White paper
Cisco public

Endpoints Security

AMP for Endpoints with Umbrella

AMP and Umbrella work in harmony to provide visibility, context and control to prevent, detect and respond to attacks targeting endpoints before damages can be caused.

© 2017 Cisco and/or its affiliates. All rights reserved.

"Cisco Advanced Malware Protection, in combination with Cisco Umbrella, has decreased the number of ransomware outbreaks to zero during the last 8 months."

Freek Bosscha, architect, NHL

"We have much greater confidence in the security of our endpoints with Cisco Umbrella combined with Cisco AMP. We have had zero malware infections since our implementation 3 years ago."

Financial services

70% Of breaches start on endpoints devices

Why?

1) Gaps in protection 2) user error 3) Gaps in visibility

Which solution?

 AMP for Endpoints is a cloud-managed, next generation endpoint security solution that rapidly detects, contains, and remediates malicious files if they evade front line defenses and infiltrate your endpoints using traditional antivirus inspection engine, machine learning, sandboxing, vulnerability monitoring, continuous analysis of file behavior, and retrospective detection.

 Umbrella is a cloud security platform that provides the first line of defense against threats hosted on the internet, whether users are on or off the corporate network. Umbrella delivers complete visibility into internet activity across all locations and endpoints, and through the use of models, can proactively block malicious requests before a connection is even established.

Prevent
Umbrella blocks malicious web requests.
AMP for Endpoints blocks malicious files and send the unknown elements to sandbox for deeper control.

Detect
Umbrella sees and stops C&C callbacks to attackers servers.
AMP for Endpoints continuously and retrospectively files activities to identify unusual behaviors.

Remediate
Umbrella Investigate provides actual and historical data on domains, IPs and compromised hashes.
AMP for Endpoints gives past attacks history while allowing control and immediate quarantine.

For more information visit www.cisco.com/go/breach

© 2017 Cisco and/or its affiliates. All rights reserved.