FIREEYE | MANDIANT

DEPLOYMENT & INTEGRATION SERVICES DATA SHEET

Network Security

BENEFITS

- **Network architecture** planning to ensure an effective security solution
- **Efficient deployment** by FireEye experts using best-practice configurations
- **Rapid response practices** conveyed to enable quick identification, triage and containment of network alerts
- **Operational readiness** that includes integration with existing technologies, such as other FireEye solutions and SIEM and SOAR systems

Overview

FireEye Deployment and Integration Services help architect and implement an effective network security solution and integrate that solution into your security response processes. Our deployment engineers use in-depth knowledge of the FireEye Network Security solution to ensure an efficient and successful deployment. We offer three types of services to help you maximize the value of your FireEye Network Security solution:

- Deployment Jumpstart Services
- Network Traffic Decryption and Inspection
- Network Security Health Check and Tuning

Deployment Jumpstart Services

Jumpstart Services for FireEye Network Security are designed to help you deploy and configure your Network Security solution quickly and effectively. Whether you are deploying our standalone network appliances or architecting and deploying a more complex distributed security solution using a centrally shared MVX service, Jumpstart Services help you architect and implement the right network solution to meet your security goals.

Jumpstart Services include architecture design review and planning for Network Security, as well as deployment and configuration of network sensors and MVX services. FireEye experts work with you to integrate Network Security with your centralized authentication service (for example, AD or LDAP) and your SIEM and discuss best practices for ongoing maintenance and management. The experts take time to review common use cases with your analysts and recommend approaches for alert review and analysis, threat investigation and pivoting to the endpoint for further analysis.

Network Security Jumpstart Services include:

- Architecture design review and planning for FireEye Network Security
- Configuration and setup based on FireEye best practices
- Connection to Mandiant Threat Intelligence and content updates
- Implementation of MVX SmartGrid, if applicable
- Configuration of applicable optional modules, such as IPS, SmartVision, and SSL inspection
- Integration with centralized authentication and directory services (for example, LDAP or AD)
- Integration of FireEye Network Security with other FireEye security tools in your environment
- Deployment checks and traffic analysis to verify proper placement and configuration
- Review of recommended management and maintenance practices
- Review of FireEye Network Security usage for analysts
- Introduction to FireEye customer resources such as the FireEye Customer Support Portal and Community and FireEye Market

Network Traffic Decryption and Inspection
When implementing network traffic decryption and inspection (SSL intercept), many factors must be considered, including network architecture to facilitate breaking SSL encryption, corporate policies on decrypting and inspecting traffic, types of traffic that should bypass inspection, and proper SSL certificates to facilitate SSL decryption. Extensive experience with implementing network traffic decryption and inspection helps FireEye experts simplify this transition for you. They can help determine an appropriate architecture for the new solution, develop a deployment plan and implement SSL decryption and inspection to avoid gaps in security coverage and business disruptions.

The Network Traffic Decryption and Inspection service includes:

- Network Security architecture review for SSL decryption
- Planning and prerequisites for implementation of SSL decryption
- Implementation of SSL decryption based on FireEye best practices
- Review of recommended management and maintenance practices specific to SSL decryption
- Review of system health and performance post implementation of SSL decryption
- Verification of SSL decryption and network traffic flow

Network Security Health Check and Tuning
With the rapid changes that occur in most corporate networks and the release of new features and capabilities in the FireEye Network 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 Network Security, the Health Check and Tuning service reviews the operation and configuration of your FireEye Network Security deployment and adjusts configurations and policies as needed to align with recommended best practices. Our experts verify that your security system achieves the desired level of network visibility and confirm the solution is up to date on software and content.

The Network Security Health Check and Tuning service includes:

- Comprehensive assessment of system health and performance
- Review of configuration settings as compared to recommended best practices
- Review of network architecture regarding placement of FireEye Network Security solution
- Explanation and enablement of new features, capabilities, and modules
- Assessment of network traffic coverage
- Review of recommended management and maintenance practices
- Review of FireEye Network Security usage for analysts

Table 1. Network Security Services Comparison.*

	Basic Jumpstart	Advanced Jumpstart	Traffic Decryption and Inspection	Health Check and Tuning
Network Security architecture review and planning	✓	✓	✓	Review
Advanced architecture (e.g. high availability)		✓		Review
Best practices configuration implementation	✓	✓	✓	Tuning
Connection to Mandiant Threat Intelligence	✓	✓		Review
Implementation of VX Smartgrid (if applicable)		✓		Tuning
Integration with central authentication (LDAP, AD)	✓	✓		Review
Onboarding with Mandiant Managed Defense (if applicable)	✓	✓		Review
Configuration of IPS module	✓	✓		Review
Implementation of SmartVision (if applicable)		✓		Review
Implementation of SSL Inspection		✓	✓	Review
Database backup and review process	✓	✓		✓
Review of management best practices	✓	✓	✓	✓
Analyst knowledge transfer (alert review and triage)	✓	✓		✓
Assessment of system health and performance	✓	✓	✓	✓
Documentation of installed solution	✓	✓	✓	✓
Assessment of network traffic coverage	✓	✓	✓	✓
API and custom integrations		Limited		

*Required quantity of services SKUs depends on size and complexity of the FireEye Network 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.