Endpoint Security Checklist for IT Leaders

Questions that reveal how prepared your endpoint security program is.

Endpoint security isn't defined by technology alone.

The ability to see what's happening, understand what it means, and take appropriate action is just as important as the protection running on each device.

This checklist walks through each of those areas – from visibility and detection to response readiness and ongoing alignment with endpoint operations.

01 Endpoint Visibility

You cannot protect what you cannot see. Ask:

- [ ] Do you know which endpoints are connected to your business environment?
- [ ] Are remote, hybrid, and distributed devices included in your coverage?
- [ ] Are servers and virtual machines included where appropriate?
- [ ] Can you tell whether endpoint agents are active, current, and communicating?
- [ ] Do you have useful reporting on endpoint coverage and security activity?
- [ ] Can you identify unmanaged or unknown devices connected to your network?
- [ ] Can you validate endpoint inventory across offices, remote users, and distributed environments?

Why it matters:

Visibility gaps create blind spots. Attackers often look for unmanaged, under-protected, or poorly monitored devices as entry points. If you cannot confidently identify what is connected to your environment, Network Discovery may help uncover unmanaged devices and improve endpoint visibility.

02 Threat Detection

Modern threats do not always look like known malware. Ask:

- [ ] Can your tools detect suspicious behavior, not just known signatures?
- [ ] Can you identify patterns such as unusual process activity, privilege escalation, lateral movement, or file encryption behavior?
- [ ] Can related events be connected into a clear investigation path?
- [ ] Do alerts include enough context for your team to understand what happened?
- [ ] Are you able to prioritize alerts based on risk?
- [ ] Do your security and IT teams have a shared view of endpoint risk, not just endpoint alerts?

Why it matters:

Detection is most useful when it gives your team enough context to make decisions quickly. A long alert queue without clarity can slow response. If you need a clearer way to identify and prioritize endpoint exposures, Vulnerability Management may help you focus remediation efforts on the vulnerabilities that matter most.

03 Alert Ownership

Every alert needs an owner. Ask:

- [ ] Who reviews endpoint alerts during business hours?
- [ ] Who reviews alerts after hours, on weekends, or during holidays?
- [ ] What happens when the primary responder is unavailable?
- [ ] Are escalation paths documented and current?
- [ ] Do you know which alerts require immediate action?

Why it matters:

Many organizations have tools that generate alerts, but limited staff to investigate them. This creates delay, fatigue, and uncertainty when fast decisions are needed.

04 Response Readiness

Detection is only the first step. Ask:

- [ ] Do you have a documented response process for endpoint threats?
- [ ] Do you know when to isolate a device, quarantine a file, terminate a process, or escalate?
- [ ] Are approval requirements clear before an incident occurs?
- [ ] Do technical teams and business leaders understand their roles?
- [ ] Have you tested your response process recently?

Why it matters:

A response plan should not be created in the middle of an incident. Clear authority and documented workflows help reduce confusion when pressure is high.

05 Ransomware Readiness

Ransomware requires speed, coordination, and containment. Ask:

- [ ] Can you detect behavior associated with ransomware activity?
- [ ] Can you quickly identify affected endpoints?
- [ ] Can you contain a device before the issue spreads?
- [ ] Do you know who approves containment actions?
- [ ] Do you have a communication plan for IT, leadership, users, and outside support teams?

Why it matters:

Ransomware response depends on more than technology. It also depends on timing, decision-making, and coordination.

06 Internal Capacity

The right security model depends on the team behind it. Ask:

- [ ] Does your team have the time to review and investigate alerts?
- [ ] Do you have endpoint security coverage outside normal business hours?
- [ ] Are alerts being investigated consistently, or only when time allows?
- [ ] Do you have the internal expertise to investigate and respond to endpoint threats?
- [ ] Are you clear on what your team can realistically own – and where additional support may be beneficial?
- [ ] Who investigates endpoint alerts when your internal team is unavailable?

Why it matters:

Endpoint security is as much an operating model decision as it is a technology decision. If inventory gaps or vulnerability prioritization are difficult to manage internally, add-on capabilities such as Network Discovery or Vulnerability Management may help strengthen your endpoint security operating model.

07 Endpoint Operations & Security Alignment

Security works better when endpoint operations are healthy. Ask:

- [ ] Are endpoint management and endpoint security teams aligned?
- [ ] Are patching, device health, and security monitoring treated as connected priorities?
- [ ] Can you validate whether protected devices are also properly managed?
- [ ] Do operational issues create security blind spots?
- [ ] Are endpoint ownership and support responsibilities clear?
- [ ] Can you connect vulnerability findings to patching or remediation workflows?

Why it matters:

Endpoint management and endpoint security are different disciplines, but they influence each other. A device that is unmanaged, outdated, vulnerable, or poorly monitored is harder to protect. Network Discovery and Vulnerability Management can help you better understand where coverage gaps and exposure risks may exist.

Add-On Fit Check

Use these questions to identify whether additional endpoint visibility or risk management capabilities may be useful for your organization.

Network Discovery may be a fit if:

- [ ] You are unsure how many devices are connected to your network.
- [ ] You suspect unmanaged or unknown devices may exist in your environment.
- [ ] Your endpoint inventory is incomplete, manual, or difficult to validate.
- [ ] Remote, hybrid, or distributed work makes device visibility harder.
- [ ] You want to identify devices that may not yet be protected.

Vulnerability Management may be a fit if:

- [ ] You want visibility into vulnerabilities across your endpoint assets.
- [ ] You need help prioritizing which vulnerabilities to address first.
- [ ] Vulnerability reviews are inconsistent or handled manually.
- [ ] Cyber insurance, compliance, or customer requirements are increasing pressure to show stronger risk management.
- [ ] Your IT and security teams need a clearer view of endpoint exposure and remediation priorities.

Note:

Vulnerability Management includes Network Discovery, so consider whether you need discovery-only visibility or broader vulnerability prioritization.

Final Self-Assessment

You may need to revisit your endpoint security strategy if:

- [ ] Endpoint coverage is incomplete or difficult to verify
- [ ] Alerts are reviewed only during business hours
- [ ] Security investigations depend on whoever is available
- [ ] Ransomware response plans are unclear or untested
- [ ] IT teams are stretched thin and alert fatigue is increasing
- [ ] Endpoint management and endpoint security operate in silos
- [ ] Leadership expects faster response than your current model can support
- [ ] You cannot easily identify unmanaged devices connected to your environment
- [ ] You do not have a consistent process for prioritizing endpoint vulnerabilities

Key Takeaway

A stronger endpoint security program is not defined by tools alone. It depends on visibility, ownership, response readiness, and the ability to act when threats appear.

For IT leaders, the most important question goes beyond having endpoint protection. Instead, it's:

"Are we ready to detect, investigate, and respond before endpoint risk becomes business disruption?"

If this checklist highlighted areas where your organization could improve visibility, strengthen response processes, or better align security operations with available resources, it may be time to take a closer look at your endpoint security strategy.

Talk to a **TPx expert** to discuss your current endpoint security strategy and whether **Managed Endpoint Security** is a good fit for your organization.