Cisco AMP for Endpoints

Uncover the 1% of threats you've been missing

Nearly all endpoint security solutions on the market claim to block 99 percent of malware. But what about the 1 percent of threats they miss? The threats in that 1 percent will wreak havoc on your network. If you rely solely on traditional point-in-time technologies, such as antivirus, those threats can go undetected for months.

Protecting users is more important than ever

Organizations are embracing more mobile, flexible workforces. Employees are enabled to be productive on and off the corporate network using a variety of devices, ranging from laptops to tablets to phones. Networks are now architected to allow remote access to even the most sensitive data.

Unfortunately, attackers are catching on to these trends. They're targeting your employees and the gold mine of data on their devices with threats designed specifically to get around traditional endpoint security tools. So how can your business continue to innovate, embrace a digital transformation, and mobilize your workforce without sacrificing security?

Next-generation endpoint security

Next-generation endpoint security is the integration of prevention, detection, and response capabilities in a single solution, leveraging the power of cloud-based analytics. Cisco® AMP for Endpoints is a lightweight connector that works on your Windows, Mac, Linux, Android, and iOS devices. It can use the public cloud or be deployed as a private cloud. AMP continuously monitors and analyzes all file and process activity within your network to uncover the 1 percent of threats that other solutions miss. AMP never loses sight of where a file goes or what it does. If a file that appeared clean upon initial inspection ever exhibits malicious behavior, AMP is there with a full history of the threat's behavior to catch, contain, and remediate.

Benefits

Cisco® AMP for Endpoints provides comprehensive protection against the most advanced attacks. It prevents breaches and blocks malware at the point of entry, then rapidly detects, contains, and remediates advanced threats that evade front-line defenses and get inside your network.

- **Prevent:** Strengthen defenses using the best global threat intelligence, and block both fileless and file-based malware in real time.
- **Detect:** Continuously monitor and record all file activity to quickly detect stealthy malware.
- **Respond:** Accelerate investigations and automatically remediate malware across PCs, Macs, Linux, servers, and mobile devices (Android and iOS).

Next steps

Talk to a Cisco sales representative or channel partner about how Cisco AMP for Endpoints can help you defend your organization from advanced cyberattacks. Visit our website to learn more.

C45-731874-12 04/18

Stop malware

AMP for Endpoints takes a cloud-based approach to threat intelligence and file analysis. The AMP cloud is constantly fed information from Cisco Talos and Cisco Threat Grid, which represent the industry's largest collection of real-time threat intelligence feeds. This cloud-based approach allows AMP to analyze files against the most up-to-date threat intelligence to protect you against today's ever-evolving malware.

Because there is no single answer to stopping malware, AMP comes with more than 15 built-in protection and detection mechanisms to prevent threats from compromising your business. These include malicious activity protection to stop ransomware, fileless-malware exploit prevention, machine-learning analysis of new threats, sandboxing, and more. If a file appears clean enough to pass all mechanisms, AMP lets it in, then continuously monitors and analyzes it for malicious behavior.

Eliminate blind spots

Cisco AMP for Endpoints provides a holistic view of your endpoints, regardless of operating system. AMP also provides visibility into anomalous traffic on connected Internet of Things (IoT) devices where a connector can't be deployed, including printers, thermostats, and security cameras.

Cisco knows that cybercriminals rarely limit themselves to one attack vector. AMP for Endpoints shares threat intelligence across your entire environment, unifying security across endpoints, network, email, the cloud, and the web. Through these integrations, AMP can see a threat in one area of your environment, then automatically block it everywhere else it appears. AMP automatically correlates files, telemetry data, behavior, and activity to proactively defend against advanced threats across all possible vectors.

Discover unknown threats

AMP's built-in sandboxing technology analyzes the behavior of suspicious files and correlates it against other information sources. File analysis produces detailed information to give you a better understanding of how to contain the outbreak and block future attacks.

When a file is deemed malicious, AMP drastically reduces the amount of time and resources required to investigate. It automatically provides insight into your most pressing questions, including:

- What happened?
- Where did the malware come from?
- Where has the malware been?
- What is the malware doing now?
- How do we stop it?

With a few clicks in AMP's browser-based management console, the file can be blocked from running on all endpoints. Cisco AMP knows every other endpoint the file has reached, so it can quarantine the file for all users. With AMP, malware remediation is surgical, with no associated collateral damage to IT systems or the business.