Kaseya 365
Endpoint

10 cybersecurity moves to outsmart hackers

A checklist for IT teams

Hackers hunt for weak spots in your endpoints every day. But with the right steps, you can turn those weak spots into strong walls that keep them out. Now is your chance to outsmart attackers, cut stress and take back time to get the joy back in your day. This checklist walks you through ten smart moves to frustrate hackers and win back your calm.

1 Unify your security tools

Disconnected tools leave blind spots that attackers exploit. Unified management strengthens defenses by giving you full visibility and faster response.

- □ See patching, AV, backup and monitoring status in one place so no endpoint slips through unprotected
- □ Correlate endpoint data in a single dashboard to detect suspicious activity across the environment
- □ Generate integrated security reports that highlight vulnerabilities and compliance gaps before attackers find them

2 Automate patch management

Unpatched software is the easiest way in for attackers. Automating patching keeps every endpoint current and removes the risk of human error.

- □ Schedule operating system and application patches to run automatically
- □ Track patch compliance across all devices including remote ones
- □ Verify and report patch success so you know vulnerabilities are closed

3 Standardize device security

Inconsistent settings create weak points that attackers can exploit. Standardizing configurations ensures every endpoint follows the same security baseline and nothing slips through.

- □ Apply baseline security policies across every device
- □ Enforce passwords, firewalls and AV settings centrally
- □ Audit regularly for policy drift and fix gaps immediately

4 Monitor health and security together

Performance problems often hide security issues. Watching system health alongside security events helps you catch suspicious behavior earlier and prevent small issues from turning into major breaches.

- □ Track CPU, memory and unusual spikes in activity
- □ Flag abnormal login attempts and suspicious access
- □ Correlate performance alerts with potential threats

5 Keep antivirus effective

Antivirus is only as strong as its latest update. Outdated or unenforced AV leaves devices exposed to known threats that attackers rely on every day.

□ Ensure signatures update daily across all devices
□ Confirm every endpoint is reporting back to the console
□ Block devices without active protection from the network

6 Strengthen endpoint defenses

Modern threats are designed to slip past traditional AV. EDR adds behavioral detection and automated response so you can stop attacks that signatures alone would miss.

□ Deploy EDR to identify suspicious behavior not caught by AV
□ Isolate compromised devices automatically
□ Roll back malicious changes and restore endpoints fast

7 Back up to bounce back

Ransomware and data loss can hit at any time. Reliable backups mean you can recover quickly without paying attackers or losing critical information.

□ Track CPU, memory and unusual spikes in activity
□ Flag abnormal login attempts and suspicious access
□ Correlate performance alerts with potential threats

8 Act fast to reduce dwell time

The longer an attacker stays inside your network, the more damage they cause. Rapid detection and response reduce dwell time and limit impact.

- □ Investigate unusual endpoint activity immediately
- □ Quarantine compromised devices quickly
- □ Remediate automatically where possible to save time

9 Gain 24/7 visibility

Threats do not stick to office hours. Continuous monitoring ensures attacks are spotted and stopped even when your team is offline.

- □ Use SOC-backed monitoring that covers nights and weekends
- □ Have experts triage alerts before they reach your team
- □ Maintain visibility across on-prem and remote endpoints

10 Outsource the overload

Too many alerts create fatigue and mistakes. Outsourcing detection and response to experts filters the noise and ensures real threats get the right attention.

- □ Let SOC/MDR providers investigate and resolve routine incidents
- □ Escalate only high-risk threats to your internal team
- □ Free your staff to focus on strategic projects instead of firefighting

A checklist is only the starting point. To stay ahead of evolving threats, IT leaders need smarter, long-term endpoint protection strategies they can put into practice right away. The **IT director's guide to smarter endpoint security** walks you through these strategies in detail.

Get the guide

Kaseya®