baanjai

ELEVATION, REIMAGINED

LEAD MAGNET · INTERNAL IT & MSP

The Endpoint Hardening Checklist

The eight endpoint controls that stop the ransomware chain — in priority order, with how to turn each one on.

A reference crib · what each control does, how to enable it, the common mistake

Information is free. Implementation is paid.
A field guide from the team behind Baanjai.

DM HARDEN on Instagram

How to use this. Ransomware rarely "breaks in" — it logs in, then turns off your defenses and deletes your recovery before you notice. This checklist covers the eight endpoint controls that stop that chain, in priority order. Each item: what it does, how to turn it on, and the mistake that quietly leaves it off. Work top to bottom — the first three block the most common attack path.

8 controls that stop the ransomware chain

In priority order. Each: what it does, how to enable it, and the common mistake.

1 Remove standing local admin

A non-admin user who gets phished can’t install malware, disable security tools, or wipe backups. This is the single highest-leverage control.

HOW TO ENABLE

Enforce via Group Policy Preferences (Local Users and Groups) or Intune; grant elevation just-in-time. See the Local-Admin Offboarding Playbook for the full method.

Common mistake: Leaving “temporary” admin grants in place — they never get removed and become the breach path.

2 Protect shadow copies & backups from tampering

Most ransomware deletes Volume Shadow Copies first so you can’t roll back. Locking recovery is what turns an incident into an inconvenience.

HOW TO ENABLE

Restrict who/what can delete shadow copies; keep at least one backup copy offline/immutable; alert on mass-deletion attempts.

Common mistake: Assuming cloud backup is enough while local recovery is deletable by any admin-level process.

3 Reduce the ransomware surface (Controlled Folder Access + ASR)

Stops untrusted processes writing to your documents and blocks the script/office/LOLBin techniques ransomware uses to detonate.

HOW TO ENABLE

Enable Microsoft Defender Controlled Folder Access and the Attack Surface Reduction (ASR) rule set — start in audit mode, then enforce.

> **Common mistake:** Skipping audit mode and enforcing blind, generating a flood of blocks, then turning it all off.

4 Harden against credential theft

Limits an attacker's ability to dump and reuse credentials to move laterally across the fleet.

HOW TO ENABLE

Turn on LSA Protection (RunAsPPL) and Credential Guard where supported; remove SMBv1; use Windows LAPS so every machine has a unique local-admin password.

> **Common mistake:** Reusing one local-admin password everywhere — one dumped hash unlocks the whole estate (pass-the-hash).

5 Add application control / allow-listing

Even with admin removed, allow-listing ensures only trusted code runs — the strongest backstop against unknown executables.

HOW TO ENABLE

Introduce execution control (e.g. WDAC) in audit-then-enforce mode; expand coverage in waves.

> **Common mistake:** Treating it as all-or-nothing and never starting; phased audit mode already lowers risk.

6 Keep patching verifiable, not aspirational

Unpatched criticals are the other common entry point. "Patched" has to be provable per machine.

HOW TO ENABLE

Run patch policies with severity rules, deferral, and reboot windows; report "last patched" per endpoint, not just a fleet percentage.

> **Common mistake:** Trusting a green compliance number while a handful of high-value machines quietly fall behind.

7 Shrink the remote attack surface

Fewer exposed doors means fewer ways in. RDP and legacy protocols are top targets.

HOW TO ENABLE

Disable unused services/legacy protocols; never expose RDP to the internet (gateway + MFA only); enforce MFA on all remote access.

> **Common mistake:** Leaving RDP open "temporarily" for a vendor and forgetting it.

8 Log and review privileged activity

If you can’t reconstruct who did what with elevated rights, you can’t investigate — or prove control to an insurer.

HOW TO ENABLE

Centralize elevation/admin logs off the endpoint; review periodically; keep an exportable trail.

> **Common mistake:** Local-only logs that the attacker you’re investigating can wipe or roll over.

How Baanjai changes this

MOST OF THIS CHECKLIST, FROM ONE CONSOLE

These controls usually mean stitching together GPOs, Defender policies, a LAPS rollout, a patch tool, and a logging pipeline. Baanjai delivers the core of them in one place — so hardening is a set of toggles you can prove, not a months-long integration project.

DOING IT BY HAND	WITH BAANJAI
Remove standing admin via GPO/Intune; grant break-glass manually.	Just-in-time, auto-expiring elevation — no standing local admin to manage.
Script shadow-copy and self-defense protections per machine.	Built-in hardening locks shadow copies, LSA, and the agent’s own self-defense.
Configure Controlled Folder Access + ASR by hand and chase audit noise.	Endpoint hardening controls applied and reported centrally, per scope.
Stand up WDAC tooling and manage policy drift.	Centrally managed application control (WDAC), audit-then-enforce.
Cross-reference patch, logs, and admin state across separate tools.	One pane: patch status, hardening state, and a full elevation audit trail together.

BOTTOM LINE

You don’t get hit because you’re a target — you get hit because your endpoints are soft and reachable. **Baanjai hardens them and proves it,** from one place.

What Baanjai is

Baanjai removes standing local admin and ransomware risk from one pane of glass: request-to-approve elevation tnat's scoped and auto-expiring, endpoint hardening (Controlled Folder Access, shadow-copy & LSA protection, application control), patch policies, and a live "who-has-what" view you can hand to an auditor. Everything in this playbook works by hand — Baanjai makes it a Tuesday.

Harden your fleet → baanjai.app/contact