CISCO
SECURE

White Paper
Cisco Public

5 Tips for Transforming your Endpoint Security

Investing in Endpoint Security? Ask if it delivers...

Digital transformation, the move to the cloud, and a rapidly expanding attack surface are driving the need for a new class of endpoint security, capable of defending organizations against a more diverse and sophisticated threat landscape. Is your endpoint security ready?

1 Prevention: Stop threats before they compromise you.

Prevent breaches and stop threats at point-of-entry in real time.

Prevention is your first line of defense. Make sure your 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 providing multifaceted prevention that combine behavioral analytics, machine learning and signatures 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 isolate compromised endpoints or 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: Continually employ cross-control detection of advanced threats.

Detect and hunt for threats on the endpoint and beyond.

Reduce the attack surface fast. Your endpoint security must provide:

- Extensive EDR capabilities to continually detect threats using advanced and cross-control detection and threat hunting capabilities
- Continuous monitoring of all files on your endpoints that eliminates time spent on mundane, manual and repetitive tasks
- Ability to spot indications of compromise (IoCs) at the earliest stages of a threat

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 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: Simplify your security with an open, integrated platform using automated incident response tools.

Remediate faster and completely with automated playbooks and advanced search.

Response should be comprehensive and fast. Your endpoint security solution should let you:

- Accelerate threat response using automated playbooks, hundreds of preloaded queries, and human-driven hunts for advanced threats
- Easily connect the dots on a malware compromise, combining external threat intelligence across multiple control points in your environment to simplify investigations, and shorten incident triage and remediation time
- Systemically respond to and remediate threats across all endpoints with automated playbooks or with a few clicks

Additional Resources

Demand more from your endpoint security. Explore Cisco Secure Endpoint.

- Cisco AMP for Endpoints At-a-Glance
- Cisco AMP for Endpoints Overview
- Customer Testimonial: Istanbul Grand Airport
- Interact with AMP
- Cisco SecureX Overview

5 Built-in Threat Defense: Unlock your full potential with SecureX.

No more siloed products. Simplify security, get visibility, and improve operational efficiency.

Juggling a bunch of siloed point products and working with multiple consoles will slow you down. Your endpoint security solution should play an essential role in a larger, integrated security platform that simplifies security, improves your visibility to threats and maximizes operational efficiency. You need a built-in platform of security technologies that:

- Integrates technologies together with true turnkey interoperability
- Accelerates time to detect and investigate threats while maintaining contextual awareness
- Accelerates time to remediate and automates workflows to lower costs and strengthen your security

For more on AMP for Endpoints:

click here