Cisco IT Brief

Advanced Malware Protection for Everywhere

Malware is getting nastier. Signature-based threats are giving way to more complex, behavior-based breaches. Hackers are creating advanced malware that can evade the best intrusion prevention systems, antivirus solutions, and other point-in-time detection tools. IT needs to have greater visibility into the scope of potential breaches, and the ability to detect, contain, and remediate advanced malware before it can cause damage or disrupt business. Enter Cisco's Advanced Malware Protection (AMP).

Fueled by top-notch global threat intelligence, AMP strengthens existing lines of defense before an attack and blocks malware trying to infiltrate the extended network during an attack. If malware gets through these defenses, AMP supplies all the information IT needs to uncover and remediate the problem quickly and cost effectively. The AMP browser-based management console gives us complete visibility into the users, applications, and devices affected, where the malware originated, what the malware is doing, and how to stop it. Cisco® AMP provides protection in the network, data center, endpoints, servers, mobile devices, email and web gateways, and virtual environments.

We're deploying AMP throughout the Cisco extended network. As of January 2016, we had:

- AMP for Networks operational at all 13 Cisco Internet Points of Presence (PoP).
- AMP for Endpoints in production for Android and in pilot for Windows and MAC OSX.
- AMP integrated in our Web and Email Security Appliances.
- AMP Threat Grid integrated into Cisco gear spanning the network. A dynamic behavior analysis and sandboxing technology, Threat Grid complements the AMP products.

> *"We've seen AMP for Endpoints catch new malware that our antivirus solution couldn't detect, and allowed into our network."*
> *–Rich West, Information Security Architect*

"AMP fetches the rare, suspicious code and then automatically hands it over to Threat Grid to be analyzed," says Rich West, Information Security (InfoSec) Architect. "Threat Grid determines if it is likely to be malware or not, and if it is, flags it to the attention of the human investigators. All of this is automated." Threat Grid analyzes the activity of every suspicious sample and artifact it receives based on more than 450 (and growing) behavioral indicators.

Stepping Up Email Malware Detection

AMP is helping us in the war against email-based malware proliferation. "Our deployment of Cisco's Email Security Appliance [ESA] blocks 80 to 90 percent of malware threats sourced through email," says Scott Heider, IT program manager, Cisco InfoSec. "With AMP integrated into our ESA solution, the ability to hunt for that needle-in-the-haystack, unknown threat is now possible without adding extra hardware or support expertise."

For More Information

Inside Cisco IT Blog: AMP Threat Grid
Cisco Advanced Malware Protection Solution