FIREEYE | MANDIANT

DEPLOYMENT & INTEGRATION SERVICES DATA SHEET

Endpoint Security

BENEFITS

- **Efficient deployment** by FireEye experts using best-practice configurations
- **Workflow processes** that enable rapid identification, triage and containment of endpoint threats
- **Effective analysis** facilitated by hands-on knowledge transfer on use of FireEye Endpoint Security and supplemental tools
- **Operational readiness** that includes integration with existing technologies, such as FireEye solutions and SIEM and SOAR systems

Overview

FireEye Deployment and Integration Services for Endpoint Security help plan and implement a complete endpoint security solution and integrate that solution into your security response processes. Our deployment engineers use in-depth knowledge of the FireEye Endpoint Security product to ensure an efficient and successful deployment. We offer several services to help you maximize the value of your FireEye Endpoint Security solution:

- Deployment Jumpstart Services
- Endpoint Security Agent Migration
- Endpoint Security Health Check and Tuning
- Supplemental IOC Tuning and Implementation

Deployment Jumpstart Services

Jumpstart Services for FireEye Endpoint Security are designed to help you deploy and configure your Endpoint Security solution quickly and effectively. Whether you are deploying in a small homogenous environment or a large, complex network, Jumpstart Services help you architect and implement the right endpoint security solution to meet your security goals.

Endpoint Security Deployment Jumpstart Services include:

- Configuration and setup of the Endpoint Security controller and agent package based on FireEye best practices
- Deconfliction with other endpoint tools via exclusions and allow lists
- Endpoint Security agent deployment and testing
- Host set creation and review of recommended best practices for static and dynamic host sets
- Policy creation and application to host sets
- Configuration and implementation of add-on modules from FireEye Market to enhance Endpoint Security
- Integration of FireEye Endpoint Security with other FireEye security tools in your environment
- Review of recommended management and maintenance practices
- Review of FireEye Endpoint Security usage for analysts, including common use cases and recommended approaches for alert review and analysis, threat investigation and host containment
- Introduction to FireEye customer resources such as the FireEye Customer Support Portal and Community and FireEye Market

Endpoint Security Agent Migration
Whether you are upgrading hardware, changing from an on-premise controller to a cloud controller, or making architecture changes in your environment, you may need to implement a new FireEye Endpoint Security controller and migrate Endpoint Security agents from one controller to another. Experienced FireEye professionals can help make this a seamless transition by determining an appropriate architecture for the new solution, developing a migration plan, and conducting the migration to avoid security coverage gaps and business disruptions.

The Endpoint Security Agent Migration service includes:

- Endpoint Security architecture review and planning
- Review of agent migration options and considerations
- Determination and implementation of agent migration plan and strategy
- Migration of custom IOCs, as applicable
- Review and migration or reconfiguration of host sets and associated policies
- Public key infrastructure (PKI) certificate backup and restore
- Integration of FireEye Endpoint Security with other FireEye security tools in your environment
- Review of recommended management and maintenance practices

Endpoint Security Health Check and Tuning
With the rapid changes that occur in most corporate networks along with the fast pace of development within the FireEye Endpoint Security solution, it can be challenging to ensure your security solutions maintain the level of visibility and protection you expect. To get the most coverage and value from FireEye Endpoint Security, the Health Check and Tuning service reviews the operation and configuration of your FireEye Endpoint Security deployment and adjusts configurations and policies as needed to align with recommended best practices. Our experts update your team on new features in the product and available innovation architecture modules that extend the product's capabilities.

The Endpoint Security Health Check and Tuning service includes:

- Comprehensive assessment of system health and performance
- Review of configuration settings as compared to recommended best practices
- Explanation and enablement of new features, capabilities, and modules
- Assessment of endpoint coverage
- Additional agent deployment and configuration, if applicable
- Agent testing and policy tuning
- Review of recommended management and maintenance practices
- Review of FireEye Endpoint Security usage for analysts

Supplemental IOC Tuning and Implementation
The Indicator of Compromise (IOC) Tuning and Implementation service implements supplemental IOCs and teaches your team to identify additional useful IOCs, tune them for your environment and enable them in FireEye Endpoint Security. To accomplish this, FireEye experts work with you to install the supplemental pack of IOCs from the FireEye Market on your Endpoint Security controller and adjust selected IOCs to meet your security requirements. Our professionals demonstrate the process, explain considerations for tuning and show you how to adjust and implement IOCs so you can tune and enable other IOCs from the supplemental pack as needed.

The Supplemental IOC Tuning and Implementation service includes:

- Download and installation of the supplemental pack of IOCs from FireEye Market
- Prioritization of IOCs for implementation on your Endpoint Security solution
- Demonstration of the process and explanation of tuning considerations
- Tuning and implementation of an agreed-upon selection of IOCs
- Knowledge transfer on the process of tuning and implementing IOCs
- Follow-up session to review progress on implementing additional IOCs, provide further guidance and address any outstanding questions

Table 1. Endpoint Security Services Comparison.*

	Basic Jumpstart	Advanced Jumpstart	Agent Migration	Health Check and Tuning	IOC Tuning and Implementation
Endpoint Security architecture review	✓	✓	✓	✓	
Best practices configuration implementation	✓	✓	✓	Tuning	
Agent deployment on pilot hosts	✓	✓			
Agent testing process on pilot hosts		✓			
Host set creation and policy configuration		✓		Tuning	
Integration with other FireEye security tools		✓	✓	✓	
Onboarding with Mandiant Managed Defense	✓	✓	✓	Review	
Configuration of innovation arch. modules		Limited		✓	
Review of management best practices	✓	✓	✓	✓	✓
Analyst knowledge transfer (IOCs, alert review)	Limited	✓	✓	✓	✓
Assessment of system health and performance	✓	✓	✓	✓	✓
Documentation of installed solution	✓	✓	✓	✓	
Development of agent migration plan			✓		
Agent, IOC, host set, and policy migration			✓		
Assessment of endpoint coverage			✓	✓	
Guidance on API and custom integrations		✓		✓	✓
Supplemental IOC tuning and implementation					✓
Knowledge transfer on IOC tuning					✓

*Required quantity of services SKUs depends on size and complexity of the FireEye Endpoint Security deployment.

To learn more about FireEye, visit: **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About FireEye, Inc.
At FireEye, our mission is to relentlessly protect organizations with innovative technology, intelligence and expertise gained on the frontlines of cyber attacks. Learn how at www.FireEye.com.

About Mandiant Solutions
Mandiant Solutions brings together the world's leading threat intelligence and frontline expertise with continuous security validation to arm organizations with the tools needed to increase security effectiveness and reduce business risk.