baanjai

ELEVATION, REIMAGINED

LEAD MAGNET · INTERNAL IT & MSP

The Cyber-Insurance Answer Sheet

The questions insurers and auditors actually ask about privilege & endpoints — and how to answer "yes."

A reference crib · what they mean, how to implement, evidence to show

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

DM AUDIT on Instagram

How to use this. The renewal form has ~47 questions and most teams can confidently answer about 9. For the privilege-and-endpoint questions that actually move your premium (and your breach odds), here's what each one is really asking, how to implement it, the evidence to show, and the mistake that quietly fails you.

6 questions insurers & auditors actually ask

Each expanded: what they mean, how to implement, evidence to show, and the common mistake.

1 Do you enforce least privilege / no standing local admin?

WHAT THEY'RE REALLY ASKING

They want to know if a single phished user can install ransomware and disable defenses.

HOW TO IMPLEMENT

Remove standing local admin (see the Offboarding Playbook); grant elevation per-action, approved and auto-expiring.

EVIDENCE TO SHOW

A live list of administrators showing it's near-zero, plus the request/approval trail.

> **Common mistake:** Answering "yes" based on an AD group name without checking the actual local Administrators membership on machines.

2 Is privileged access time-bound and approved?

WHAT THEY'RE REALLY ASKING

Whether admin is a standing entitlement or a momentary, justified grant.

HOW TO IMPLEMENT

Use just-in-time elevation: requested, approved, scoped to the task, and expiring automatically.

EVIDENCE TO SHOW

Records showing elevations start and end, with the approver and reason on each.

> **Common mistake:** Permanent membership in an "admins" group counts as standing access, even if rarely used.

3 Are endpoints protected against backup / shadow-copy tampering?

WHAT THEY'RE REALLY ASKING

Whether malware can delete your recovery points before you notice (most ransomware does this first).

HOW TO IMPLEMENT

Lock Volume Shadow Copies and recovery from tampering; restrict who/what can run vssadmin-style deletes.

EVIDENCE TO SHOW

Configuration screenshot of the protection plus a test showing deletion is blocked.

> **Common mistake:** Assuming backups alone suffice — if shadow copies are deletable on the endpoint, local recovery is gone.

4 Do you have application control / allow-listing?

WHAT THEY'RE REALLY ASKING

Whether arbitrary executables (and living-off-the-land tools) can run unchecked.

HOW TO IMPLEMENT

Introduce execution control (e.g. WDAC/allow-listing), even phased in audit-then-enforce mode.

EVIDENCE TO SHOW

The policy and its scope; coverage percentage across the fleet.

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

5 Can you produce patch status on demand?

WHAT THEY'RE REALLY ASKING

Whether "patched" is verifiable per machine or just a green dashboard.

HOW TO IMPLEMENT

Maintain per-endpoint patch state with policies for severity, deferral, and reboot windows.

EVIDENCE TO SHOW

A current report with "last patched" per machine and outstanding criticals.

> **Common mistake:** Reporting compliance percentages while individual high-risk machines quietly fall behind.

6 Is admin access logged and reviewable?

WHAT THEY'RE REALLY ASKING

Whether you could reconstruct who did what with elevated rights after an incident.

HOW TO IMPLEMENT

Log every elevation/approval centrally and review periodically.

EVIDENCE TO SHOW

An exportable audit trail: who, what, when, approved by whom.

> **Common mistake:** Local-only logs that roll over or are wiped by the very attacker you'd be investigating.

How Baanjai changes this

TURN PARAGRAPHS INTO SCREENSHOTS

Most of these answers depend on the same foundation: least privilege, time-bound elevation, hardened endpoints, patch visibility, and an audit trail. Baanjai delivers all of them from one console — so the questionnaire stops being an essay and becomes a set of screenshots.

DOING IT BY HAND	WITH BAANJAI
Least privilege / no standing admin	Live who-has-admin view + just-in-time, auto-expiring elevation.
Time-bound, approved access	Every elevation requested, approved, scoped, and time-boxed by default.
Shadow-copy & recovery protection	Built-in hardening locks shadow copies, LSA, and self-defense against tampering.
Application control	Centrally managed allow-listing (WDAC), audit-then-enforce.
Patch status on demand	Per-endpoint patch policies and current status, reportable any time.
Logged & reviewable admin access	Full, exportable elevation/approval audit trail.

BOTTOM LINE

"We're basically compliant" is the most expensive sentence in IT. Baanjai turns most of this answer sheet into evidence you can paste straight into the form — and into a lower premium.

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.

Get audit-ready → baanjai.app/contact