APPLY
SITUATIONAL
AWARENESS
From actionable intelligence to intelligent action
Get actionable insight from your security systems

The Situation
One of the questions IT and security professionals ask most frequently is, “Can you tell me how this piece of malware got onto my system?”

If you administer or manage endpoints, you probably have discovered an infected or compromised system. Your first reaction is to find the system and clean it, so that it does not affect your other systems and the user can get back to work. Your second reaction is probably, “How did this system get infected or compromised?” Unfortunately, most organizations do not have the ability to easily piece together all the information needed to understand an incident such as this. If just a single system is affected, it is a luxury for an administrator to track down the root cause—a luxury few can or choose to afford.

However, an infected or compromised system can be a sign that your cyberinfrastructure is threatened. If you can find a way to know more about an incident than just which system you fixed or quarantined, you may end up saving your organization time and money.

Driving Concerns
Situational awareness has become a priority for organizations concerned with the increasing volume and subtlety of attacks—both in the public and private sector.

To achieve situational awareness, you must collect, identify, process, and comprehend the data from not only your internal IT infrastructure, but also from external sources. From this wealth of data, you need to produce actionable information to help yourself and others make decisions on the operation and defense of your IT infrastructure.

Unfortunately, there is no “out of the box” solution for achieving situational awareness. That is one reason most organizations believe the road to situational awareness is slow. Common obstacles include:

• **Collaboration**—Instead of viewing IT as an ecosystem, many companies have siloed their IT departments into functional islands such as networks, servers, and desktops. This divides not only the people involved, it also divides the data and the investigation. Pools of data and people form—pools that never mix or synchronize with one another. Logs and other data that are kept separate may make the situation seem benign. Everyone has a piece of the puzzle, but no one knows what the whole picture looks like. Keeping teams and data separate also wastes time and energy. For example, during a security event, multiple teams could be investigating the same data in parallel.

• **Historical data**—Historical data can hold clues to ongoing attacks as well as future attacks. If enterprises are collecting logs, it is usually for compliance reasons. They seldom mine the available data to glean attack clues, improve their security, or mitigate risk in their environments.

• **Accurate knowledge of existing assets**—Many organizations have unknown devices on their network or devices that enter and exit the network between scheduled asset and vulnerability scans. These devices frequently lack patches and controls and present a vulnerable attack surface. Organizations need a constantly updated view of the devices on their network.

• **Readily-available critical data**—After an event, forensic teams usually find evidence of breaches or cyberattacks in the logs collected by IT departments. For situational awareness, IT departments need to get to this critical data during the event—when it can be most useful. Instead, the data they need is hard to find, hard to interpret, lost, or drowned out by all the other data. This is usually due to the disparate tools being used by the different siloed organizations.
Apply Situational Awareness

- **Predictive analysis**—The objective of situational awareness is to reduce risk by adjusting countermeasures as threats and risks change. Without historical data, easily accessible current data, and an efficient way to analyze them, an organization cannot predict or speculate where the next attack or security breach may occur and cannot adjust security systems accordingly. IT organizations need to know about new threats and vulnerabilities, and they need to know how their infrastructure may be at risk relative to these emerging dangers.

- **Wide-angle view of vulnerabilities and threats**—Besides being blinded by silos within their own IT ecosystems, organizations can also miss a wider perspective, a viewpoint that includes what is going on beyond the network perimeter. For example, many IT teams do not track patching or threats for vendors other than Microsoft. What about Adobe, Apple, and Oracle (particularly Java) applications used in the infrastructure? These platforms have become the attack surface of choice. Also, few organizations track vulnerabilities and attacks related to their business or vertical industry. For example, if you run an IT team for a bank, do you track the vulnerabilities relevant to financial services? System and network administrators need to understand what is happening outside their network and how this activity may affect them and the business or its assets.

These are some of the challenges standing in the way of gaining situational awareness. If you can overcome them, you can reduce the time to discovery and make risk and mitigation decisions based on a well-rounded and complete data set.

**Decision Elements**

These factors could influence your architecture:
- Where you store data such as logs and events.
- Whether you manage network peripherals such as your firewall directly or you outsource this function.
- The number of events per second your network devices are generating.

**Solution Description**

To attain situational awareness, your organization must break down technical walls that keep teams and critical data separated. You must allow the decision makers managing your risk to see not only your internal infrastructure as a whole, but also to see beyond your perimeter to external actors, external dependencies, and all associated threats.

- **Bring it all together**—The solution should not only gather all logs into a central location, but also make them accessible from a central web user interface (UI). A central web UI allows the multiple teams within IT to see the whole picture. Bringing all the logs and data of your IT ecosystem together not only makes access easier, it fosters collaboration among teams. Teams will no longer waste time looking at the same data; they can find the root cause to an incident or compliance violation faster.

- **Easy event analysis regardless of your timeframe**—Now you need to analyze the events and logs. The solution should make it easy for you to access all this data for immediate analysis, widen your search across longer periods of time, or focus on a particular moment. All event details should be preserved according to forensic best practices (in the event you need to present the information in court) and must be easy to access in a timely fashion.

- **Beyond your perimeter**—IT administrators should be able to view new threats in the wild, filter out irrelevant noise (vulnerabilities affecting applications they do not use), and zero in on the threats that pertain to their IT infrastructure and business.

- **Responding**—Once you understand the nature and scope of the event, the solution must allow you to respond or react in a timely fashion. Policies and thresholds linked to risk should trigger automated responses, such as activation of countermeasures, and alert you to the highest priority events that could damage your organization’s risk posture and valued assets.

- **Forecasting**—For your IT organization to move from reactive to proactive, you must be able to map out where you might have issues in the future. Forecasting that an incident may occur or where it may occur helps the IT team prepare and proactively defend against an attack. Therefore, the solution has to allow quick access to pertinent information for analysis and forecasting. This data needs to include information about your infrastructure, as well as threat feeds about the latest vulnerabilities that may affect your applications, servers, endpoints, and network. This will help you correlate this information and know where your risks are, so that you can manage them effectively.
Technologies Used in the McAfee Solution

The McAfee solution has two primary security management components: McAfee® Enterprise Security Manager, (the McAfee security and information event management [SIEM] solution) and McAfee® ePolicy Orchestrator® (McAfee ePO™) software. This core platform includes and leverages integrations within the Security Connected portfolio and with McAfee Security Innovation Alliance partners to extend visibility and control across the entire security and compliance management environment. McAfee Enterprise Security Manager provides data capture, correlation, and analysis and a central command and control (C&C) console. It unites and makes sense of disparate IT data sources and provides a tight integration with the McAfee ePO software policy-based management environment that provides control and an additional set of integrations. IT teams throughout the enterprise can access and navigate all this information to allow real-time collaboration, controlled response, and accurate reporting.

Figure 1. McAfee correlates data across sources to facilitate assessment and guide prompt action.

- **Centralized and accessible logs**—McAfee Enterprise Security Manager provides data capture, correlation, and analysis and a central C&C console. IT teams throughout the enterprise can access and navigate all this information to allow real-time collaboration, controlled response, and accurate reporting. The optional McAfee Event Log Manager efficiently collects, compresses, and stores all log files and provides advanced searching, analytics, correlation, alerting, and reporting.

- **Data and analytics at your fingertips**—Like other SIEMs, McAfee Enterprise Security Manager collects logs, events, and data from the various appliances and software running your IT infrastructure. However, the speed and capacity of McAfee Enterprise Security Manager separates it from other SIEM solutions. For example, you can collect all the logs from all the data sources you want to monitor, correlate events, and report on months of data in less than 10 seconds. For historical analysis, the system can process billions of events from multiple years—presenting query results in seconds, not hours. Events and alerts provide easy, one-click access to the original source log record for forensics.

- **Real-time visibility with context**—McAfee Enterprise Security Manager brings together all the data you need to assess the situation in context. The McAfee Enterprise Security Manager system can show you the relevant threat data related to the assets that you value most as threats and vulnerabilities evolve. Extensible dynamic watch lists store context and continually categorize external and internal systems based on risk and past behavior so you can focus monitoring efforts on those with the highest risk.

## Visualize, Investigate, Respond

- See log frequencies
- Search for logs
- Correlate events
- What data is involved?
- Who is involved?
- Are they a bad actor?
- What is the risk of the system?
- What is the risk of the user?

## Advanced Correlation Engine

- Global Threat Landscape
  - Threat intelligence feed
  - Immediate alerting
  - Historical analysis

- Enterprise Risk Landscape
  - Vulnerabilities
  - Countermeasures
  - Individuals

## Dynamic Context

- Content Aware

## Traditional Context

- Log Management

Apply Situational Awareness
» **Threats**—McAfee Global Threat Intelligence for McAfee Enterprise Security Manager feeds real-time threat data into the McAfee Enterprise Security Manager correlation engine. SIEM-connected devices can perform reputation checks in real time and immediately alert security analysts when a system has interacted with a known bad actor.

» **Risk**—McAfee Risk Advisor feeds the SIEM asset valuation data and information about the criticality of data. McAfee Risk Advisor helps you understand if a critical asset is protected by proactively correlating a threat feed with vulnerability and countermeasure information to pinpoint at-risk critical assets that require immediate attention. McAfee Risk Advisor helps determine what countermeasures you need and when you need them. The McAfee Advanced Correlation Engine appliance deploys alongside McAfee Enterprise Security Manager to identify and score threat events in real time using both rule- and risk-based logic. You tell McAfee Advanced Correlation Engine what you value—users or groups, applications, specific servers, or subnets—and it will alert you if the asset is threatened.

» **Asset inventory**—The McAfee Asset Manager module of McAfee Vulnerability Manager can passively monitor network traffic to collect a full software and hardware asset inventory and user-to-asset mapping from active, virtualized, mobile, and hidden devices. McAfee Vulnerability Manager for Databases automatically discovers all databases and helps you assess potential vulnerabilities.

» **Host state and vulnerability**—McAfee ePO software provides access to host software and countermeasure data, including installed applications, patch levels, and vulnerability data collected from McAfee Vulnerability Manager scans. New scans can be automatically initiated from the SIEM based on system risk. Real time for McAfee ePO, when used in conjunction with McAfee Enterprise Security Manager, allows deep inspection of real-time system state—automatically identifying which applications, accounts, and other processes are running within a specified time window so you can know the precise situation and determine if new threats are relevant. Analysts have on-demand access to other system details, including users, security and system configuration, files present, open ports, and patch levels.

» **Application usage**—Extend McAfee Enterprise Security Manager with McAfee Application Data Monitor to monitor from the network stack to the application layer. You can fully inspect application contents to achieve the deepest visibility into how your network is being used and threats that may be masquerading as legitimate applications.

• **Intelligent action**—Alerts and the workflow notify analysts immediately when attacks are occurring, applying advanced analytics for intelligent prioritization of issues. For example, flow analysis and baselining identify security-relevant anomalous behavior. IT can leverage policies and integrations to increase monitoring, correlate data, gauge risk, or drive an instant, automatic remediation, such as issuing new configurations, implementing new policies, and deploying software updates. Actions can include:

  » **Hosts**—McAfee ePO software integration allows tagging of suspicious systems and adjustment of policy settings automatically from the SIEM, as well as automated remediation to the endpoint, ensuring that internal systems are protected from active attacks.

  » **Networks**—Active quarantining from the SIEM to the McAfee Network Security Platform stops attacks in their tracks.

  » **Data**—Deep integration with McAfee Data Loss Prevention (DLP) delivers strong data type context and the ability to automatically adjust DLP policy settings from the SIEM via McAfee ePO software.

• **Prediction**—Once your organization captures baselines for what you consider “normal” behavior for users, roles, or networks, your systems should provide guidance as risks change over time. Anomalous behavior can signal attack precursors such as network reconnaissance, disgruntled insiders, and inappropriate use of resources. While any individual event may be either worrisome or benign and worth investigation, a string of unusual events for a host, user, or timeframe could signal very significant trouble.
» Dynamic insights—McAfee Global Threat Intelligence can keep McAfee products and your risk management dashboard up to date with changing threat and risk data, as well as information on communications with risky actors and addresses.

» Automated alerting—McAfee Enterprise Security Manager can bring your attention to anything outside the normal standard. The SIEM solution provides analytics connected to alerts and thresholds, as well as watch lists, so you can predict where you may face events and take action to intervene or mitigate risk.

» Spotlights—To increase the effectiveness of future monitoring processes, analysts can quickly adjust McAfee Enterprise Security Manager to detect future recurrences, improving security monitoring for the long term.

» Risk mitigation—SIEM integrations with other McAfee products permit automated quarantine of suspicious hosts throughout the network.

**McAfee Enterprise Security Manager**

McAfee Enterprise Security Manager is an enterprise-class security information and event management system (SIEM) that identifies, correlates, and remediates threats. Through automated collection of the data throughout your enterprise and real-time correlation and prioritization, McAfee Enterprise Security Manager helps you find the events and logs needed to answer questions, identify root causes to incidents, and bring together data for audits. You are free to spend more time on analyzing, forecasting, and adjusting countermeasures to changing events.

McAfee Enterprise Security Manager actions include:

- Full collection, analysis, and reporting of log and event data at enterprise speed and scale.
- Automatic establishment of security baselines in real time, so you can easily see “normal” versus “abnormal” behavior.
- Proactive risk and threat detection based on your organization’s priorities.
- Automated launching of remediations involving changes in configuration, policy, or installation of software updates.
- Auditing of device configurations and detection of configuration changes.
- Tracking and logging of all incident investigations and response activities.

Several options help you customize your SIEM environment to your risk posture:

- **McAfee Global Threat Intelligence for Enterprise Security Manager**—This optional subscription service continually delivers and adjusts source reputations for more than 140 million IP addresses, bringing the context of external system reputations directly into the security event stream and quickly identifying current and past interactions with known bad actors.

- **McAfee Enterprise Log Manager**—If it is a log, McAfee Enterprise Log Manager can collect and store it: syslogs, event logs, application logs, and firewall logs. Logs are signed and validated, ensuring authenticity and integrity, a necessity for regulatory compliance. Integration with McAfee Enterprise Security Manager provides advanced searching, analytics, correlation, alerting, and reporting with the greatest operational efficiency.

- **McAfee Advanced Correlation Engine**—The standalone McAfee Advanced Correlation Engine appliance supplements McAfee Enterprise Security Manager event correlation with two dedicated correlation engines and purpose-built performance. It has a risk detection engine that generates a risk score using rule-less risk score correlation and a threat detection engine that detects threats using traditional rule-based event correlation. Its processing power and data engine support rich event correlation across your entire enterprise and scale to accommodate even the largest networks.

- **McAfee Application Data Monitor**—This appliance can decode an entire application session, providing a full analysis of underlying protocols and session integrity all the way up to the contents of the application (such as the text of an email or its attachments). These details allow accurate analysis of real application use, while also enabling you to enforce application use policies and to detect malicious, covert traffic. When McAfee Application Data Monitor detects a violation, it preserves all details of that application session for use in incident response and forensics or for compliance audit requirements.
McAfee ePolicy Orchestrator software
McAfee Enterprise Security Manager connects with McAfee ePO software through a two-way integration for improved threat tracking and risk assessment. This connection brings together the entire McAfee portfolio plus the dozens of McAfee Security Innovation Alliance partner solutions to create a complete framework enabling your IT organization to attain situational awareness.

McAfee ePO software provides flexible, automated management so you can identify, manage, and respond to security issues and threats. You can define how McAfee ePO software should direct alerts and security responses based on the type and criticality of security events in your environment. In addition, you can create automated workflows between your security and IT operations systems to quickly remediate outstanding issues.

McAfee ePO software also gives you the controls to react to issues as you discover them within your infrastructure.

• If you are concerned about a desktop or server, then McAfee ePO software can work with defenses such as McAfee Host Intrusion Prevention System, McAfee VirusScan® Enterprise, and McAfee Application Control to help mitigate the risk. You can deploy a new control on vulnerable desktops, laptops, or servers; update a policy; run a vulnerability or audit scan to review your risk posture; and create alerts and reports to increase visibility.
• If the risk is email-borne, then the McAfee Email Gateway or McAfee Security for Email Servers can help.
• McAfee Firewall Enterprise, McAfee Network Security Platform, and McAfee Web Gateway can be used to shield against network attacks that have been discovered or forecasted.

All of these products are integrated with McAfee ePO software and McAfee Enterprise Security Manager to enable an efficient response to present and immediate threats or future risks.

McAfee ePO software stores information on all hosts in its repository. If you deploy the passive discovery and monitoring feature in McAfee Vulnerability Manager, you can augment the McAfee ePO software database with valuable information about the usage and profile of each device on your network.

Real Time for McAfee ePO
Real Time for McAfee ePO is an add-on option for McAfee ePO software available with McAfee endpoint suites. It provides instant visibility into the security state and health of McAfee products across large numbers of endpoints and leverages an efficient architecture to avoid bottlenecks and scale visibility, updates, and control to networks of all sizes. You can gather up-to-date details about McAfee software on specific systems or groups of systems and ensure that defenses are installed, active, up to date, and enforcing the right policies. Best practice queries and an optimized design display security status for managed clients in moments. Administrators see details in context and can remediate security issues as events are happening, not after the fact. In large or complex environments, the design delivers this knowledge up to a thousand times faster than with standard McAfee ePO software.

McAfee Vulnerability Manager
Agentless McAfee Vulnerability Manager provides fast, precise, and complete insights into two basic questions about your network assets: "What do I have?" and "Is it vulnerable?" McAfee Vulnerability Manager enhances the depth of information available as you assess a situation, providing on-demand scans when needed. It integrates with McAfee ePO software so that you can correlate your findings with ways to remediate or determine if the risk needs to be mitigated. You can:

• Uncover and scan existing unknown devices and assets that may be missing scans.
• Discover and scan new, potentially noncompliant devices accessing your network in real time, between scheduled scans.
• Audit for vulnerabilities, misconfigurations, and malware and remediate based on priority.
• Provide conclusive evidence that systems are not vulnerable, so you can focus attention elsewhere.
• Identify and correlate new threats to your asset and vulnerability data.
• Audit for compliance with policies across the network, data center, and mobile devices.
• Categorize data by asset or network, filter to select and organize results in reports, and create reports while scans are running.

The McAfee Asset Manager Module is included with the purchase of McAfee Vulnerability Manager. This feature increases asset and network visibility through always-on passive discovery and monitoring. As it monitors traffic, the system will discover everything on your network, including rogue devices, forgotten VMware hosts, and mobile devices. It provides a real-time inventory, including device profiles and the identities of device users, and creates a physical network topology for each site. Hardware and software details of each new asset are stored in the McAfee ePO software inventory. As it watches, it enumerates devices, patterns, and communications—details that help you gauge and mitigate risk.

**McAfee Risk Advisor**
Many enterprises waste time patching systems when they already have a mitigating control in place. Whereas McAfee Vulnerability Manager gives visibility into your assets, McAfee Risk Advisor can tell you whether or not the asset is at risk. From the McAfee Risk Advisor global risk dashboards, you can quickly drill down to get granular details of a threat and how it relates to specific assets. A consolidated threat feed viewer shows you updated information about new and current threats from millions of collection points. In addition to threat descriptions and analyses, the threat feed supplies recommended remediations, links to threat discussion groups and notices, various risk-scoring methods, a list of applications affected, and insight into how threats affect regulatory mandates. McAfee Risk Advisor maps the threat feed to specific McAfee countermeasures that are deployed (or should be deployed) to ensure an optimized security posture. Ultimately, McAfee Risk Advisor provides a clear ROI, enabling you to focus your priorities.

**Impact of the Solution**
Better risk analysis allows for more insightful action and better security for your business. The McAfee solution for situational awareness will help your organization become sensitive to and informed of changing events as they occur. Instead of making tentative and reactionary decisions based on little data, you will take decisive action based on a clear understanding of correlated events and their implications for your infrastructure. Your organization can move from cleaning up after incidents to preventing incidents through thoughtful and timely countermeasures that mitigate an attack or a security breach. As you become more aware of your security posture, you can determine if you are at risk to present-day exploits or future attacks. Once you have analyzed your posture, the solution gives you the ability to mitigate or accept the risk with higher confidence in each decision.

**Additional Resources**
www.mcafee.com/epo
www.mcafee.com/siem
www.mcafee.com/vm
www.mcafee.com/riskadvisor
www.mcafee.com/gti

For more information about the Security Connected Reference Architecture, visit:
www.mcafee.com/securityconnected

\[\text{http://www.uscg.mil/auxiliary/training/tct/chap5.pdf}\]