



# Increasing Security and Compliance with End-to-End System Monitoring and Management

## Table of Contents

Overview	3
The Enterprise Network	3
Configure all devices	3
Monitor all devices	3
Remediate and audit	3
McAfee and ArcSight	4
ArcSight Products and the Joint Solution	4
McAfee Products and the Joint Solution	5
Integrated Solution Details	5
Example 1—ArcSight ESM integrated with the McAfee ePO platform and the McAfee Data Loss Prevention solution	6
Example 2—ArcSight ESM integrated with the McAfee ePO platform and the McAfee Network Access Control solution	6
Example 3—ArcSight ESM integrated with the McAfee ePO platform and the McAfee Policy Auditor software	7
Example 4—ArcSight ESM integrated with the McAfee ePO platform and the McAfee Host Intrusion Prevention software	7
Conclusion	8

McAfee, the world's largest dedicated security technology company, and ArcSight, the market leader in the security information and event management (SIEM) industry, have created a joint solution to shorten the amount of time between detection of a security incident and when a response can be made. Through its participation in the McAfee® Security Innovation Alliance program, ArcSight has created an integration between ArcSight ESM and the McAfee ePolicy Orchestrator® (McAfee ePO™) platform. This paper describes the integration and the value the joint solution delivers across a range of possible threats.

#### Key Points

McAfee–ArcSight integration benefits:

- Comprehensive data collection
- Advanced attack detection
- Wide range of protective measures
- Closed-loop auditing for compliance

ArcSight product areas covered:

- ArcSight Connector Appliance
- ArcSight Logger
- ArcSight ESM

McAfee product areas covered:

- McAfee ePolicy Orchestrator
- McAfee Total Protection for Endpoint
- McAfee Network Access Control
- McAfee Policy Auditor
- McAfee Host Data Loss Prevention
- McAfee Host Intrusion Prevention

#### The Enterprise Network

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.

#### Configure all devices

Each device type has its own settings, patches, and policies, and many organizations create reference configurations for each. Most devices typically receive their reference configuration and subsequent updates from a centralized management console, such as the McAfee ePO management platform. Sound reference configurations, however, are only a starting point for a secure network.

The next step is to then defend against new vulnerabilities and malware that are encountered every day and that impact both new and existing applications, the operating system, and sensitive data. Adding to the urgency of this need for proactive defense is the fact that, if permitted, end users routinely violate security policies, and many IT administrators access and update systems directly. The result is a serious increase in security risk for an organization.

#### Monitor all devices

Monitoring system and network activity has become a core requirement for a comprehensive IT strategy. Monitoring ensures that policies and configurations are in fact working properly and new malware and vulnerabilities are detected promptly. If an incident or breach does occur, monitoring finds it quickly, so that response and remediation can begin before the problem compounds. Three factors directly influence the effectiveness of monitoring for security and compliance:

- *Coverage*—The more data that is fed into the monitoring engine, the more likely that engine will find potential problems. A broad collection of activity event data is, therefore, key to accurate monitoring.
- *Data volume*—A sound monitoring solution must be able to keep up with high volumes of traffic from all endpoints and network devices
- *Analysis*—Security analysis is driven by rules and correlation. Effective rules applied to accurate data provide the ability to sift through the “noise” of daily enterprise activity to find the incidents that actually require attention. Effective correlation increases the monitoring engine's ability to find subtle problems within the millions of events that take place on the network each day.

#### Remediate and audit

When the monitoring engine detects security incidents or compliance violations, the same solution that manages device configuration can also enable corrective actions. For instance, it might help quarantine a device, update software, install a patch or new security definitions, or deploy new access policies. All potentially affected systems can then receive the updates, either automatically or via workflows initiated by an administrator.

Finally, after all affected systems are successfully reconfigured, an audit scan would take place to ensure that the new policies, files, and other essential components are correctly installed and working. The configuration console's dashboard is updated with the results of the audit, and administrators then feel confident that the devices they manage are once again secure and compliant.

### McAfee and ArcSight

To some organizations, the functions described in the previous section may seem too ambitious. Fortunately, products that perform these functions are available today from McAfee and ArcSight, who have created a technology alliance. Their integrated products automate the cycle of “collect-detect-protect-inspect” for the corporate network and reduce the time from incident detection to response and remediation.

- *Collect*—By collecting activity information from almost every device on the network, the McAfee–ArcSight solution ensures global coverage. Attackers cannot slip through because of insufficient visibility.
- *Detect*—Through advanced analytics and multidevice correlation, the McAfee–ArcSight solution detects even the most sophisticated external attacks or coordinated breaches from trusted insiders. Upon detection, the solution can automatically initiate protective measures to prevent damage.
- *Protect*—Through its advanced understanding of both security risk and device configurations, the McAfee–ArcSight solution enables a range of protective measures. These include updating policies, installing patches, modifying malware signature files, notifying administrators, or taking other actions on managed devices.
- *Inspect*—To close the loop, the McAfee–ArcSight solution can run new audit scans of affected systems to ensure that protective actions were successful and to verify compliance for auditors. The results are fed back into the event correlation engine to more accurately detect future security incidents on the network.



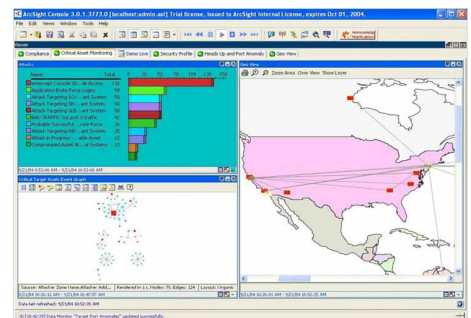
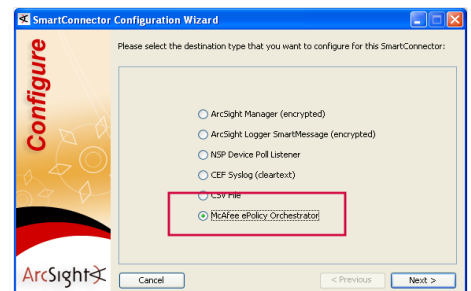
The result of this cycle is better security, improved compliance, and reduced costs through automation.

### ArcSight Products and the Joint Solution

ArcSight brings several key products to the partnership. The first is the ArcSight Connector Appliance, available in multiple sizes. ArcSight Connectors collect event data in native format from hundreds of types of systems. The Connectors transform the data to a common format, allowing more powerful analysis through multidevice correlation. The ArcSight Forwarding Connector includes a pre-built graphic user interface (GUI) option for sending correlated security events to the McAfee ePO platform.

The second product is ArcSight Logger, a self-contained appliance for long-term storage of activity event data. ArcSight Logger retains all events collected by the Connectors for later reporting and contextual analysis.

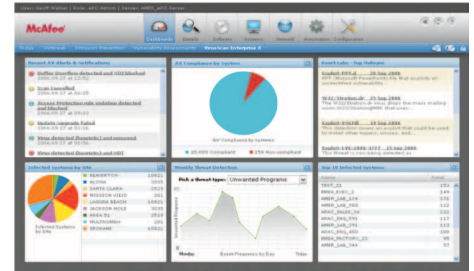
The third product is ArcSight ESM, a leading solution for real-time analysis and correlation of security event information. Like ArcSight Logger, ESM also receives normalized events from the ArcSight Connectors. While Logger stores events for later reporting, ESM correlates events in real time to determine if potential security or compliance incidents are occurring. ArcSight ESM can correlate events over time, against trends, and across multiple systems to find even subtle breaches or attacks.



Taken together, the ArcSight products cover the “collect and detect” phases of the security cycle. When a problem is detected, ArcSight ESM sends an alert to the McAfee ePO platform, where an administrator can initiate the “protect and inspect” phases.

### McAfee Products and the Joint Solution

McAfee also brings several key products to the partnership. The McAfee ePolicy Orchestrator platform is the industry-leading solution for managing security and compliance. The McAfee ePO platform manages nearly 60 million endpoints for more than 35,000 customers. Based on a single-agent, single-console architecture, the McAfee ePO platform manages security policies and configurations and presents intelligent security that is automated and actionable.



McAfee Total Protection™ for Endpoint software provides comprehensive protection from today’s advanced threats in a single, integrated solution. It works with the McAfee ePO platform to deliver continuous and updated protection against threats like spyware, malware, rootkits, email viruses, spam, potentially unwanted programs, zero-day hacker attacks, and more. Key technologies here include anti-virus, anti-spyware, and host intrusion prevention system (HIPS).

The advanced version of McAfee Total Protection for Endpoint software offers McAfee Network Access Control (NAC) capabilities to help identify, quarantine, and remediate affected systems. Also included in the advanced version is McAfee Policy Auditor software, which helps organizations proactively define, measure, and report on system compliance, based on industry, regulatory, and corporate security policies. McAfee Policy Auditor software finds and reports vulnerabilities, service misconfigurations, and policy violations. By mapping IT controls against predefined policies, McAfee Policy Auditor software automates what is usually a manual audit process and enables organizations to produce consistent and accurate reporting against internal and external policies.

An additional product that contributes to the McAfee–ArcSight solution is the McAfee Data Loss Prevention (DLP) appliance, which protects against theft and accidental disclosure of confidential data across networks, through applications, and via removable storage devices.

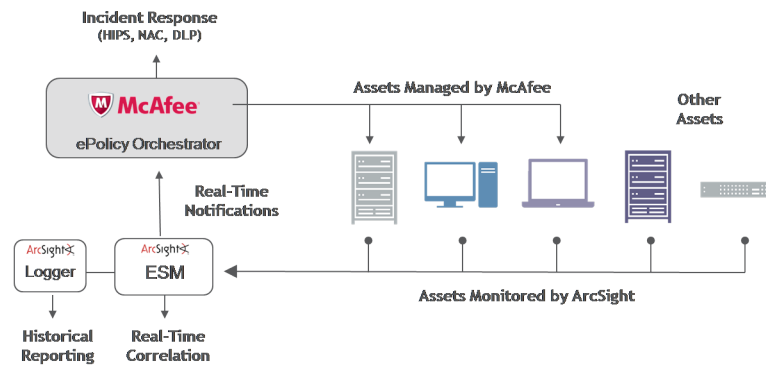


Figure 1. The integration of McAfee and ArcSight enables market-leading management and monitoring of network assets.

### Integrated Solution Details

This section discusses the McAfee–ArcSight solution in more depth and focuses on four real-world examples where ArcSight detects critical security incidents and sends them to McAfee ePO consoles. Depending on the nature of the incident and the McAfee security software installed on the endpoint, the McAfee ePO platform administrator can take the right corrective action to mitigate the incident.

**Example 1—ArcSight ESM, the McAfee ePO platform, and the McAfee Data Loss Prevention solution**  
 On a financial company's network, for example, ArcSight event collectors and the ESM correlation engine might detect any of the following security events: (a) an inactive/deactivated account is being used, (b) an unauthorized user has accessed a critical server, or (c) an attacked system is sending suspicious communication. In all cases, ArcSight ESM promptly alerts the McAfee ePO platform about all information related to the event.

The McAfee ePO administrator can then use the McAfee Data Loss Prevention solution to alter the removable media policy on the host to lock down data outflow or to begin monitoring the asset in stealth mode, as shown in the figure below. In addition to assets, new removable media access policies and monitoring can also be applied to specific users.

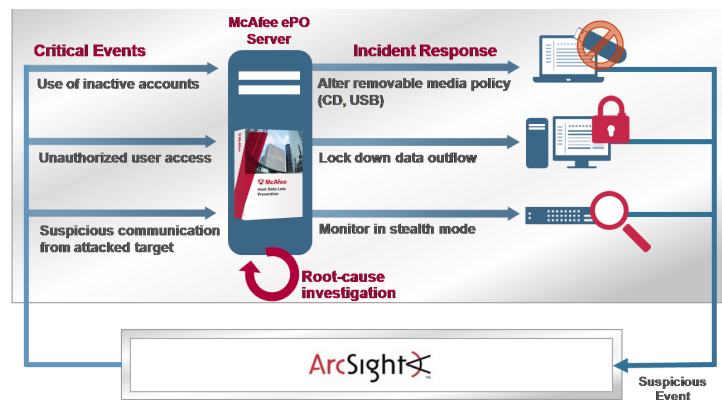


Figure 2. ArcSight ESM, McAfee ePO platform, and the McAfee Data Loss Prevention solution.

**Example 2—ArcSight ESM, the McAfee ePO platform, and the McAfee Network Access Control solution**  
 On a large enterprise network, ArcSight event collectors and the ESM correlation engine might identify any one of the following notable threats: (a) an attack on an asset has succeeded, (b) a compromised asset begins attacking other internal systems, or (c) a compromised asset is sending suspicious communication.

ArcSight ESM immediately places an alert in the McAfee ePO console. As shown below, the McAfee ePO administrator can use the McAfee Network Access Control solution to either quarantine the host or reduce its access privileges on the network, and more rapidly begin a root cause investigation.

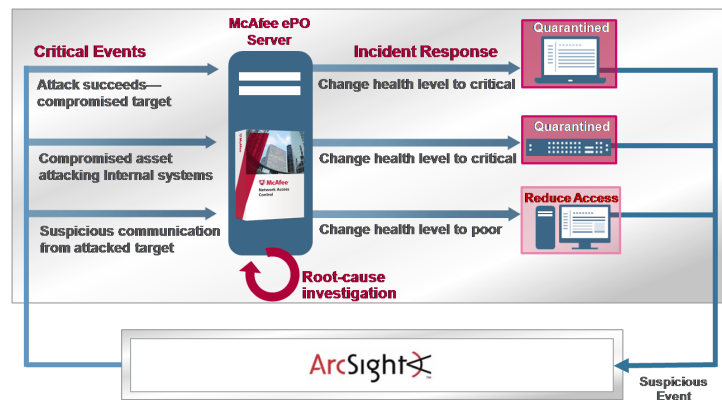


Figure 3. ArcSight ESM, the McAfee ePO platform, and the McAfee Network Access Control solution.

**Example 3—ArcSight ESM, the McAfee ePO platform, and the McAfee Policy Auditor software**  
 On a healthcare provider’s network, ArcSight event collectors and the ESM correlation engine might identify critical security incidents, such as unauthorized administrative access or privilege escalation, which are often the precursors to more severe security breaches. ArcSight ESM sends all relevant details as an alert to the McAfee ePO dashboard.

The McAfee ePO administrator can use McAfee Policy Auditor software to run audit scans to detect what configurations or privileges have changed since the last scheduled scan and perform further root-cause investigation in ArcSight ESM to reconstruct the chain of events.

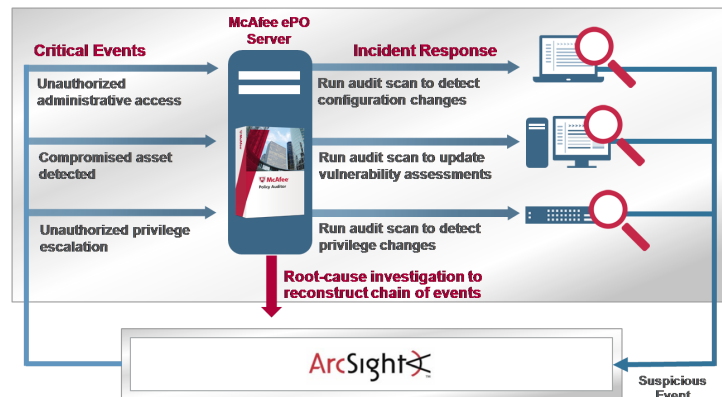


Figure 4. ArcSight ESM, the McAfee ePO platform, and the McAfee Policy Auditor software.

**Example 4—ArcSight ESM, the McAfee ePO platform, and McAfee Host Intrusion Prevention software**  
 On a major manufacturing company’s network, for example, ArcSight event collectors and the ESM correlation engine identify one or more of the following critical security incidents: (a) a brute-force attack, (b) an unauthorized configuration change on a server, or (c) a SQL injection attack on a database.

ArcSight ESM sends all relevant details as an alert to the McAfee ePO dashboard. As shown in the figure below, the ePO administrator can use McAfee Host Intrusion Prevention software to install new firewall filtering rules or new server policies to block the attacks.

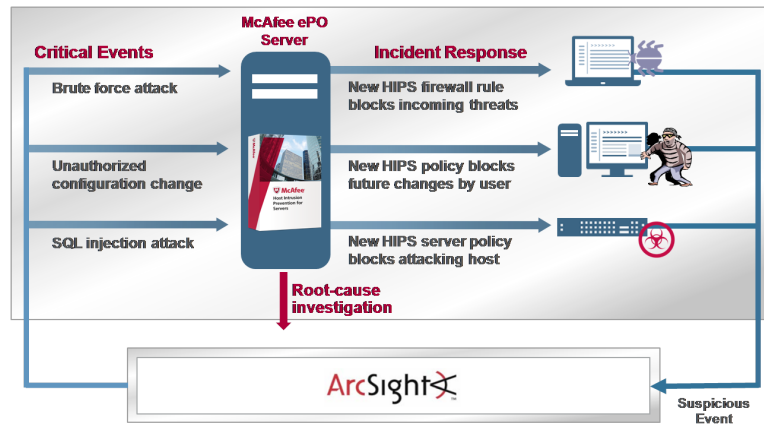


Figure 5. ArcSight ESM, the McAfee ePO platform, and the McAfee Host Intrusion Prevention software.

### **Conclusion**

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.

To learn more, please contact your local McAfee or ArcSight sales representative, or for a solution brief, please visit: [http://www.mcafee.com/us/partners/security\\_innovation\\_alliance/sia\\_partner\\_listings.html#arcsight](http://www.mcafee.com/us/partners/security_innovation_alliance/sia_partner_listings.html#arcsight).

