At-a-Glance

Cisco's AMP for Endpoints Deployment

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

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.

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

- Conduct a remote kick-off call and project plan review, identify key stakeholders, and provide a Project Management Plan including a time-line and schedule of activities
- Make recommendations for deployment and configuration based upon network topology review, asset classification, current technology configuration, and defensive posture

- Review Customer's information security, information technology, change-control policies, and Bill of Materials
- Review best practices for deployment, strategy, design, and configuration

Deployment

- Define AMP for Endpoints policies
- Identify initial alpha deployment endpoints
- Deploy, configure, and initially tune and validate an alpha implementation of AMP for Endpoints with a pre-defined limited number of endpoint connectors
- Identify prioritized endpoints for a limited production deployment
- Perform one connector package push for up to six endpoint groups

Post-Deployment

- Validate the performance of the limited production deployment and provide a remote supplemental optimization tune approximately 30 days post deployment
- Provide knowledge transfer on the use of AMP for Endpoints analytics components
- Provide and review a Deployment Summary Report (DSR) summarizing the AMP for Endpoints deployment

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

For more information, visit www.cisco.com/go/services/security.

C45-734143-00 09/16