

# McAfee Solution Services

## Essential services for McAfee® SIEM solutions

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. Let McAfee® Solution Services give you peace of mind with a team of certified security experts using industry best practices and proven methodologies to plan, design, and implement your McAfee security information and event management (SIEM) solution.

### Your Challenge

As an IT security professional, you need to successfully manage competing priorities. These can include collecting events from disparate systems, trying to manually correlate data from different sources, and monitoring all activities on all systems, networks, databases, and applications. At McAfee offers 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

McAfee Solution Services delivery methodology is designed to reduce the time you spend planning, designing, and implementing your SIEM solution. 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 SIEM solution for years to come. Rely on McAfee Solution Services and feel confident that you are taking advantage of the full potential of your McAfee security solution.

### Our Methodology and Packaged Offer

McAfee Solution Services 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.

### Intelligent Security by Design

---

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

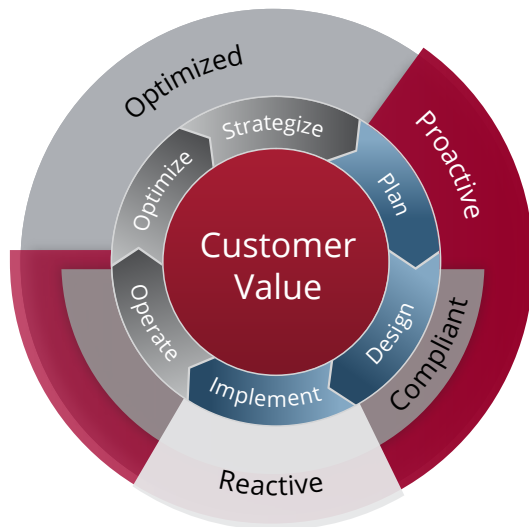
### Benefits

---

With McAfee Solutions Services, you gain peace of mind knowing:

- Your integration includes McAfee project management.
- We discuss your specific security objectives.
- We design, configure, and test your solution.
- We share best practices and recommendations.
- Your staff receives formal classroom and hands-on training.

## DATA SHEET



**Figure 1.** McAfee Professional Services methodology.

This SIEM packaged offer focuses on the planning, design, and implementation stages of your McAfee engagement. It also includes the following:

- **Project management**
- **Classroom training**
- **Product installation**
  - McAfee Enterprise Security Manager
  - McAfee Event Receiver(s)
  - McAfee Enterprise Log Manager
  - McAfee Advanced Correlation Engine
  - McAfee Enterprise Security Manager/McAfee Event Receiver/McAfee Enterprise Log Manager integrated appliance

### 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 SIEM solution.

### Stage 2: Design

Next, McAfee Solution Services professionals will review McAfee SIEM installation prerequisites and will configure the network interfaces of the McAfee SIEM appliances and the direct attached storage (DAS) devices where applicable.

### Stage 3: Implement

This stage consists of a variety of activities including configuration of the following:

- This stage consists of a variety of activities including configuration of the following:
- McAfee Enterprise Security Manager, McAfee Event Log Manager, McAfee Event Receiver(s), and Advanced Correlation Engine
- FIPS mode, where applicable
- Key devices and test communications
- Login security
- Users, groups, and privileges
- SIEM integration with McAfee® ePolicy Orchestrator® (McAfee ePO™) software/McAfee Network Security Manager/McAfee Vulnerability Manager
- Redundancy for primary and secondary receivers in high-availability mode
- Storage pool definitions
- Windows events rules, filter rules, alerting, and notifications

### Develop Your Strategy

McAfee helps you get up and running so that you can become operational with confidence.

### Ordering Information

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

### Additional Services

- Preparing for upgrades
- Migrating to a McAfee SIEM solution
- Vulnerability management program development
- Security operations center assessment
- Incident response assessment
- Incident response

## DATA SHEET

This stage also includes:

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

## Knowledge Transfer

Finally, we ensure clear and effective knowledge transfer to your team, which occurs interactively throughout the course of the engagement. This covers the installation, configuration, and administration of your McAfee security solution.

## Learn More

McAfee 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. Find out more at [www.mcafee.com/services](http://www.mcafee.com/services) or email us at [SolutionServices@McAfee.com](mailto:SolutionServices@McAfee.com).

### Scope

<b>Installation of McAfee SIEM solution</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>▪ McAfee Enterprise Security Manager</li> <li>▪ McAfee Event Receivers</li> <li>▪ McAfee Enterprise Log Manager</li> <li>▪ McAfee Enterprise Security Manager/McAfee Event Receiver/McAfee Enterprise Log Manager combo</li> <li>▪ Install and configure SAN adapters</li> </ul>			
<b>Define data sources and configure data source rules</b>	Up to 50	Up to 150	Up to 250
<b>Configure McAfee Enterprise Security Manager rules</b>	Included	Included	Included
<b>Demonstrate filtering rules</b>	Included	Included	Included
<b>Demonstrate custom correlation rule(s)</b>	Up to one	Up to two	Up to five
<b>Demonstrate custom event view(s)</b>	Up to one	Up to two	Up to five
<b>Demonstrate watch list</b>	Up to one	Up to two	Up to five
<b>Demonstrate report</b>	Up to one	Up to two	Up to five
<b>Purchase these SKUs in the quantity indicated:</b>			
<b>TRN-VOUCHER</b>	26 per student	26 per student	26 per student
<b>MD-DEPLOY</b>	4	6	10



2821 Mission College Boulevard  
 Santa Clara, CA 95054  
 888 847 8766  
[www.mcafee.com](http://www.mcafee.com)

McAfee and the McAfee logo, ePolicy Orchestrator, and McAfee ePO are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others. Copyright © 2017 McAfee, LLC  
 61416ds\_siem-sol-services\_1014  
 OCTOBER 2014