

## Security Event and Log Management

Report critical security events from endpoints and network devices to McAfee ePolicy Orchestrator



**McAfee Compatible Solution**  
 • ArcSight ESM 4.0 and McAfee ePO 4.0 and 4.5

ArcSight's market-leading log and event management solutions are now integrated with McAfee® ePolicy Orchestrator® (McAfee ePO™), McAfee's centralized security and compliance management platform. The integrated solution enables powerful new security workflows that link real-time monitoring, threat detection, and incident response.

### Business Problem

In organizations of even moderate size, the number and types of devices on the network can easily overwhelm an administrator's ability to manage and secure both the perimeter and the interior. Firewalls, VPNs, intrusion prevention systems, routers, switches, database servers, application servers, desktops laptops, and handheld devices are common, and an automated and comprehensive solution is highly desirable for configuring, monitoring, remediating, and auditing these devices.

In most enterprises, IT managers must perform at least three major tasks: (1) monitor their systems, network devices, and end-user activity; (2) implement real-time threat visibility, incident detection, and response; and (3) achieve and maintain regulatory compliance.

Today's security threats and economic challenges demand that industry-leading solutions in all three spheres interoperate to provide better protection, reduce operational costs, and streamline the compliance life cycle.

### McAfee and ArcSight Joint Solution and Benefits

ArcSight Enterprise Security Manager (ESM) integrates with McAfee ePO to enable closed-loop security monitoring, log management and policy enforcement. By passing alerts generated from correlated events into McAfee ePO, ArcSight ESM drives the quick detection of security threats, compliance violations and policy breaches, improving the context for targeted countermeasure, audit, and remediation functions provided by McAfee security solutions.

More specifically, the integrated solution works as follows:

- ArcSight Connectors gather log data from hundreds of network device types
- ArcSight ESM performs event correlation to determine in real time if a security breach has occurred
- Incident notifications are then sent to McAfee ePO, along with information about the host appliance, impacted host, impacted application, protocol, threat type, and other data
- Examples of corrective actions within McAfee ePO include updating security policies, running a virus scan, pushing out new signatures or patches, enhancing endpoint protection, starting a compliance audit scan, and more
- In parallel, administrators can perform historical drill-down and root-cause analysis in the ArcSight ESM console

The integrated solution helps bridge the gap between event monitoring and incident response, helping security administrators respond with prioritized and targeted countermeasures. Working together, McAfee and ArcSight deliver a more comprehensive solution, while reducing operational costs and improving security and compliance.

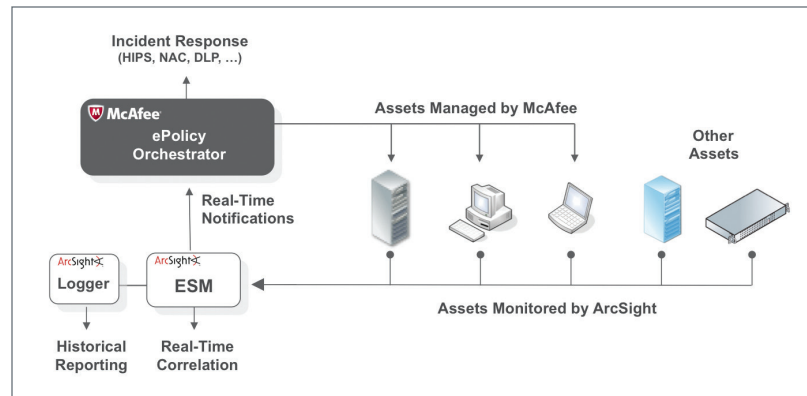


Figure 1. ArcSight and McAfee integration overview.

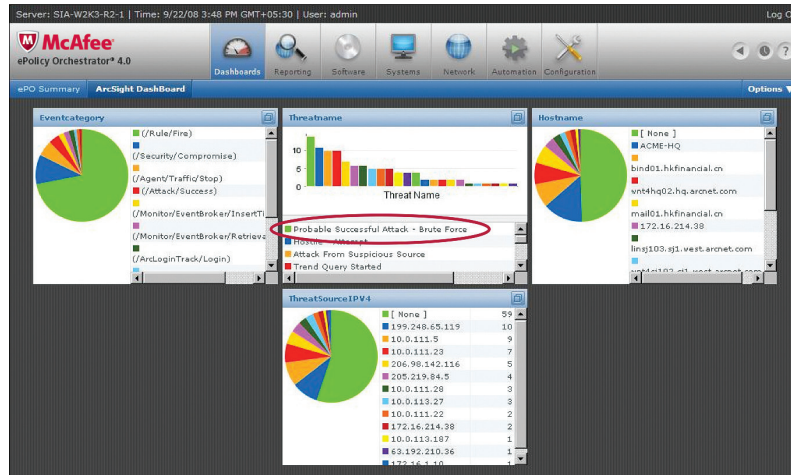


Figure 2. McAfee ePO dashboard with ArcSight events.

The joint solution from McAfee and ArcSight helps bridge the gap between event monitoring and incident response. While extremely powerful, the integration is available out of the box and is very straightforward to configure and use. Customers can harness the power of ArcSight security monitoring while also leveraging the comprehensive security management of McAfee ePO software. Security administrators can respond to incidents with prioritized and targeted countermeasures and also perform root-cause investigation. Working together, McAfee and ArcSight deliver a comprehensive solution while reducing operational costs and improving security and compliance.

### About ArcSight

ArcSight is a leading global provider of security monitoring (SIEM) and compliance management solutions. ArcSight identifies, assesses, and mitigates both internal and external cyberthreats and risks across the organization for activities associated with critical assets and processes.

### About McAfee ePolicy Orchestrator (ePO) software

McAfee ePO software is the industry-leading security and compliance management platform. With its single agent and single-console architecture, ePO software provides intelligent protection that is automated and actionable, enabling organizations to reduce costs and improve threat protection and compliance.

