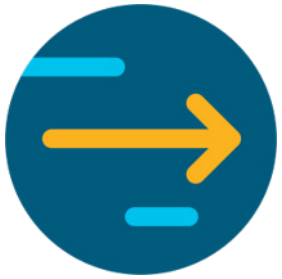

Cisco AMP for Endpoints Deployment Services

Protecting against Malware to the Ends of Your Network

Even if you have the best of guards at your doors, you still want protectors inside. That's what Cisco® Advanced Malware Protection (AMP) for Endpoints gives you. Intrusion prevention catches malefactors when they try to enter your network, but it's a one-shot assessment of incoming communications. Once something's in, intrusion prevention doesn't see it again. What happens if once something has passed through the gates, it's found to be malware?

AMP offers the only advanced malware protection system that covers endpoints before, during, and after an attack with continuous data gathering and advanced analytics. By using this information with Cisco retrospective security tools such as retrospection, attack chain correlation, behavioral indications of compromise, trajectory, and breach hunting, security managers can turn back time on threats. You can trace processes, file activities, and communications to understand the full extent of an infection, establish the root cause, and perform remediation.

Cisco's Advanced Malware Protection (AMP) for Endpoints Deployment services help you install this protection smoothly. We deploy, configure, test, and initially tune the implementation across up to six (6) endpoint groups within 45 days. Using Cisco best-practices, we help you avoid mistakes that can slow down deployment, increase costs, and possibly leave your network unprotected.

Benefits

- Achieve visibility and control across your environment through detailed, actionable reporting and analytics
- Create actionable intelligence for your security analysts, including Retrospective Security
- Integrate Advanced Malware Protection for Endpoints with your existing security processes
- Ensure your staff has the skills to operate the solution, via knowledge transfer throughout the engagement
- Build tailored protection profiles for different departments
- Meet internal and external audit requirements for the implementation by taking advantage of vendor best practices

Case Study

Real Estate

Challenges

- Lack of operational security methodology (vulnerability management, patching, upgrades)
- Lacking centralized incident management and individuals to tune appliances
- Attackers leveraging phishing e-mails and drive-by attacks, locking random computers and over TB of data

Solution

- Assisted client's security team to investigate root causes for infection
- Deployed Cisco AMP for endpoints to facilitate end-point protection, analysis, and remediation.
- Reconfigured Cisco ESA, CWS, and McAfee EPO

Outcome

- Cisco provided SME's to assist in broader response efforts.
- Utilized proven methodologies and techniques to stay ahead of the attackers, allowing for 90% reduction in compromise and data loss from continued attacks.
- Cisco's comprehensive intelligence alongside FireAMPtechnology enabled prevention and detection of unknown customer threats and enhanced visibility

Getting the Protection Up and Running Quickly

Planning and implementing of your deployment is quick, but it's thorough. These are the steps we take before, during, and after deployment.

Pre-Deployment

To begin, we work with you to perform many planning activities. These can include reviewing the project plan, Bill of Materials (BoM), network topologies, asset classification, and any other relevant documentation. We also gather information via the Deployment Profile Questionnaire.

Deployment

In this phase, we work with you to define AMP policies and the endpoints for an initial deployment. Then we perform the initial deployment in a limited production environment.

Post-Deployment

Here, we validate the limited production deployment, and provide additional tuning support approximately 30 days after deployment. We also deliver knowledge transfer, and give you a report that summarizes the deployment within your environment

Cisco's AMP for Endpoints Deployment is sold in two sizes: for deployments of up to 5000 devices or up to 25,000 devices, with the opportunity for custom scoping to fit your specific needs.

Next Steps

Visit www.cisco.com/go/securityservices to connect with our advisors and protect your business today.

JUNE 2018