5 Tips for Choosing a Next-Generation Endpoint Security Solution

Invest in a Next-Generation Endpoint Security Solution. Ask if it delivers...

1 Prevention: Block threats at the first sign of malicious behavior

Prevent breaches and block malware at point-of-entry in real time.

Prevention is your first line of defense. Make sure your Next-Gen Endpoint Security:

- Gets real-time feeds of the most up-to-date global threat intelligence to protect you against the newest, ever-evolving threats 24/7
- Saves you time by doing the heavy-lifting using multiple preventative and detection tools to stop ransomware, fileless malware, malicious cryptomining, and other threats before they make it onto your endpoints
- Analyzes the behavior of unknown or suspect files, to automatically quarantine newly discovered malicious files, without having to deploy a complex third-party sandbox
- Spots vulnerabilities and automatically identifies and quarantines suspicious executables before they become real problems

2 Detection: Proactively hunt for the riskiest 1% of threats

You don't need another solution that blocks 99% of threats.

Uncover the 1% of threats you've been missing. Your Next-Gen Endpoint Security must provide:

- Built-in threat hunting tools powered by global threat intelligence to identify new threats faster
- Continuous monitoring of all files on your endpoints that gives you back time away from doing mundane, manual monitoring tasks
- Ability to spot indications of compromise (IoCs) at the earliest stages of a threat
- Full history of file activity so you can scope a compromise from start to finish
- Retrospective security against previously benign files that start becoming malicious

Additional Resources

Demand more from your endpoint security. Explore Cisco AMP For Endpoints.

Cisco AMP For Endpoints Overview

Cisco AMP For Endpoints Demo

Customer Testimonial: Istanbul Grand Airport

Interact with AMP

For more on Endpoint Security click here.

3 Detection at Speed: Dramatically shrink Time to Detection

Spot threats in hours or minutes, not days, weeks, or months.

The industry average to detect a breach after it occurs is about 200 days. Your Next-Gen Endpoint Security solution should be detecting them in minutes or hours by:

- Continuously watching file activity and communications across PCs, Macs, Linux, servers, and mobile devices (Android and iOS) to quickly detect stealthy malware
- Correlating data with the most up-to-date behavioral indicators, telemetry data, and other global threat intelligence so you don't have to spend copious amounts of time doing the research
- Prioritizing threat alerts so you are always resolving the riskiest threats first

4 Response: Take back control of your time using simple, automated incident response tools

Investigating an incident can take long hours costing precious time away from your family.

Response should be comprehensive and fast. Your Next-Gen Endpoint Security solution should let you:

- Accelerate investigations and reduce management complexity by easily searching across all endpoints and malware artifacts
- Easily connect the dots on a malware compromise, marrying external threat intelligence with internal log data across your environment to simplify investigations, and shorten incident triage and mitigation time
- Systemically respond to and remediate malware across all endpoints automatically or with just a few clicks

5 Integrated Threat Defense: See the threat once, block it everywhere else

No more siloed products. Get systemic prevention, detection, and response.

Juggling a bunch of siloed point products and working with multiple consoles will slow you down. Your Next-Gen Endpoint Security solution, should play an essential role in a larger, integrated threat defense architecture that improves your security posture and operational efficiency. You need:

- An integrated architecture of security technologies that can work together to close security gaps and detect threats faster across your entire security ecosystem
- Cloud-based technology that provides protection everywhere, from endpoint to network, email, and web
- Threat intelligence and event data shared and correlated across all security tools, and communicated to the security team so they can proactively defend against advanced threats across all possible vectors