wsmprovhost.exe` (Hyper-V hosts only)

|                      |                                                                                                                                                                                                                                                            |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| APPLICATIONS         | No child processes except what Monitor shows (the remote runspace runs inside <code>wsmprovhost</code> itself and never spawns <code>powershell.exe</code> ; children are whatever remote commands call, such as <code>netsh</code> or <code>dism</code> ) |
| INTERNET             | Blocked                                                                                                                                                                                                                                                    |
| FILES / REGISTRY     | —                                                                                                                                                                                                                                                          |
| NOTES / FREE OVERLAP | Deny elsewhere.                                                                                                                                                                                                                                            |

## ☐ `w3wp.exe` ★ (IIS, Exchange, SharePoint)

|                      |                                                                                                                                                               |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| APPLICATIONS         | No child processes: a webshell spawns <code>cmd</code> or <code>powershell</code> under the worker                                                            |
| INTERNET             | —                                                                                                                                                             |
| FILES / REGISTRY     | —                                                                                                                                                             |
| NOTES / FREE OVERLAP | Server-side code hosts need the no-child ringfence the interpreter row gives <code>java</code> . Monitor first for app pools that legitimately spawn helpers. |

## ☐ `sqlservr.exe`

|                      |                                                                                                 |
|----------------------|-------------------------------------------------------------------------------------------------|
| APPLICATIONS         | No child processes ( <code>xp_cmdshell</code> )                                                 |
| INTERNET             | Blocked                                                                                         |
| FILES / REGISTRY     | —                                                                                               |
| NOTES / FREE OVERLAP | Also disable <code>xp_cmdshell</code> and Ole Automation in SQL; the ringfence is the backstop. |

## ☐ `services.exe`

|                      |                                                                                                                                    |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------|
| APPLICATIONS         | Children limited to known service binaries (smbexec-style service > <code>cmd</code> )                                             |
| INTERNET             | Blocked                                                                                                                            |
| FILES / REGISTRY     | —                                                                                                                                  |
| NOTES / FREE OVERLAP | Monitor 2–4 weeks; pair with 7045 alerting on a new service whose ImagePath contains <code>cmd</code> or <code>powershell</code> . |

## ☐ Backup service binaries

|                      |                                                                                                             |
|----------------------|-------------------------------------------------------------------------------------------------------------|
| APPLICATIONS         | No child processes except the backup product's own components                                               |
| INTERNET             | Vendor FQDNs only                                                                                           |
| FILES / REGISTRY     | —                                                                                                           |
| NOTES / FREE OVERLAP | A backup server runs as the most privileged account in the domain; its services should never spawn a shell. |

## ☐ `winlogon.exe`

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| APPLICATIONS         | Children limited to <code>userinit</code> , <code>LogonUI</code> , <code>dwm</code> , <code>fontdrvhost</code> , <code>mpnotify</code> , <code>wlrmrdr</code> , <code>rdpclip</code> (RDP sessions) and the accessibility tools <code>sethc</code> , <code>utilman</code> , <code>osk</code> , <code>narrator</code> , <code>magnify</code> , <code>displayswitch</code> , nothing else; confirm the list against two weeks of Monitor before enforcing |
| INTERNET             | Blocked                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| FILES / REGISTRY     | Registry ringfence: deny writes under <code>Image File Execution Options</code>                                                                                                                                                                                                                                                                                                                                                                         |
| NOTES / FREE OVERLAP | Closes the sticky-keys family of backdoors. Free: FIM on IFEO.                                                                                                                                                                                                                                                                                                                                                                                          |

### ❑ `vmwp.exe` (Hyper-V)

|                      |                                                                                                                                   |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| APPLICATIONS         | —                                                                                                                                 |
| INTERNET             | Blocked                                                                                                                           |
| FILES / REGISTRY     | <b>Never</b> add a Files or Registry ringfence to <code>vmms</code> <code>vmwp</code> <code>vmcompute</code> <code>clussvc</code> |
| NOTES / FREE OVERLAP | —                                                                                                                                 |

### ❑ Vendor suites (HVAC, VMS, print management)

|                      |                                                            |
|----------------------|------------------------------------------------------------|
| APPLICATIONS         | Own processes only                                         |
| INTERNET             | Vendor license and update FQDNs only                       |
| FILES / REGISTRY     | Deny reads outside install, data and recording paths       |
| NOTES / FREE OVERLAP | Monitor 3–4 weeks; the noisiest ringfences you will build. |

### ❑ Interpreters where required ( `java` `python` `node` )

|                      |                                                                                  |
|----------------------|----------------------------------------------------------------------------------|
| APPLICATIONS         | No child processes except the vendor's                                           |
| INTERNET             | Blocked                                                                          |
| FILES / REGISTRY     | Deny <code>%TEMP%</code> and Downloads                                           |
| NOTES / FREE OVERLAP | Permit by path + certificate of the vendor's bundled runtime, never system-wide. |

## C4 · Fixes to an inherited policy set

Most ThreatLocker tenants were built over years by more than one admin. These are the patterns to look for before adding anything new.

| PATTERN                                                                                                                                                                             | ACTION                                                                                                 |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|
| Policies named "Ringfenced" with empty ringfence tabs (WMI, Office, Office Installer, RunDLL are the usual ones)                                                                    | Configure the tabs, or remove the application from DC and server groups                                |
| Each group's Default policy                                                                                                                                                         | Confirm <b>Deny</b> , not Monitor                                                                      |
| Time-windowed deny policies (nights-and-weekends style)                                                                                                                             | Retire; make the deny permanent (Task Manager and the like)                                            |
| An MMC block policy on DCs                                                                                                                                                          | Keep; remove redundant per-snap-in entries such as <code>dsa.msc</code>                                |
| Denies that sit below a broad permit ( <code>certutil</code> <code>signtool</code> <code>mshta</code> <code>bcdedit</code> at a higher order number than a Microsoft-signed permit) | Move them into the top deny block                                                                      |
| Browsers, Office, OneDrive, Google Updater, Windows Phone, Communication App on DCs and servers                                                                                     | Uninstall; delete the policies; explain any historical match in Unified Audit                          |
| <code>spoolsv.exe</code> on DCs                                                                                                                                                     | Ringfence until print is off the DC, then disable the service + Deny. Print belongs on a member server |
| Add-Type .NET / Windows Assembly .NET permits                                                                                                                                       | Review any historical match; usually unnecessary with Constrained Mode                                 |

## C5 · Workstation-specific

### ☐ Deny remote execution and admin tools for users

|                  |                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| THREATLOCKER     | <code>winrs</code> <code>wsmprohost</code> <code>winrshost</code> <code>psexec</code> <code>paexec</code> <code>wmic</code> <code>schtasks</code> <code>at</code> <code>dsquery</code> <code>dsget</code> <code>ldifde</code> <code>csvde</code> <code>adfind</code> <code>nltest</code> <code>dsacis</code> , RSAT, SharpHound / BloodHound / AD Explorer / PingCastle / PowerView, <code>mmc</code> |
| APPLOCKER / FREE | AL deny; Everyone deny + IT allow                                                                                                                                                                                                                                                                                                                                                                     |

### ☐ Recon tools

|                  |                                                                                                                                                                                        |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| THREATLOCKER     | <code>whoami</code> <code>quser</code> <code>qwinsta</code> <code>nbtstat</code> <code>arp</code> <code>route</code> <code>netstat</code> : deny or ringfence (Monitor; logon scripts) |
| APPLOCKER / FREE | AL deny for users                                                                                                                                                                      |

### ☐ Credential CLIs

|                  |                                                                                                                                          |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| THREATLOCKER     | <code>cmdkey</code> <code>vaultcmd</code> ringfence; Storage Control on browser <code>Login Data</code> and <code>System32\config</code> |
| APPLOCKER / FREE | ASR LSASS; no AL equivalent for storage                                                                                                  |

### ☐ Elevation Control

|                  |                                                                                           |
|------------------|-------------------------------------------------------------------------------------------|
| THREATLOCKER     | No local admins; installers elevated by policy; alert on the first-ever elevation request |
| APPLOCKER / FREE | LAPS + no local admin; no equivalent for just-in-time elevation                           |

### ☐ Admin hygiene

|                  |                                                                                                                                               |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| THREATLOCKER     | No admin, especially a Domain Admin, types a password on a workstation; Protected Users + deny interactive logon for DA on the workstation OU |
| APPLOCKER / FREE | GPO                                                                                                                                           |

### ☐ Interpreters

|                  |                                                                                                                                                   |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| THREATLOCKER     | <code>python</code> <code>node</code> <code>java</code> <code>autoit3</code> <code>AutoHotkey</code> : deny unless needed; ringfence where needed |
| APPLOCKER / FREE | AL deny                                                                                                                                           |

### ☐ File associations

|                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| THREATLOCKER     | <code>.js</code> <code>.jse</code> <code>.vbs</code> <code>.vbe</code> <code>.wsf</code> <code>.wsh</code> > Notepad; also <code>.hta</code> <code>.msc</code> (GrimResource) <code>.chm</code> <code>.scr</code> <code>.pif</code> <code>.cpl</code> <code>.reg</code> <code>.scf</code> <code>.xll</code> <code>.rdp</code> (rogue-RDP phishing) <code>.library-ms</code> <code>.search-ms</code> <code>.vhd</code> <code>.vhdx</code> <code>.application</code> ; <code>.iso</code> / <code>.img</code> mount handler removed or Storage Control deny; disable the <code>search-ms:</code> and <code>ms-appinstaller:</code> protocol handlers ( <code>EnableMSAppInstallerProtocol = 0</code> ); remove <code>ms-msdt:</code> |
| APPLOCKER / FREE | GPO                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

### ☐ Browser extensions

|                  |                                                                                |
|------------------|--------------------------------------------------------------------------------|
| THREATLOCKER     | Allowlist by ID (Chrome / Edge GPO or Google Admin); Chrome Remote Desktop off |
| APPLOCKER / FREE | GPO / Admin console                                                            |

### ☐ Storage Control

|                  |                                                                                                                                                                          |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| THREATLOCKER     | Deny execution from <code>%TEMP%</code> , Downloads, <code>AppData\Local\Temp</code> , <code>C:\Users\Public</code> , unowned <code>ProgramData</code> , removable media |
| APPLOCKER / FREE | AL path deny rules (partial)                                                                                                                                             |

### ☐ Rollout

|                  |                                                                      |
|------------------|----------------------------------------------------------------------|
| THREATLOCKER     | Monitor 4–6 weeks; carve permits by parent for logon scripts and RMM |
| APPLOCKER / FREE | AL audit mode                                                        |

## C6 · Servers by role

Role-by-role summary.

| ROLE          | TIER | KEY PERMITS                                                                                                                   | KEY DENIES / NOTES                                                                                                                                                                                                                                                                                                    | INBOUND                                                                               | OUTBOUND                                                  |
|---------------|------|-------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|-----------------------------------------------------------|
| DHCP          | 1    | <code>netsh</code> ringfenced, <code>mmc</code> ringfenced                                                                    | Nothing third-party; dedicated DNS update credential; DHCP snooping on switches; no Option 252                                                                                                                                                                                                                        | UDP 67 from clients and relays; 647 failover; 135 + RPC from the jump host            | 68; 53/88/389/445 to DCs; 647                             |
| Print         | 1    | <code>spoolsv</code> ringfenced to its helpers + the print-management suite by certificate                                    | <code>printbrm</code> IT only; Point-and-Print restrictions; <code>RestrictDriverInstallationToAdministrators = 1</code> ; <code>RpcAuthnLevelPrivacyEnabled = 1</code> ; v4 drivers                                                                                                                                  | 445, 135 + RPC, 9191/9192 from client VLANs                                           | 9100/515/631/161 to the printer VLAN; DCs; vendor license |
| HVAC / BAS    | OT   | Vendor suite + bundled JRE by path + certificate, ringfenced                                                                  | Not domain-joined if possible; vendor RMM denied; vendor access time-boxed via ZTNA or jump host; controllers inbound only from this server                                                                                                                                                                           | 80/443 from the facilities VLAN or jump host; 47808/1911/502 from the controller VLAN | Controller VLAN; vendor FQDNs; SMTP relay; NTP            |
| Hyper-V       | 0    | Core Files; backup transport components by certificate; <code>wsmprovhost</code> ringfenced only if WAC or PowerShell is used | No Files ringfence on <code>vmms</code> , <code>vmwp</code> , <code>vmcompute</code> , <code>clussvc</code> ; <code>netsh</code> ringfenced; BitLocker CSVs; vTPM on DC, backup and sync VMs; Storage Control on <code>*, vhd*</code> outside VM paths; alert on DC export or checkpoint; Hyper-V Administrators = DA | 3389/5985/135 from the PAW; 445/6600/3343 between nodes; the backup server            | Nodes, storage (3260/445), DCs, WSUS; <b>no internet</b>  |
| Camera / VMS  | OT   | Vendor suite + SQL Express by certificate, ringfenced                                                                         | Cameras inbound only from the VMS, no internet; recording path under Storage Control; footage not in the primary backup                                                                                                                                                                                               | Vendor client ports from the security-staff VLAN; 3389 from the jump host             | 554/80/443 to the camera VLAN; vendor FQDNs; SMTP; NTP    |
| ESXi (if any) | 0    | —                                                                                                                             | ThreatLocker does not run here: lockdown mode, SSH off, vCenter MFA, management VLAN from the PAW only, vCenter export and snapshot alerting                                                                                                                                                                          | —                                                                                     | —                                                         |

## C7 · Network Control and Windows Firewall GPO

### ☐ Workstation › DC

|                 |                                                                                                                                                                                                                                                                                   |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RULE            | Allow 53, 88, 123/udp (w32time; without it clock skew breaks Kerberos within weeks), 389/636 plus 389/udp (LDAP, used by the DC locator), 445 (SYSVOL and NETLOGON; required for GPO), 464, 3268/3269, 135 + RPC dynamic (test before cutting). Deny 5985/5986, 3389, 139/NetBIOS |
| FREE EQUIVALENT | Windows Firewall inbound rules on the DC OU scoped to source subnets                                                                                                                                                                                                              |

### ☐ Jump host / PAW › DCs and servers

|                 |                                                                                           |
|-----------------|-------------------------------------------------------------------------------------------|
| RULE            | Allow 3389, 5985/5986 (where WinRM is kept), 135/445 admin from the jump host object only |
| FREE EQUIVALENT | Firewall rule with remote IP = jump host                                                  |

### ☐ Workstation › workstation

|                 |                                                |
|-----------------|------------------------------------------------|
| RULE            | Deny all inbound on 445, 135, 3389, 5985, 5900 |
| FREE EQUIVALENT | Firewall inbound block on the workstation OU   |

### ☐ Workstation › internet

|                 |                                                                                                                                           |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| RULE            | Deny 445/139/137-138 (NTLM leak), 25, 1433, 3389, 5985, 22 (except IT), 4443/8443/9001; 53/853 only to internal DNS; DoH hostnames denied |
| FREE EQUIVALENT | Firewall outbound block rules                                                                                                             |

### ☐ Servers › internet

|                 |                                                                                                                                                                       |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RULE            | <b>Default deny.</b> Allow WSUS / Windows Update, Defender, NTP, KMS, CA CRL, ThreatLocker, RMM, backup cloud, named vendor FQDNs. Alert on any LLM-provider hostname |
| FREE EQUIVALENT | Perimeter firewall per VLAN; Windows Firewall outbound default block on the server OU                                                                                 |

### ☐ Printer, camera and controller VLANs

|                 |                                             |
|-----------------|---------------------------------------------|
| RULE            | Inbound only from their server; no internet |
| FREE EQUIVALENT | Perimeter firewall                          |

### ☐ Guest and BYOD

|                 |                                                                      |
|-----------------|----------------------------------------------------------------------|
| RULE            | Internet only; no route to server or management subnets; logged deny |
| FREE EQUIVALENT | Perimeter firewall                                                   |

### ☐ RDP schedule

|                 |                                                                        |
|-----------------|------------------------------------------------------------------------|
| RULE            | Server RDP restricted to business hours; break-glass via the jump host |
| FREE EQUIVALENT | Perimeter firewall schedule                                            |

### ☐ WinRM

|                 |                                                                                                                                                                   |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RULE            | Service disabled by GPO on workstations and on servers nobody manages remotely; 5985/5986 open only from the management subnet where kept; HTTPS + JEA where used |
| FREE EQUIVALENT | GPO + firewall                                                                                                                                                    |

### ☐ QUIC and Encrypted Client Hello ★

|                 |                                                                                                                                                                                       |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RULE            | Block UDP 443 (QUIC) at the perimeter and in Network Control, or TLS inspection is bypassed entirely. Disable Encrypted Client Hello in browsers by GPO: SNI filtering is blind to it |
| FREE EQUIVALENT | Firewall outbound block UDP 443; Chrome and Edge <code>EncryptedClientHelloEnabled = 0</code>                                                                                         |

## ❑ WebClient service ★

|                 |                                                                                                                                                                                             |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RULE            | Disable the WebClient service by GPO. The 445 egress deny does nothing against WebDAV over 80/443 ( <code>\\host@80\</code> , <code>.library-ms</code> , <code>search-ms</code> NTLM leaks) |
| FREE EQUIVALENT | GPO System Services > WebClient = Disabled                                                                                                                                                  |

## ❑ DNS resolver side ★

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RULE            | "53 only to internal DNS" does not stop tunneling: the DC resolves recursively for the attacker. Forward the DCs to a filtering resolver that logs, rate-limits and blocks DGA and tunnel patterns. Prohibit Windows 11 native DoH by GPO (separate from the browser setting). Block known DoH resolvers: by IP in Windows Firewall ( <code>1.1.1.1</code> , <code>8.8.8.8</code> , <code>9.9.9.9</code> and the published ranges for NextDNS, AdGuard, Mullvad and Control D) and by hostname on the DNS filter ( <code>dns.nextdns.io</code> , <code>dns.adguard.com</code> , <code>dns.mullvad.net</code> , <code>dns.controlld.com</code> ) |
| FREE EQUIVALENT | DNS Server forwarders; GPO Network > DNS Client > Configure DNS over HTTPS = Prohibit; firewall IP block                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

## ❑ IPv6 tunnels, WPAD, STUN, SSDP

|                 |                                                                                                                                                                                                                                                                                                           |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RULE            | Disable Teredo, 6to4 and ISATAP; block protocol 41 and UDP 3544; prefer IPv4 to defang mitm6. Disable WPAD auto-proxy and block the <code>wpad</code> name. STUN (UDP 3478; TLS variant on TCP 5349): most P2P remote tools and WebRTC C2 need it; allow only to Teams and Zoom ranges. Disable SSDP/UPnP |
| FREE EQUIVALENT | GPO TCP/IP settings and <code>netsh interface teredo set state disabled</code> ; DNS block on <code>wpad</code> ; firewall                                                                                                                                                                                |

## ❑ Workstation egress default-deny with an explicit proxy

|                 |                                                                                                                                                                                                             |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RULE            | Instead of listing bad ports, make workstation egress default-deny through an explicit proxy. That collapses the port list (plus 1080, 4444, 50050, 6667/6697, 5222, 1883, 9001, 1194, 51820) into one rule |
| FREE EQUIVALENT | Firewall outbound default block on the workstation OU; proxy by GPO                                                                                                                                         |

## ❑ Registry and file ringfences on proxy and host pivots

|                 |                                                                                                                                                                                                                                                                                  |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RULE            | FIM or Registry ringfence on <code>PortProxy</code> ( <code>netsh portproxy</code> SOCKS pivots), <code>Internet Settings\ProxyServer</code> and <code>AutoConfigURL</code> , <code>drivers\etc\hosts</code> , and Outlook <code>WebView\Inbox\URL</code> (Specula home-page C2) |
| FREE EQUIVALENT | File-integrity monitoring and registry auditing to the SIEM                                                                                                                                                                                                                      |

## C8 · Egress and command-and-control

### ❑ RMM abuse

#### CONTROL

Permit one RMM by certificate + path; **explicit deny** every other (AnyDesk, ScreenConnect, Atera, Splashtop, TeamViewer, NetSupport, Level, RustDesk, Syncro, Action1, Supremo, LogMeIn, GoTo, Zoho, VNC, Ammyy, DWAgent); deny [quickassist.exe](#) and [msra.exe](#) for non-IT; outbound denies to other vendors' relays and ports (5938, 6568/7070, 8040/8041, 5900-5910, 7000). Also deny the ones leading recent intrusion statistics: SimpleHelp, Kaseya VSA, NinjaOne, Datto RMM ( [CagService](#) ), N-able Take Control ( [BASupSvc](#) ), Pulseway, ManageEngine / Zoho Assist, BeyondTrust / Bomgar, MeshAgent / Tactical RMM, Remote Utilities ( [rutserv.exe](#) ), UltraViewer, AeroAdmin, Radmin (4899), Iperius, RemotePC, Parsec, NoMachine (4000), DameWare (6129), Getscreen, ISL Online, Chrome Remote Desktop host ( [remoting\\_host.exe](#) ); ports RustDesk 21115–21119, NetSupport 5405, Splashtop 6783–6785, Kaseya 5721, Remote Utilities 5650

#### FREE EQUIVALENT

AL publisher deny per vendor; firewall outbound block

### ❑ Tunnelers

#### CONTROL

Deny [cloudflared](#) [ngrok](#) [tailscale](#) [chisel](#) [ligolo](#) [frp](#) [plink](#) [socat](#) [devtunnel](#); [netsh](#) ringfenced; deny outbound to [\\*.ngrok.io](#) [\\*.ngrok-free.app](#) [\\*.trycloudflare.com](#) [\\*.argotunnel.com](#) [\\*.tailscale.com](#) [\\*.zerotier.com](#) [\\*.localtonet.com](#). Also: [\\*.ngrok.app](#) [\\*.ngrok.dev](#) [connect.ngrok-agent.com](#) [\\*.cfargotunnel.com](#) [localhost.run](#) [serveo.net](#) [pinggy.io](#) [\\*.locx.io](#) (LocalXpose) [zrok.io](#) [playit.gg](#) [bore.pub](#) [pagekite.net](#) [\\*.ts.net](#) (Tailscale Funnel) [\\*.netbird.io](#), Hamachi, Cloudflare WARP ( [warp-svc.exe](#) ), [\\*.cloudflareclient.com](#), commercial VPN clients (Proton, Mullvad, Nord), Tor ( [tor.exe](#) ), directory-authority IPs, the Snowflake broker; Brave bundles Tor, set [TorDisabled](#), I2P (7657), Psiphon, v2ray / Xray, gost, rathole, revsocks; Edge Secure Network, Opera VPN and iCloud Private Relay ( [mask.icloud.com](#) ) off via GPO

#### FREE EQUIVALENT

AL deny (mostly unsigned, so default deny catches them); proxy or firewall hostname block

### ❑ Cloud-service C2 and exfiltration

#### CONTROL

Deny Discord CDN and webhooks, [api.telegram.org](#), WhatsApp Web, Pastebin, transfer.sh, file.io, anonfiles, gofile, mega.nz, ShareFile / Dropbox / Box / WeTransfer unless used; **tenant restrictions** for M365 and Google at the proxy; deny workstation 80/443 to raw cloud-compute IP ranges unless allowlisted; NRD and uncategorized blocked. Dead-drop, webhook and storage C2: Slack ( [hooks.slack.com](#), [files.slack.com](#) ), Teams incoming webhooks ( [\\*.webhook.office.com](#) ), Power Automate ( [\\*.logic.azure.com](#) ), Zapier and IFTTT hooks, [t.me](#) and [telegra.ph](#), Trello, Notion and Airtable APIs, [steamcommunity.com/profiles](#) (Vidar's resolver), [api.github.com](#), gists and [raw.githubusercontent.com](#), GitLab, Imgur, Dropbox and Box API hosts, [\\*.blob.core.windows.net](#) [\\*.s3.amazonaws.com](#) [storage.googleapis.com](#) [firebaseio.com](#), Backblaze, Wasabi, [\\*.r2.dev](#). Free hosting as C2: [\\*.workers.dev](#) [\\*.pages.dev](#) [\\*.vercel.app](#) [\\*.netlify.app](#) [\\*.herokuapp.com](#) [\\*.onrender.com](#) [\\*.fly.dev](#) [\\*.glitch.me](#) [\\*.replit.app](#) [\\*.hf.space](#) [\\*.github.io](#) [\\*.azurewebsites.net](#) [\\*.cloudfunctions.net](#) [\\*.run.app](#) [script.google.com](#). Pastes: [paste.ee](#) [reentry.co](#) [hastebin](#), [privatebin](#), [controlc.com](#) [termbin.com](#) [0x0.st](#) [catbox.moe](#) [pixeldrain](#), [bashupload](#), [temp.sh](#) [filebin.net](#) [ufile.io](#)

#### FREE EQUIVALENT

Proxy or SWG only; a classroom web filter covers domain blocklists but not IP, port, process or tenant restrictions

### ❑ Dynamic DNS ★

#### CONTROL

AsyncRAT, XWorm, Remcos, DcRAT and Quasar almost all use [\\*.duckdns.org](#), No-IP ( [\\*.ddns.net](#) [\\*.hopto.org](#) [\\*.zaproto.org](#) [\\*.sytes.net](#) [\\*.myftp.org](#) [\\*.redirectme.net](#) [\\*.servehttp.com](#) ), [\\*.dyndns.org](#) [\\*.dynu.net](#), afraid.org domains ( [\\*.mo00.com](#) [\\*.chickenkiller.com](#) ), [\\*.cloudns.\\*](#). NRD blocking does not catch these; the parent domains are old. Block the Dynamic-DNS category at the proxy and alert on any hit

#### FREE EQUIVALENT

Proxy or SWG category block; DNS log alert

### ❑ SMTP and FTP exfiltration ★

#### CONTROL

Denying 25 alone is not enough: Agent Tesla, Snake Keylogger and most stealers exfiltrate over 587/465/2525 to [smtp.gmail.com](#), [smtp.office365.com](#), SendGrid, Mailgun and Brevo. Deny 25/465/587/2525 from everything except the mail relay. Same for 21/FTP

#### FREE EQUIVALENT

Firewall outbound block with the relay as the only exception

### ❑ Never-legitimate tripwires

#### CONTROL

Cheap, high-signal, no false positives: OAST and collaborator domains ( [\\*.oast.\\*](#) [\\*.oastify.com](#) [\\*.burpcollaborator.net](#) [interact.sh](#) [dnslog.cn](#) [webhook.site](#) [requestbin](#), [pipedream](#), [ntfy.sh](#) ); external-IP checks from a non-browser process ( [api.ipify.org](#) [ifconfig.me](#) [icanhazip.com](#) [ipinfo.io](#) [ip-api.com](#) [checkip.amazonaws.com](#) ); any process other than Office, Teams, OneDrive and browsers reaching [graph.microsoft.com](#) [login.microsoftonline.com](#) [\\*.sharepoint.com](#) [docs.google.com](#) [www.googleapis.com](#). That per-process rule is the only practical defense against OneDrive or Google-Docs C2 in a tenant that must allow those hosts

#### FREE EQUIVALENT

Proxy and DNS log alerts; no free per-process equivalent

### ❑ DNS tunneling

#### CONTROL

53/853 only to internal DNS; DoH endpoints denied; browser DoH off by GPO; public resolvers blocked by IP; DNS query logging with TXT-volume and entropy alerts

#### FREE EQUIVALENT

Firewall + GPO + DNS logs to the SIEM

## ❑ ICMP and protocol

|                 |                                                        |
|-----------------|--------------------------------------------------------|
| CONTROL         | Deny outbound ICMP from workstations except monitoring |
| FREE EQUIVALENT | Firewall                                               |

## ❑ Loaders

|                 |                                                                                                                                                                                                                                                                                          |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CONTROL         | Interpreters denied or ringfenced; Electron and WebView no child processes; WSH off for users; file associations remapped; ISO mount handler removed; extension allowlist; MOTW macro block; HVCI + vulnerable-driver blocklist; <a href="#">mavinject</a> deny + rundll32 DLL blocklist |
| FREE EQUIVALENT | ASR + GPO + WDAC driver blocklist                                                                                                                                                                                                                                                        |

## ❑ Segmentation

|                 |                                                                                                                                                                                                         |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CONTROL         | Endpoint inbound default-deny; servers reachable only on service ports; Tier 0 on its own VLAN from PAWs only; IoT, printer and camera VLANs isolated; a micro-segmentation product where budget allows |
| FREE EQUIVALENT | Perimeter firewall VLAN ACLs + firewall GPO                                                                                                                                                             |

## ❑ Egress architecture

|                 |                                                                                                                                                                                            |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CONTROL         | Both ThreatLocker Network Control (per process) and the perimeter firewall (catches what the agent missed); a proxy with TLS inspection, category and reputation, NRD, tenant restrictions |
| FREE EQUIVALENT | —                                                                                                                                                                                          |

## C9 · Identity and protocol

GPO; the same for ThreatLocker and AppLocker environments.

### ☐ DCSync rights

|                |                                                                                                                                    |
|----------------|------------------------------------------------------------------------------------------------------------------------------------|
| IMPLEMENTATION | Only DCs, Administrators and one sync account hold Replicating Directory Changes All; delete stale MSOL_, ADSync and Exchange ACEs |
| AUDIT FIRST    | Event 4662 with GUID <code>1131f6ad-9c07-11d1-f79f-00c04fc2dcd2</code> from a non-DC > alert                                       |

### ☐ krbtgt

|                |                                                |
|----------------|------------------------------------------------|
| IMPLEMENTATION | Rotate twice, 24 h apart; after any compromise |
| AUDIT FIRST    | —                                              |

### ☐ Protected Users

|                |                                                                                                                                 |
|----------------|---------------------------------------------------------------------------------------------------------------------------------|
| IMPLEMENTATION | Every human admin and <code>-adm</code> account, one per day; break-glass excluded; deny-logon GPO on the workstation OU for DA |
| AUDIT FIRST    | Test one account; watch 4625 and 4771                                                                                           |

### ☐ NTLMv1

|                |                                                                                                  |
|----------------|--------------------------------------------------------------------------------------------------|
| IMPLEMENTATION | <code>LmCompatibilityLevel = 5</code> , DCs first, then all; no LM hash storage                  |
| AUDIT FIRST    | NTLM audit 8004 / 4624 <code>LmPackageName = NTLM V1</code> for 2 weeks; copiers are the holdout |

### ☐ LDAP signing and channel binding

|                |                                                                                                 |
|----------------|-------------------------------------------------------------------------------------------------|
| IMPLEMENTATION | Required                                                                                        |
| AUDIT FIRST    | Event 2889 on DCs for 2 weeks; fix the web filter, print-management, VPN and RADIUS binds first |

### ☐ SMB signing

|                |                 |
|----------------|-----------------|
| IMPLEMENTATION | Required on all |
| AUDIT FIRST    | —               |

### ☐ AD CS

|                |                                                                                                                                                          |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| IMPLEMENTATION | Locksmith monthly; no enrollee-supplied subject with client auth for broad groups; manager approval; lock template ACLs (ESC4 > ESC1); AD CS not on a DC |
| AUDIT FIRST    | Locksmith report                                                                                                                                         |

### ☐ DnsAdmins

|                |                                                                                                                                               |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| IMPLEMENTATION | Treat as Domain Admins on any DNS server missing the October 2021 update; audit membership everywhere; pair with the <code>dnscmd</code> deny |
| AUDIT FIRST    | —                                                                                                                                             |

### ☐ DSRM

|                |                                                |
|----------------|------------------------------------------------|
| IMPLEMENTATION | Rotate; <code>DsrAdminLogonBehavior = 0</code> |
| AUDIT FIRST    | —                                              |

### ☐ Logon rights

|                |                                                                                                                                                                                              |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IMPLEMENTATION | Default Domain Controllers Policy: deny network, batch, service and RDP logon for all non-tier-0, including service and automation accounts; smart card or Windows Hello for Business for DA |
| AUDIT FIRST    | <code>gpresult</code> ; scope to the DC OU only                                                                                                                                              |

## ☐ Hypervisor admins

IMPLEMENTATION Tier 0; PAW only; vTPM + BitLocker on DC VMs; snapshot and export alerting

AUDIT FIRST —

## ☐ Backup and VM export hygiene

IMPLEMENTATION Never land a DC VMDK, VHDX, IFM or system-state on a general share; Storage Control on \*.vmdk \*.vhdx \*.vhd \*.bak \*.dit outside the repository; backup server off-domain or Tier 0; immutable repository; backup admins not DA; alert on retention change

AUDIT FIRST —

## ☐ BYOVD

IMPLEMENTATION HVCI / Memory Integrity + the Microsoft vulnerable-driver blocklist on DCs, servers and workstations; alert on new driver loads

AUDIT FIRST WDAC driver blocklist

## ☐ LDAP enumeration

IMPLEMENTATION Event 1644 expensive-query logging; alert on one host issuing thousands of queries in minutes

AUDIT FIRST —

## ☐ LLMNR, NBT-NS and mDNS

IMPLEMENTATION Off by GPO; NetBIOS off via DHCP; EnableMDNS = 0

AUDIT FIRST —

## ☐ Spooler on DCs and hypervisors

IMPLEMENTATION Disabled

AUDIT FIRST Get-Service Spooler

## ☐ LAPS

IMPLEMENTATION Windows LAPS; 30-day + on-use rotation; audit reads

AUDIT FIRST —

## ☐ Password policy

IMPLEMENTATION Length over rotation; fine-grained policy for admins and service accounts

AUDIT FIRST —

## ☐ LSASS hardening

IMPLEMENTATION RunAsPPL with the UEFI lock; Credential Guard (Enterprise and Education SKUs since Windows 10, Server 2016+; on by default from Windows 11 22H2 Enterprise); wDigest UseLogonCredential = 0 ; Remote Credential Guard or Restricted Admin for RDP; reduced CachedLogonsCount on servers. Every LSASS-dumper deny in C2 is a tripwire; these make the dump worthless even when a new tool slips past

AUDIT FIRST Credential Guard readiness tool; check LSA protection events 12 and 3065/3066 before enabling the UEFI lock

## ☐ Automation and agent accounts

IMPLEMENTATION Dedicated scoped account; denied all logon types to DCs; no portal access; rotate any credential an AI agent was run with

AUDIT FIRST —

---

## C11 · ThreatLocker portal and agent protection

### ☐ Portal

CONTROL

MFA enforced; no shared admin accounts; IP allowlist; alert on any computer moved out of Secured mode and any policy edit in the DC and Tier 0 groups

### ☐ Agent

CONTROL

Uninstall password set; tamper protection on

### ☐ AppLocker equivalent

CONTROL

Application Identity service Automatic + alert on stop; GPO permissions audited (who can edit the AppLocker GPO = who can disable it)

## C12 · Verification and troubleshooting

| SYMPTOM / CHECK                                  | WHERE TO LOOK                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Did a policy block something?                    | Unified Audit > group > Action Deny > date > group by application. AppLocker: Event 8004 (8003 in audit) for EXE and DLL; 8007 (8006) for scripts and MSI                                                                                                                                                                                                                                   |
| Are DCs actually enforcing?                      | Group mode = Secured; Default = Deny; an empty "Last Match" on existing denies can mean the group was still in Learning or Monitor                                                                                                                                                                                                                                                          |
| "Users can't sign in, a password reset fixes it" | Not an application-control symptom. Check <b>4740</b> lockouts (caller computer > the retrying ringfenced app); unlock without reset to confirm; <b>4723 vs 4724</b> for expired or must-change; <b>4768/4771</b> <code>0xE / 0x18</code> for RC4 and AES key issues (Protected Users or the encryption GPO). Bulk unlock: <a href="#">Search-ADAccount -LockedOut \   Unlock-ADAccount</a> |
| GPO not applying after Network Control           | 445 to DCs blocked; Event 1058/1030 on clients                                                                                                                                                                                                                                                                                                                                              |
| Backups "succeed" but no guest processing        | backup job warnings; ThreatLocker deny on the backup agent runtime                                                                                                                                                                                                                                                                                                                          |
| Which clients would break on LDAP signing        | Event 2889                                                                                                                                                                                                                                                                                                                                                                                  |
| Which devices still use NTLMv1                   | NTLM/Operational 8004; 4624 LmPackageName                                                                                                                                                                                                                                                                                                                                                   |
| Who can DCSync                                   | <code>(Get-Acl "AD:\DC=domain,DC=local").Access \   ? {(\$_.ObjectType -eq '1131f6ad-9c07-11d1-f79f-00c04fc2dcd2')}</code>                                                                                                                                                                                                                                                                  |
| Can a workstation reach a DC on admin ports      | <code>Test-NetConnection dc01 -Port 5985</code> from a workstation; must fail                                                                                                                                                                                                                                                                                                               |
| Does DNS leave another way                       | From a workstation, <code>nslookup example.com 8.8.8.8</code> ; must fail                                                                                                                                                                                                                                                                                                                   |
| Hyper-V DC export                                | Hyper-V-VMMS Admin log export and checkpoint events (confirm the IDs on a test export); file-integrity monitoring on the export path                                                                                                                                                                                                                                                        |

## C13 · Detect: alert rules

ThreatLocker Detect plus your SIEM. “Yes” means the event is never legitimate and gets an automated response.

| RULE                                                                                                                                                                        | NEVER LEGITIMATE? › ACTIVE RESPONSE |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------|
| DCSync (4662) from a non-DC                                                                                                                                                 | Yes › disable account, isolate host |
| Kerberoast (4769) for the decoy SPN                                                                                                                                         | Yes › disable account               |
| Any match on a Secured tripwire deny on a DC ( <code>ntdsutil</code> <code>wsmprovhost</code> <code>dnscmd</code> <code>esentutl</code> LSASS dumpers)                      | Yes › isolate host                  |
| Computer moved out of Secured mode; DC or Tier 0 policy edited                                                                                                              | Yes › page                          |
| Privileged-group add (4728/4732/4756) outside a change window; new account (4720)                                                                                           | Yes › page                          |
| New external forwarding rule; Vault export outside the records role                                                                                                         | Yes › suspend user                  |
| Logon type 3 to a DC from a workstation subnet by a non-computer, non-tier-0 account                                                                                        | Review                              |
| WinRM operational log on any DC or Tier 1 host                                                                                                                              | Review                              |
| Script-block 4104 outside admin hosts                                                                                                                                       | Review                              |
| Network Control denies from a process with no prior network history; one host hitting 3+ C2-related denies in 10 minutes                                                    | Review                              |
| Process launch from Downloads or Temp; any RMM binary; any interpreter on a server; first-ever elevation request                                                            | Review                              |
| New driver load on any host; retention change or job deletion in the backup products                                                                                        | Review                              |
| Server VLAN DNS query for any LLM-provider hostname                                                                                                                         | Review                              |
| DNS: TXT or NULL volume, labels over 50 characters, high entropy                                                                                                            | Review                              |
| Weekly directory diff: users, privileged groups, domain and OU ACEs, GPO links, trusts                                                                                      | Review                              |
| Scheduled task created or updated (4698/4702) outside admin hosts; the <code>schtasks</code> ringfence does not stop execution                                              | Review                              |
| Beacon periodicity (RITA / Zeek); JA4 fingerprints; TLS to a raw IP with no SNI; HTTP to a raw IP                                                                           | Review                              |
| Scripting user-agents ( <code>python-requests</code> <code>curl</code> <code>WindowsPowerShell</code> ); long-lived outbound TCP                                            | Review                              |
| NXDOMAIN bursts (DGA); BITS-Client 59/60 events with external URLs                                                                                                          | Review                              |
| 7045 new service with <code>cmd</code> or <code>powershell</code> in ImagePath; <code>System.Management.Automation.dll</code> loaded by a non-PowerShell process (Sysmon 7) | Review                              |
| Any hit on a Dynamic-DNS, OAST or external-IP-check domain from a non-browser process                                                                                       | Yes › isolate host                  |
| Workspace and Entra logs exported to the SIEM; 18 months or more of retention                                                                                               | —                                   |

---

## C14 · Deception

### ☐ Service account with an SPN nobody uses

ALERT ON

Any 4769 for it

### ☐ `creds.csv` in the script share with a SACL

ALERT ON

4663 read

### ☐ Canary document and API key (canarytokens.org)

ALERT ON

Any access

### ☐ Decoy computer object; honeypot host on the client VLAN answering 445/3389/5985

ALERT ON

Any connection

### ☐ Canary DC name in DNS; fake RMM shortcut; fake `ngrok.exe` permit request

ALERT ON

Any touch

**Gate:** every deny has been through Monitor first; every GPO has been through its audit event first; each alert rule has an owner and a documented response.