SOLUTION BRIEF

Advanced Threat Defense for SIEM

Compress malware detection and remediation time with advanced analytics

Finding and stopping advanced malware threats pose two very different types of problems for the security team today:

- **Challenge 1:** Accurate, in-depth analysis of unknown files and executables
- **Challenge 2:** Contextualization of file data with network traffic, reputation, system state information, security events, and other indirect indicators

Key Advantages

- Reveals and acts on deep insights into malware
- Slashes elapsed time from initial malware detection to complete security restoration
- Allows integrations and scripts to quickly identify and blacklist the domains and IP addresses where malware attacks originate
- Builds watchlists of convicted files and alerts when internal hosts attempt to download, install, or execute a convicted file
- Identifies internal systems that have previously communicated with newly identified malware sources
- Hunts back up to six months for IoCs in security and network data
- Tags affected hosts to be quarantined, scanned, or receive new endpoint policies or protections

For success, incident investigators need both a microscope—to look deep into the malware—and a radar system—to see and scope events in context. So far, two deployment models occur most frequently.

Advanced detection solutions often use some form of sandboxing technology, where suspicious files execute in an isolated virtual environment and are monitored to assess behavior for signs of malicious intent. A sandbox solution provides an essential complement to conventional signature-based inspection of known malware.

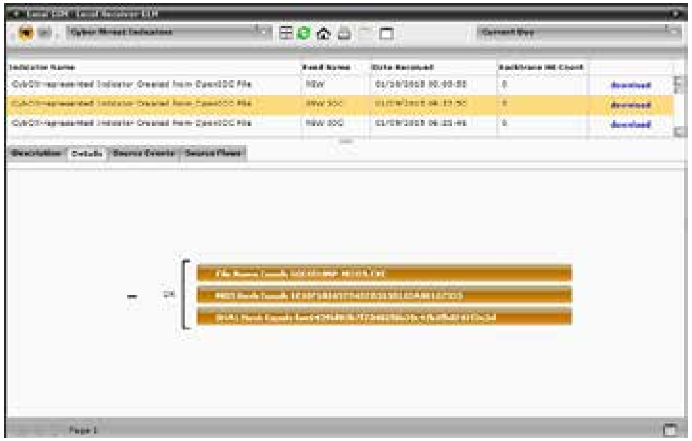
Security information and event management (SIEM) solutions collect a range of security and other data from security controls and devices throughout the environment. While initially focused on log management, modern SIEM solutions help you correlate malware findings with context, user and application data, threat intelligence, and organizational information. They provide advanced analytical tools and workflows to quickly interrogate very large data sets, identify attacks that evade front-line defenses, and trigger defensive and corrective responses. SIEM solutions help the security team answer four questions:

- Has this environment been attacked?
- What systems were affected and what was the impact?
- What must be done to secure and restore compromised systems?
- What should we look for in the future to identify similar activity?

When used together, these capabilities can enable understanding and incident response for unknown attacks. When they extract extensive data from the advanced malware, these capabilities dramatically compress time to response, both by reducing uncertainty and by accelerating processes.

Advanced Analytics: Deep Dissection Feeds Real-Time Response

McAfee provides key capabilities and integrations that significantly upgrade your options for solving these interlocking challenges. Unlike basic syslog data integrations between sandbox and SIEM, McAfee integrates rich indicator of compromise (IoC) artifacts from McAfee® Advanced Threat Defense, the industry's most powerful advanced malware detection appliance, with the correlation and advanced analytic speed of McAfee Enterprise Security Manager, an industry-leading SIEM solution.



Indicator Name	Feed Name	Date Received	Backtrace Hit Count	
CybOX-represented Indicator Created from OpenIOC File	NEW	[illegible]	0	download
CybOX-represented Indicator Created from OpenIOC File	NEW IOC	[illegible]	0	download
CybOX-represented Indicator Created from OpenIOC File	NEW IOC	[illegible]	0	download

Figure 1. Cyber Threat Manager in McAfee Enterprise Security Manager incorporates IoC data in its analysis.

Enabling an Integrated Security Framework with Data Exchange Layer

McAfee Threat Intelligence Exchange, McAfee Advanced Threat Defense, and McAfee Enterprise Security Manager leverage our proprietary data exchange layer, an ultra-fast, bidirectional communications fabric that enables information and context sharing between any connected security technologies. The data exchange layer fabric is highly scalable and provides low-latency transactions via persistent network connectivity, allowing instantaneous communication and action across any enabled device.

Products connected on the data exchange layer simply subscribe and publish to the fabric without the need for complex application programming interface (API)-based integration efforts or burdensome configurations. It marks a new era in security where all components come together to work as a single cohesive system, regardless of vendor or underlying architecture.

When McAfee Advanced Threat Defense identifies a malicious file or executable, it funnels STIX-formatted IoC artifacts to McAfee Enterprise Security Manager, which can then interpret and act on these artifacts. For both the original payload and any nested (unpacked) payloads revealed in the analysis, the data transferred includes the name, hash (MD5 or SHA-1), and severity of the convicted file, the gateway or device that first detected it, the message that carried it, the source and destination systems, and the source URL. The Cyber Threat Manager in McAfee Enterprise Security Manager incorporates this data in its correlations and analysis.

The combination of this newly derived, detailed threat data with McAfee Enterprise Security Manager's comprehensive security information repository and analytical resources enables a new level of insight, defensive options, and remediation. The security team can now:

- **Update protections:** Use integrations and scripts to quickly identify and blacklist (via updates to McAfee and third-party products) the domains and IP addresses where malware attacks originate.
- **Monitor for new, related file activities:** Create dynamic watchlists of convicted files and generate alerts when internal hosts attempt to download, install, or execute that file.
- **Backtrace for malicious artifacts:** As part of the IoC ingestion workflow, McAfee Enterprise Security Manager will look back up to six months to hunt for indications of these artifacts in any network or system data it has retained. For example, it can reveal internal systems that have previously communicated with newly identified malware sources.
- **Take action to clean up:** McAfee Enterprise Security Manager can tag affected hosts to be serviced by McAfee ePolicy Orchestrator® (McAfee ePO™) software, with actions such as running an aggressive scan, deploying new endpoint policies or protections, or quarantining hosts.

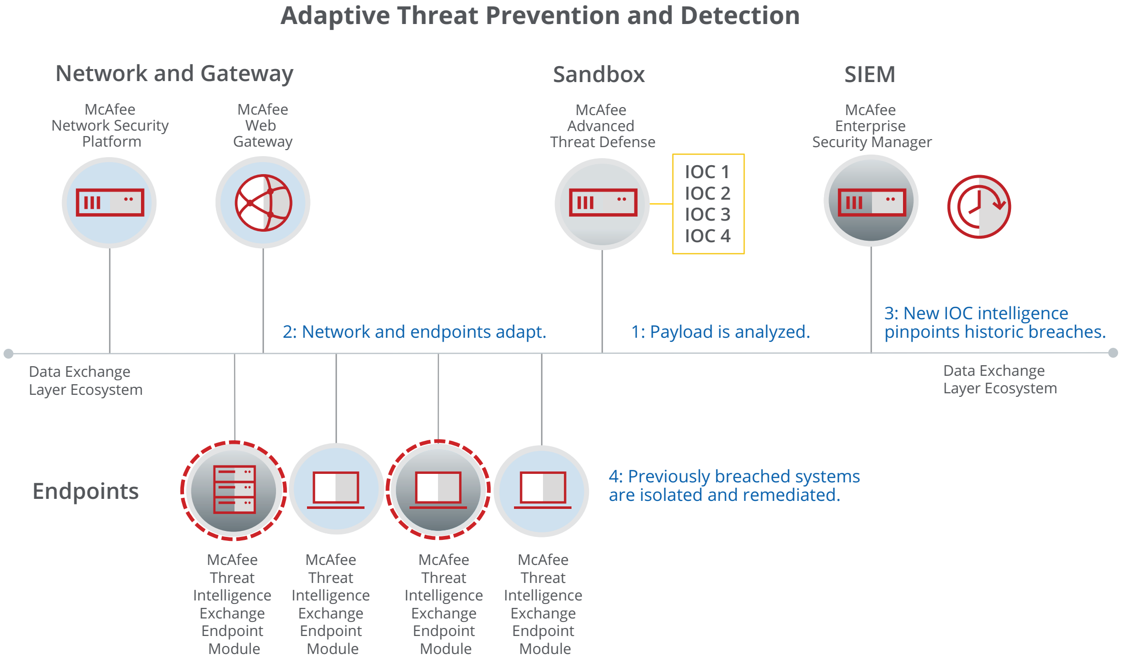

Adaptive Threat Prevention and Detection
Network and Gateway
McAfee Network Security Platform
McAfee Web Gateway
Sandbox
McAfee Advanced Threat Defense
IOC 1
IOC 2
IOC 3
IOC 4
SIEM
McAfee Enterprise Security Manager
2: Network and endpoints adapt.
1: Payload is analyzed.
3: New IOC intelligence pinpoints historic breaches.
Data Exchange Layer Ecosystem
Data Exchange Layer Ecosystem
Endpoints
4: Previously breached systems are isolated and remediated.
McAfee Threat Intelligence Exchange Endpoint Module
McAfee Threat Intelligence Exchange Endpoint Module
McAfee Threat Intelligence Exchange Endpoint Module
McAfee Threat Intelligence Exchange Endpoint Module

Figure 2. IoC artifacts derived from malware payloads can be directly used to contain and remediate threats.

By collecting, interpreting, and taking action on the detailed findings of McAfee Advanced Threat Defense, McAfee Enterprise Security Manager becomes an even more valuable part of incident management.

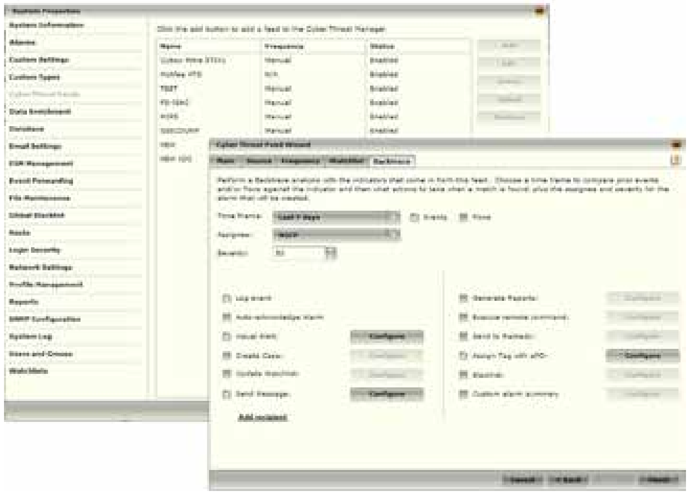


Figure 3. McAfee Enterprise Security Manager can hunt for previous instances of an IoC and initiate a customized response.

A Powerful Solution to Defend Against Emerging Malware Threats

The combination of McAfee Advanced Threat Defense and McAfee Enterprise Security Manager is the industry's most penetrating and complete file inspection solution with its most powerful platform for security information and event correlation and incident response. The result is an unparalleled ability to find emerging threats in network traffic and endpoint systems, to effectively block future attacks, and to quickly find and repair affected systems, even in the largest environment.

For more information visit **www.mcafee.com/atd**.

Integrated Security

McAfee delivers an integrated security system that helps you prevent and respond to emerging threats. Resolve more threats faster and with fewer resources through stronger protection, superior detection, and rapid correction. Our trusted on-premises and cloud-enabled solutions and services help you secure your enterprise against advanced attacks. Our connected architecture and centralized management reduce complexity and improve operational efficiency across your entire security infrastructure. McAfee is committed to being your number one security partner—providing a complete set of integrated security capabilities.

McAfee™
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

62414brf_atd-siem_0516
MAY 2016