FIREEYE | MANDIANT

DEPLOYMENT & INTEGRATION SERVICES DATA SHEET

Network Forensics and Investigation Analysis

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 effective use of network forensics and analysis capabilities
- **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 forensics solution and integrate that solution into your security operations processes. Our deployment engineers use in-depth knowledge of the FireEye Network Forensics solution to ensure an efficient and successful deployment. We offer two types of services to help you maximize the value of your Network Forensics solution:

- Deployment Jumpstart Services
- Network Forensics Health Check and Tuning

Deployment Jumpstart Services

Jumpstart Services for FireEye Network Forensics are designed to help you quickly and effectively deploy and configure your Network Forensics solution alone or in conjunction with an investigation analysis appliance. Whether you are deploying a single packet capture appliance or architecting and deploying a more complex multi-appliance network forensics solution with external storage and a network analysis cluster, Jumpstart Services help you architect and implement the right solution to meet your goals for packet capture and analysis.

Jumpstart Services include architecture design review and planning for Network Forensics, as well as deployment and configuration of components, including network forensics appliances (PX series) and investigation analysis appliances (IA series). FireEye experts work with you to integrate Network Forensics with your centralized authentication service (for example, AD or LDAP), your SIEM, and other FireEye technologies, such as FireEye Endpoint Security. During deployment, FireEye experts review common use cases and best practices for ongoing maintenance and management with your analysts and recommend approaches for alert review and analysis, threat investigation, and pivoting to the endpoint for further analysis.

Network Forensics Jumpstart Services include:

- Architecture design review and planning for FireEye Network Forensics
- Configuration and setup based on FireEye best practices
- Connection to Mandiant Threat Intelligence and content update services
- Implementation of investigation analysis appliance clustering, as applicable
- Deployment and configuration of storage shelves or external storage, as applicable
- Integration with centralized authentication and directory services (for example, LDAP and AD)
- Integration of Network Forensics with other FireEye products in your environment
- Deployment checks and traffic analysis to verify proper placement and configuration
- Review of recommended management and maintenance practices
- Review of Network Forensics use for analysts
- Introduction to FireEye customer resources such as the FireEye Customer Support Portal and Community and FireEye Market

Network Forensics Health Check and Tuning

With the rapid changes that occur in most corporate networks, it can be challenging to ensure your security monitoring solutions maintain the level of network visibility you expect. Discovering that your packet capture solution missed critical traffic due to a network change leaves the team with a major gap in forensics information. To get the most coverage and value from Network Forensics, the Health Check and Tuning service reviews the operation and configuration of your Network Forensics 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 Forensics 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 Network Forensics
- Verification of connectivity and data exchange between integrated components of the solution
- Explanation and enablement of new features, capabilities, and modules
- Assessment of network traffic coverage
- Review of recommended management and maintenance practices
- Review of Network Forensics usage for analysts

Table 1. Network Forensics and Analysis Services Comparison.*

	Basic Jumpstart	Advanced Jumpstart	Health Check and Tuning
Network Forensics architecture review and planning	✓	✓	Review
Advanced architecture (for example, IA clusters and IA Director)		✓	Review
Best practices configuration implementation	✓	✓	Tuning
Implementation of storage shelves or external storage		✓	Review
Connection to Mandiant Threat Intelligence	✓	✓	Review
Integration with central authentication (LDAP, AD)		✓	Review
Onboarding with Mandiant Managed Defense (if applicable)	✓	✓	Review
Integration with other FireEye technology and SIEM		✓	Review
Review of management best practices	✓	✓	✓
Analyst knowledge transfer	✓	✓	✓
Assessment of system health and performance	✓	✓	✓
Documentation of installed solution	✓	✓	✓
Assessment of network traffic coverage	✓	✓	✓
Guidance on API and custom integrations		✓	✓

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