

Endpoint Security Risk Assessment

ASSESSMENT

Delivered by Knovation Solutions

What it is: A non-intrusive evaluation of endpoint security posture across Windows, macOS, and Linux devices. Identifies active and latent malware, exploited and exploitable vulnerabilities, end-of-life software, and applications being used in ways that create risk. Runs in parallel with existing antivirus and EDR products. No requirement to remove or disable anything already in place.

When you use it: Where endpoint protection is deployed but what it is and is not seeing has never been independently verified. Antivirus and EDR report on what they block. This reports on what they never had visibility of.

Capabilities

Threat Hunting Assessment

- Detects malware, potentially unwanted programs, exploits and network attacks present on endpoints
- Surfaces latent threats that have not yet executed
- Identifies attack indicators that have not resulted in a blocked event

Vulnerability and Patch Exposure

- Separates vulnerabilities actively exploited in the wild from the general vulnerability backlog
- Reports critical and important vulnerabilities present across assessed endpoints
- Identifies end-of-life software still in daily use and no longer receiving vendor updates

Living-off-the-Land Detection

- Identifies legitimate system utilities and administrative tools executed in patterns associated with malicious activity
- Surfaces activity conventional antivirus does not flag, because the tools themselves are trusted

Zero-Trust Application Assessment

- Classifies every process executing on assessed endpoints
- Identifies unclassified or unexpected executables running in the environment

Endpoint Risk Status

- Risk profile across the full assessed device estate
- Per-device risk scoring, allowing prioritisation by exposure rather than by device count

Application and Bandwidth Visibility

- Inventory of applications actually executing, rather than what is believed to be installed
- Identifies applications generating unusually high download or upload volumes

Severity Classification

- Critical: confirmed malware executed, or exposure representing immediate risk of compromise
- High: latent malware capable of executing, or attack surface requiring urgent reduction
- Medium: additional risk factors to address preemptively rather than reactively

Prerequisites for POC

Required

- Administrative access to deploy the endpoint agent, either remotely or through existing deployment tooling
- Agreement on the device population to be assessed
- Confirmation that assessed endpoints are not already licensed for the same endpoint security platform, as the assessment is intended for environments protected by a third-party product

Optional (Extends Assessment)

- Coverage of higher-exposure devices such as laptops, which materially improves the value of the findings

Operating Conditions

- The assessment runs in audit mode throughout. It detects and records; it does not block, quarantine or remove
- Existing antivirus and EDR remain fully operational and continue to provide protection for the duration
- Transparent to end users. No local alerts or tray icons appear, and protection updates are suppressed so no device restarts are triggered
- The assessment can be deactivated at any point
- In scope: Windows, macOS and Linux. Android and iOS are assessed separately

Typical POC Timeline

- **Day 1:** Agent deployment to the agreed device population
- **Week 1-2:** Assessment window for estates up to 50 endpoints. Up to four weeks for larger estates, to allow sufficient behavioural data to accumulate
- **Following the window:** Report generation, findings review and prioritised remediation planning

Outcomes

You will have:

- A severity-ranked inventory of active and latent threats present on assessed endpoints
- Identification of vulnerabilities under active exploitation, separated from the general backlog
- A list of end-of-life software still running in the environment
- Visibility of living-off-the-land activity that signature-based tools do not flag
- An application inventory reflecting what is actually executing
- A prioritised remediation sequence, actionable with existing tooling
- An evidence base for endpoint security decisions, independent of vendor claims

Next step: Findings inform endpoint architecture decisions and feed into wider network and cloud security planning.

Closing

*We appreciate the opportunity to support your organisation in strengthening its endpoint security posture.
Please contact us at info@knovation.co.za with any questions regarding this assessment.*