Cisco AMP for Endpoints

Uncover the riskiest 1% of threats you've been missing. In hours. Not days or months.

Nearly all endpoint security solutions claim to block 99% of malware. But what about the 1% of threats they miss? The most dangerous 1% of threats 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 200 days on average. For months on end, they can be creeping in and moving laterally across your network causing damage through stealthy malware campaigns without you even knowing it–until it's too late.

Protecting users at speed with maximum precision

Modern malware has evolved, making it harder and longer to identify and contain. Cybersecurity teams are struggling with an overwhelming volume of alerts. They spend copious amounts of time preventing, detecting, and responding to threats, while still relying on manual processes and using a plethora of poorly integrated tools. Protecting users is more important than ever, but does it have to come at the expense of unreasonable threat "volume fatigue" or precious time away from your family? Defending users from today's advanced threats calls for a next-generation endpoint security solution that delivers precision, speed, and efficiency.

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 global threat intelligence and cloud-based analytics. Cisco® Advanced Malware Protection (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 find and automatically eliminate the riskiest 1% 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 becomes a problem, AMP is there with a full history of the threat's activity to catch, contain, and remediate at the first sign of malicious behavior.

Benefits

Cisco AMP for Endpoints provides maximum protection against the most advanced attacks fast, so you can take back control of your time for innovation. It prevents breaches and blocks malware at the point of entry, then rapidly detects, contains, and remediates advanced threats that evade front-line defenses.

- **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 cyber attacks. Visit our website to learn more.

C45-731874-13 01/19

Stop malware

AMP for Endpoints takes a cloud-based approach to threat intelligence and file analysis. The AMP cloud is constantly fed with information from Talos™ and Cisco Threat Grid. Access to the industry's largest collection of real-time global threat intelligence feeds dramatically shrinks your own threat research times. 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.

Doing the heavy lifting for you, 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, to proactively defend against advanced threats across all possible vectors.

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, networks, email, the cloud, and the web. Through these integrations, AMP can see a threat in one area of your environment and then automatically block it everywhere else it appears. AMP automatically correlates files, telemetry data, behavior, and activity to simplify investigations and shorten incident triage and mitigation time.

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. AMP also eliminates the guesswork, allowing security personnel to take back control of their time by protecting your endpoints against the most challenging threats with less time, effort, and cost to do so.

When a file is deemed malicious, AMP drastically reduces the amount of time and resources required to investigate. It automatically provides insight into what happened, how the malware got in, where has it been, what it is doing now, and how to stop it.

With a few clicks in AMP's browser-based management console, the file can be blocked from running on all endpoints. 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.