



# McAfee Enterprise Security Manager Deployment Services

## Intel Security Solution Services

### Intelligent Security by Design

Our Solution Services team is committed to helping you realize the full value of your McAfee security investment.

### Benefits

- To establish the Customer with “Best Practices” installation as it relates to their specific SIEM environment while meeting their business and security needs.
- Provide a technical knowledge transfer for their SIEM environment.

We live and work in an ever-evolving, data-driven environment that's making it vital for businesses to integrate intelligent and scalable security information and event management (SIEM) solutions. The Intel® Security Solution Services team can provide you peace of mind with a team of security experts—using industry best practices and proven methodologies—to plan, design, and implement your McAfee® Enterprise Security Manager solution.

### Your Challenge

As an IT security professional, you need to successfully manage competing priorities. These can include collecting events from disparate systems, manually correlating data from different sources, and monitoring activities on all systems, networks, databases, and applications. At Intel Security, we offer a global team of security specialists to help implement a solution that addresses your challenge—from planning, to design, through implementation. Our experts do what they do best so you can focus on what you do best.

### Our Value

Our Solution Services delivery methodology is designed to reduce the time you spend planning, designing, and implementing your SIEM solution—McAfee Enterprise Security Manager. We can help you get up and running with a solution that allows you to react quickly and efficiently to new threats, and understand the significance of past threats. Through instructor-led training and hands-on knowledge

transfer, your staff will be better prepared to effectively maintain and operate your solution for years to come. Rely on our expertise and feel confident that you are taking advantage of the full potential of your SIEM solution.

### Our Methodology and Packaged Offer

Our consultants provide a unique combination of knowledge, experience, and resources to reduce implementation risk, increase protection efficacy, and allow you to experience all that our solutions have to offer.

This McAfee Enterprise Security Manager packaged offer focuses on the planning, design, and implementation stages of your Professional Services engagement. It also includes project management and product installation based on Scope of Services Table (below) and a knowledge transfer for your SIEM security team.

### Develop Your Strategy

We help you get up and running so you can become operational with confidence.

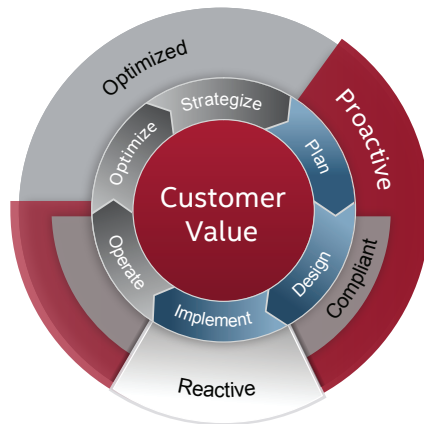


Figure 1. Professional Services Methodology.

### Stage 1: Plan

In this initial stage, we review your current network architecture, change control, and other business processes to facilitate the implementation of your McAfee Enterprise Security Manager solution.

### Stage 2: Design

Next, we will review McAfee Enterprise Security Manager installation prerequisites, and will configure the network interfaces of the McAfee Enterprise Security Manager appliances and the direct attached storage (DAS) devices where applicable.

### Stage 3: Implement

During the implementation stage, we manage a variety of activities including configuration of the following:

- McAfee Enterprise Security Manager, Event Log Manager, Receiver(s), Advanced Correlation Engine, and Direct Attached Storage.
- Federal information processing standards (FIPS) Mode (where applicable).

- Login security.
- Users, groups, and privileges.
- Integration with McAfee ePolicy Orchestrator® (McAfee ePO™) software/ McAfee Network Security Manager/ McAfee Vulnerability Manager.
- Redundancy for applicable devices.
- Data sources.
- McAfee Enterprise Log Manager storage pools.
- Windows events rules, filter rules, alerting, and notifications.

To ensure a successful deployment, we also include the following:

- Correlation and aggregation tuning.
- File maintenance.
- Demonstration of event views.
- Review of the reporting feature.
- Demonstration of custom correlation rules.
- Demonstration of advanced syslog parsing rules.
- Demonstration of Event Log Manager usage in Enterprise Security Manager interface.

### Knowledge Transfer

Finally, we ensure clear and effective knowledge-transfer to your team—occurring interactively throughout the course of the engagement. This covers the installation, configuration, and administration of your McAfee Enterprise Security Manager solution.

## Data Sheet

### Ordering Information

We provide packaged offerings of varying durations to meet your organization's deployment objectives. (See chart for scope.)

### Project Deliverables

- Ensure that the McAfee Enterprise Security Manager solution is working to its full potential.
- Daily Status Reports that show daily activities as outlined in the Solution Services deployment methodology.
- End of Summary report that will demonstrate all of the activities performed over the course of the engagement while highlighting key points and configuration details.

Scope	160 Hours	240 Hours	400 Hours
<b>Installation of McAfee Enterprise Security Manager</b>	Up to five at one site	Up to 10 at up to two sites	Up to 20 at up to four sites
<ul style="list-style-type: none"> <li>• Enterprise Security Manager</li> <li>• McAfee Receivers</li> <li>• McAfee Enterprise Log Manager</li> <li>• Enterprise Security Manager/Receiver/Enterprise Log Manager (Combo/All-in-One)</li> <li>• Install and configure Storage Area Network Adapters</li> <li>• Install Direct Attached Storage</li> <li>• Advanced Correlation Engine</li> </ul>			
<b>Install and configure Storage Area Network Adapters</b>	Included when purchased	Included when purchased	Included when purchased
<b>Define data sources and configure data source rules</b>	Up to 500	Up to 2000	Up to 5000
<b>Demonstrate Filtering Rules</b>	Up to ten	Up to twenty	Up to fifty
<b>Demonstrate Custom Correlation Rule(s)</b>	Up to ten	Up to twenty	Up to fifty
<b>Demonstrate Advanced Syslog Parsing Rule(s)</b>	Up to two	Up to five	Up to fifteen
<b>Demonstrate Custom Events/Flows Views</b>	Up to five	Up to ten	Up to twenty
<b>Demonstrate Reports</b>	Up to five	Up to ten	Up to twenty
<b>Demonstrate Watchlists</b>	Up to ten	Up to twenty	Up to fifty
<b>Demonstrate Alarms</b>	Up to ten	Up to twenty	Up to fifty
<b>Configure McAfee ePO software as a data source</b>	Included, when currently implemented	Included, when currently implemented	Included, when currently implemented
<b>Configure McAfee Threat Intelligence Exchange as a data source through McAfee ePO software</b>	Included, when currently implemented	Included, when currently implemented	Included, when currently implemented
<b>Configure McAfee Advanced Threat Defense as a data source</b>	Included, when currently implemented	Included, when currently implemented	Included, when currently implemented

### Learn More

Intel Security Professional Services is the key to ensuring your organization gets the most out of its SIEM investment. We offer customized services for businesses of all sizes, in all industries, with even the most complex systems requirements. We can help you close the gaps in your business continuity program that will

enable a resilient and sustainable organization that's able to survive catastrophic disruptions. Our consultants can help your organization assess current policies, create new programs that meet compliance goals, and cost-effectively prepare for security emergencies. Find out more at [www.mcafee.com/services](http://www.mcafee.com/services).

