Solution Brief

Security Information and Event Management and Integrated Endpoint Security

Automate attack response and analysis to shorten incident response time.

Responding to incidents as fast as possible is crucial to disrupting the attack and preventing extensive damage. Yet the entire process can take weeks and even months to complete.

- **Siloed operations make it difficult to respond quickly:** For instance, you might need to call the network team to ask them to limit communications to a compromised endpoint instead of being able to quickly take action yourself.
- **Siloed security products make investigation and forensics slow:** Collecting the necessary data and making sense of it after a breach can take a very long time. This makes it hard, if not impossible, to answer key questions such as: How did they get in? Who got exposed? Has the damage already been done?

The first step to effectively responding to an attack is identifying triggers that will begin the process. The best triggers clearly describe a suspicious or malicious behavior with enough precision that the reaction to it is clear. Triggers must also be highly accurate if they are to be relied upon for automated responses. Below are a few examples.

- **Anti-social behaviors:** Most enterprises will see activity coming from within or outside their networks which, while not immediately alarming, is clearly not related to their business. Often these behaviors are the precursors to an actual attack.
- **Password guessing:** High volumes of incorrect passwords are indicators of automated tools used by attackers to attempt to guess user credentials.
- **Network reconnaissance:** Host scans, port scans, and similar activities are equivalent to jiggling the doorknob of a house to see if it's locked. This kind of activity should only originate from trusted partners.
- **Application reconnaissance:** Attackers will often begin a campaign with a series of probes designed to understand the attack surface of their target. This activity may be seen in application logs as high volumes of requests from a host, often for resources that do not exist.

Key Advantages

- Speed time from detection to containment.
- Find both historical and current indicators of compromise.
- Automate investigations and remediation.
- Industry-leading countermeasures, intelligence, and adaptive architecture to protect against highly sophisticated attacks.
- Detect stealthy maneuvering through expansive visibility and advanced analytics.
- Prioritization and fluid response to correct breaches as quickly as possible.

intel Security

While most enterprises strive to investigate these types of events, the sheer volume can quickly become overwhelming to incident responders. Even running a simple malware scan on a likely infected host may take hours or days to get scheduled, depending on the organization's operational maturity. All the while, the malware is free to execute the attacker's payload, exfiltrating data or spreading more across the enterprise infrastructure. What's needed is a simple, automated method to stop attacks as soon as they are detected. Freezing the attack gives responders time to investigate the scope and take advanced remediation steps as required.

Better Detection with Integrated Solutions

During a breach, you need to act quickly—and you also need to make sure you don't overreact. Even after the attack is shut down, you will still need to investigate, remediate, and ensure that the threat is no longer in your environment. The combination of McAfee® Enterprise Security Manager, the foundation of the security information and event management (SIEM) solution family from Intel Security, and McAfee® Complete Endpoint Protection suites provides an integrated security framework that enables security teams to move quickly to prioritize and automate attack response and analysis so that you can compress incident response time to a minimum.

When deployed in your environment, McAfee Enterprise Security Manager integrates with McAfee Complete Endpoint Protection suite via McAfee® ePolicy Orchestrator® (McAfee ePO™) software to provide deep situational awareness to complement your existing McAfee ePO software visibility. McAfee ePO software allows administrators to categorize systems via manual or criteria-based "tags." Through the McAfee ePO software web application programming interface (API), McAfee Enterprise Security Manager can assign tags to systems in McAfee ePO software in response to triggers seen by McAfee Enterprise Security Manager, just as a McAfee ePO software administrator might do via the McAfee ePO software interface. These tags may then be used as the basis for assigning configuration profiles to assets, launching tasks on managed endpoints, or filtering dashboards and reports. Security operations can then take appropriate actions as needed, helping their organizations respond to attacks more quickly and efficiently than would be possible when relying solely on the security operation center (SOC) staff to drive incident responses.

All this allows you to:

- **Shorten time from detection to containment:** By assigning the proper tags, McAfee Enterprise Security Manager can quickly and automatically bring systems exhibiting suspicious behaviors to the attention of endpoint security operations and take appropriate response—either automated or interactive.
- **Locate stealthy malicious artifacts:** McAfee Endpoint Security Manager can look back up to six months to hunt for indicators of compromise (IoCs) in any retained network or system data. For example, it can reveal endpoints that have communicated with malware sources not previously identified, helping you locate potentially compromised systems.
- **Simplify cleanup and remediation:** McAfee Endpoint Security Manager can tag affected hosts that need to be serviced by McAfee ePO software with automated actions, such as running an aggressive scan, deploying new endpoint policies and protections, or quarantining hosts.

"Experience tells us that no single system can be 100% successful in preventing all compromises. This is especially true in today's always on, always connected world, where unsuspecting users are being targeted by social engineering and sophisticated, well-financed cybercriminals who relentlessly attack with advanced persistent threats that look to invade and exploit any security vulnerability. What is needed is a holistic approach that can leverage multiple interconnected security solutions as a single security ecosystem, providing security analysts the actionable intelligence they need to secure the modern IT environment."

—ESG Research Report, *IT Spending Intentions Survey, February 2015*

Use Cases

Below are some examples of how an integrated security framework helps enable your security team.

McAfee Host Intrusion Prevention

To contain a threat and allow time for incident response or for system managers to begin their investigation, you can configure a new tag within McAfee ePO software with a generic restrictive policy, such as "lockdown." Any systems with the lockdown tag will get a restrictive host intrusion prevention policy applied to prevent compromise of other systems. The lockdown policy can still allow Intel Security product communications, Microsoft Active Directory connections, and other bare minimum essentials (such as a ping from internal addresses and DNS capabilities). Based on correlation rules, or through event investigation within the SIEM solution, you can have McAfee ePO software manually or automatically apply the lockdown tag to a system and send the agent a wake-up call.

McAfee Data Loss Prevention Endpoint

You can use a watchlist as a filter to further investigate other activities performed by users that might indicate insider threat activity or negligence or may uncover data loss prevention (DLP) policy changes or exceptions that should be evaluated. When a DLP policy violation occurs, users can be added to a watchlist. Watchlist values can be configured to age after a period of time. For example, when a user violates a DLP policy, their user ID can be added to a watchlist for five days. You can also create a correlation rule to monitor for DLP policy violations, where the source user is also on the watchlist and to trigger a notification that a user has violated DLP rules multiple times within five days.

McAfee VirusScan® Enterprise

Identify high-risk IPs and users through a watchlist based on virus detection events. You can create a rule where any system or users that had virus detection events are added to a watchlist for a period of time (30 days, for example). Correlation rules can monitor for repeat offenders by looking at virus detection events and watchlists. Any system or user that is found to be a repeat offender can be identified as high risk, which could be a tag within McAfee ePO software. Based on the tag within McAfee ePO software, a more restrictive VirusScan policy can be applied, and more frequent on-demand scans can be run. You can also generate regular McAfee ePO software dashboards and reports for systems that have the high-risk tag applied.

McAfee ePO tagging

To simplify some of this work, you can create a group within McAfee ePO software and assign restrictive policies to that group. Multiple tags can be applied to those systems in a single SIEM action. These tags can trigger McAfee ePO software to automatically sort systems into this group. This way, not only is the system in a more restricted policy state, but also, within McAfee ePO software, it's easy to identify the systems for other types of reporting or system management. Once systems have been confirmed as "remediated," McAfee ePO software administrators can clear the tags and allow automatic sorting or manual sorting to place the system back into its normal group. Once part of the normal group, the standard policies will take place at the next agent to server communication and policy enforcement intervals.

An Efficient Solution for Improved Detection and Correction

To shorten response times and contain the largest number of threats possible, organizations need security that seamlessly integrates. Intel Security addresses this critical need through our leading technologies in endpoint and SIEM. Intel Security endpoint solutions, McAfee ePO software, and McAfee Enterprise Security Manager offer a truly connected approach to putting actionable threat information and control at the fingertips of security management teams—all with the fastest available performance to enable you to take action in real time.

Learn More

For more information visit **www.mcafee.com/siem** or **www.mcafee.com/endpoint**.

62230brf_siem-ep_0316_ETMG

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com