Cisco AMP for Endpoints

Relentless Breach Defense

Dealing with a data breach can put many strains on your security team – even more so when you are already reeling from a talent shortage. Faced with an incident, they now have to spend copious amount of time detecting, containing and remediating the problem. As malware becomes more evasive, traditional antivirus falls short in protecting your endpoints. One thing is clear, defending against breaches today requires modern defenses and technology that simplifies your security operations.

Endpoint Protection Platform + Endpoint Detection and Response

Endpoint Protection Platform (EPP) delivers next generation antivirus that stops today's complex attacks. Endpoint Detection and Response (EDR) offers more advanced capabilities like detecting and investigating security incidents, and the ability to remediate endpoints quickly. We bring EPP and EDR capabilities together for a unified and more complete solution, called Cisco® Advanced Malware Protection (AMP) for Endpoints.

AMP for Endpoints leverages multiple protection engines fueled by Cisco Talos threat intelligence to block threats before they target you. New EDR capabilities make threat hunting easy. AMP for Endpoints integrates seamlessly with other security technologies so you can respond to threats completely with security that works together.

Benefits

Replace your legacy antivirus completely. **Cisco AMP for Endpoints offers cloud-delivered Endpoint Protection and advanced Endpoint Detection and Response.** We stop breaches and block malware, then rapidly detect, contain, and remediate advanced threats that evade front-line defenses.

- **Prevent:** Block known malware automatically leveraging the best global threat intelligence, and enforce Zero Trust by blocking risky endpoints from gaining access to applications.
- **Detect:** Run complex queries and advanced investigations across all endpoints, and continuously monitor all file activity to detect stealthy malware.
- **Respond:** Rapidly contain the attack by isolating an infected endpoint and remediating malware across PCs, Macs, Linux, servers, and mobile devices (Android and iOS).

© 2020 Cisco and/or its affiliates. All rights reserved.

New Packages

AMP for Endpoints Essentials

- Next Gen Antivirus Protection
- Continuous Behavioral Monitoring
- Dynamic File Analysis
- Vulnerability Identification
- Endpoint Isolation

AMP for Endpoints Advantage

- Advanced Endpoint Detection and Response
- Full Subscription to Threat Grid Cloud

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.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

Block threats. Before they target you.

Endpoint protection is only as good as the intelligence it acts on. That's why we employ machine learning and multiple protection engines fueled by Cisco Talos, the largest non-governmental threat intelligence organization on the planet. We discover more vulnerabilities than other vendors and push out protection before the bad guys can exploit them, giving you an advantage. And because we're Cisco, Talos sees more network traffic than any other vendor. Whether a threat originates on the Internet, in an email, or on someone else's network, our cloud-based global telemetry sees a threat once, anywhere in the world, and blocks it everywhere, across AMP for Endpoints and our entire security platform.

Know everything. About every endpoint.

We simplify threat hunting by automating advanced investigative queries across any or all of your endpoints. Whether you are doing an investigation as part of incident response, threat hunting, IT operations, or vulnerability and compliance, we get you the answers you need. We have preloaded scripts so you can leverage the expertise of our Talos threat hunters or even customize your own. We provide deeper visibility on what happened to any endpoint at any given time by taking a snapshot of its current state. We continuously monitor and analyze the behavior of your endpoints, giving you everything you need to investigate and respond to the riskiest threats quickly and confidently.

If a file that appeared clean upon initial inspection ever becomes a problem, we can provide a full history of the threat's activity to catch, isolate, contain, and remediate at the first sign of malicious behavior.

Respond completely. With security that works together.

Threats are not one dimensional and neither should your defenses be. That's why we built AMP for Endpoints with out-of-the-box integrations with the rest of the Cisco security platform to block, detect, investigate and respond to threats across your entire environment – not just your endpoints. With security that works together, we help you streamline your security operations, making security investigations faster and easier. You will get to the root cause fast, and automate actions to stop a threat in its tracks. We empower you to respond to attacks at the first sign of malicious behavior using one-click isolation of any endpoint, everywhere. Importantly, we have broader control beyond just the endpoint. We instrument our endpoint security to leverage threat intelligence from web, email, cloud and network security solutions; and multi-factor authentication integration for Zero-Trust, creating security defenses that work together for more effective protection and response against the most challenging threats with less time, effort, and cost to do so.