At-a-Glance

Benefits

- Achieve visibility and control across your environment through detailed, actionable reporting
- Create actionable intelligence for your security analysts
- 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
- Quantify results to management with post-deployment reporting
- Build tailored protection profiles for different departments
- Meet internal and external audit requirements for the implementation by taking advantage of vendor best practices

Cisco Security Deployment Service for AMP for Endpoints

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 (FireAMP) 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 (IOCs), trajectory, and breach hunting, security managers can turn back time on threats. They can trace processes, file activities, and communications to understand the full extent of an infection, establish the root cause, and perform remediation.

Cisco's Deployment Services for Advanced Malware Protection (AMP) for Endpoints help you install this protection smoothly. We deploy, configure, test, and tune the implementation across an initial 500 endpoints in 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

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

Predeployment

- Conduct remote kick-off call to review project plan and identify key stakeholders
- Perform a gap assessment to best practices document for pre-deployment and configuration
- Create a Deployment Profile Report outlining the configuration of your specific deployment
- Test AMP on your gold images for different operating systems

Deployment

- Deploy, configure, test, and tune the implementation of AMP
- Create a prioritized deployment roadmap of applicable endpoints and push the developed package to one business unit for up to 500 endpoints
- Validate the performance and success of the distribution
- Update the Deployment Profile Report with installation and initial tuning results

Postdeployment

- Perform a remote supplemental optimization tuning within 30 days after deployment to improve the AMP solution to address any performance and security objectives
- Update the Deployment Profile Report again, with results from the secondary tune

Cisco Security Deployment Service for AMP for Endpoints is sold in two sizes: for deployments of up to 5000 devices or up to 25,000 devices.

Next Steps

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