White Paper

Advanced Targeted Attacks: It Takes a System

Real-time context sharing supports early attack detection and adaptive threat prevention.

intel Security

Table of Contents

Executive Summary

For the second consecutive year at the Black Hat Conference, McAfee, a part of Intel Security, polled security practitioners to gauge their challenges with advanced malware used in low-prevalence and targeted attacks. Despite many investments in "silver bullet" products, detection continued to lead the list of challenges. Key to detection is filtering the signal from the noise, while avoiding false positives took over as the second greatest problem for 25% of respondents. Timely protection and response continued to present major frustrations.

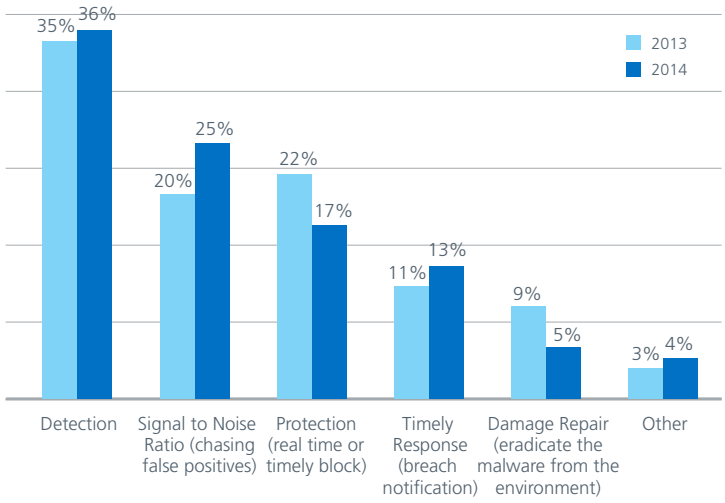

Figure 1. Black Hat attendees indicated they still have challenges defending against advanced malware.

These challenges result from insufficient integration between inspection, intelligence gathering, analytics, and enforcement elements of the security architecture. These are the technology underpinnings of the prevent/detect/respond process of incident response.

Integration improves effectiveness, as the active sharing of data and accelerated cross-control processes make it practical and possible for every security control to leverage the strengths and experiences of the others around it. It is an adaptive threat prevention model that is quickly replacing traditional, unintegrated architectures as security teams work to achieve sustainable advantage against complex threats.

Rather than treating each malware interaction as a stand-alone event, an adaptive threat prevention model integrates processes and data through an efficient messaging layer. This provides reinforcing levels of inspection and analysis informed by expanded forms of intelligence and connects end-to-end components to generate and consume as much actionable intelligence as possible from each contact and process.

The shift to adaptive threat prevention helps overcome the all-too-common functional fences that shackle detection, response, and any chance of improved prevention. Silos of data and point controls complicate operations and increase risk. For example, the data each control generates and the context of each situation are poorly captured and seldom shared. A firewall may block a payload coming from an untrusted domain because it knows about communications, not malware. It will permit that payload coming through a trusted domain. Similarly, anti-malware could block unknown payloads received from known bad addresses if it knows to think beyond the payload or look within the payload to consider IP addresses.

Unintegrated security functions like these keep organizations in a firefighting mode, always reacting and pouring human resources into each breach. Process inefficiency exhausts scarce investigative resources and lengthens the timeline in which data and networks are exposed to determined attackers. These islands of security products, data sets, and operations give sophisticated attackers ample space and white noise in which to enter, hide, and persist within your organization.

Achieving Sustainable Advantage

With McAfee® Threat Intelligence Exchange and the Security Connected platform, security professionals now have a high-performance system that integrates workflows and data to overcome siloed operations. It shifts the model from firefighting to agile, intelligence-fueled threat prevention. Global, local, and third-party threat intelligence and organizational knowledge come together to make smarter execution-time decisions, while performing deep analysis of suspicious files. By sending contextual attack insights—what we call indicators of attack (IoAs)—to cross-vector detection, containment, and remediation systems, security analysts get a sustainable advantage against advanced targeted attacks.

What Is an Indicator of Attack?
It is a unique construction of unknown attributes, IoCs, and contextual information (including organizational intelligence and risk) into a dynamic, situational picture that guides response.

By building on and integrating real-time communications into existing security investments in McAfee and third-party solutions, McAfee helps your organization cost effectively prevent compromises and close the coverage gap between encounter and containment. This paper describes four use cases for capturing the protection and cost savings offered by this cutting-edge approach using McAfee Threat Intelligence Exchange:

- Enhance endpoint effectiveness by taking action on collective threat intelligence. (integration with VirusScan® Enterprise and SiteAdvisor® Enterprise).
- Use VirusTotal integration to evaluate inputs and measurements from other anti-malware vendors to determine how you want to prosecute a given potential threat in your own environment.
- Improve advanced malware detection and response by adding dynamic sandboxing and static analytics and connecting to network components (add McAfee Advanced Threat Defense and gateway products).
- Place collective threat intelligence in the context of historic and unfolding attack sequences to act immediately: disrupt active attacks, investigate past incidents, and monitor for future events (add McAfee Enterprise Security Manager).

Building Blocks for Adaptive Threat Prevention

McAfee Threat Intelligence Exchange uses the McAfee data exchange layer, a bidirectional communication fabric enabling security intelligence and adaptive security through product integration simplicity and context sharing. McAfee Threat Intelligence Exchange collects and shares reputation information and makes protective decisions over the wire in real time. The Security Connected framework has always included automation and integration. McAfee Threat Intelligence Exchange takes advantage of the data exchange layer to change the threat prevention dynamic through contextualization of expanded intelligence and real-time orchestration throughout the environment.

Immunize and adapt, end to end.
Enterprise security teams gain local control over potential malware and threat classification, while security components share their analyses of samples instantly and upgrade their enforcement accordingly. McAfee Threat Intelligence Exchange uses the data exchange layer to knit endpoints,

gateways, and other security components into a full-fledged, advanced targeted attack defense system. You reduce risk. You create a sustainable advantage through optimized and updated protections against future attacks. And you minimize the operational costs and burdens associated with siloed protections against advanced targeted attacks.

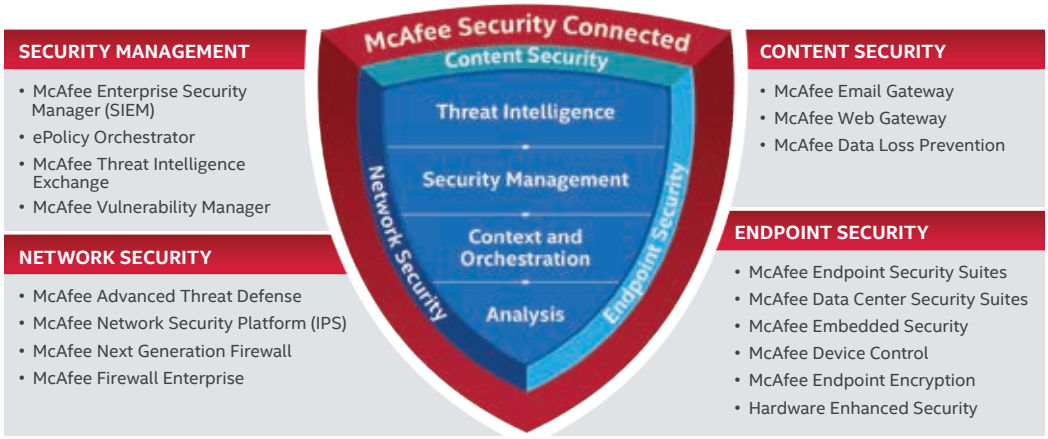

Figure 2. McAfee Threat Intelligence Exchange and the data exchange layer create a dynamic framework for sustainable advantage in the Security Connected platform.

McAfee Threat Intelligence Exchange components operate as a single collaborative system to immediately share relevant data among network, endpoint, data, applications, and other security solutions, enabling security intelligence and implementing adaptive security. McAfee Threat Intelligence Exchange closes the gap from encounter to containment for advanced targeted attacks from days, weeks, and months down to milliseconds.

Data exchange layer: Orchestrate in real time.
Integration simplicity provided through the data exchange layer reduces implementation and operational costs. Instead of integrating through low-level APIs on a one-to-one basis, the data exchange layer communications fabric allows products to integrate via a common information model that supports a variety of communications methodologies. These capabilities mean the data exchange layer supports the automatic configuration of products, reducing errors and eliminating effort.

The data exchange layer provides a real-time, bidirectional communications fabric where connected components maintain a persistent connection. Through an abstraction layer, a connection persists among endpoints, gateways, and other security components, enabling them to share intelligence in real time regardless of their location. This model means that you can broadcast security command-and-control from on-premises security controls to remote nodes in other offices, and even those behind remote devices with network address translation (NAT) capabilities, including firewalls and home gateways.

Communication security is ensured by encrypting all traffic with transport layer security (TLS), the requirement for certificate-based mutual strong authentication of all participants, and the enforcement of authorization by the fabric. This design ensures that payloads are secure and the fabric itself is protected from external attack or misappropriation.

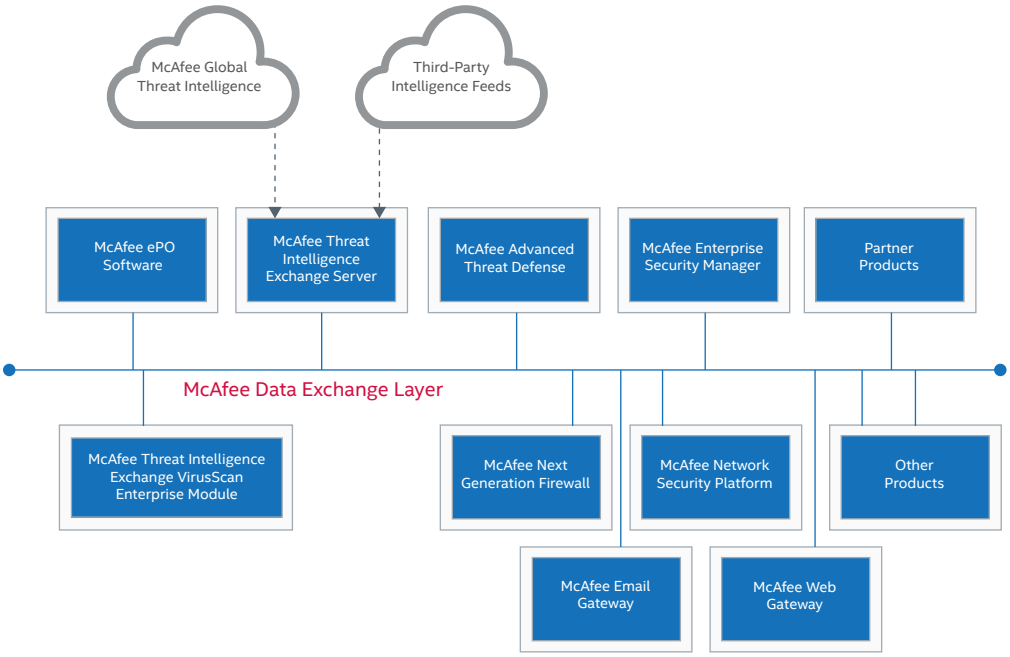

Figure 3. The data exchange layer provides a real-time communications framework that will allow security components to act as one.

McAfee Threat Intelligence Exchange: Tap the power of knowledge.
McAfee Threat Intelligence Exchange makes it possible for administrators to easily tailor and act on comprehensive threat intelligence. This is the aggregation of global intelligence data sources, such as McAfee Global Threat Intelligence (McAfee GTI), VirusTotal, and third-party feeds, plus local threat intelligence sourced from real-time and historical event data coming from endpoints, gateways, and other security components. You can assemble, override, augment, and tune the intelligence source information to drive actions in your own environment. "Smart listing" implements your own blacklists and whitelists of files and certificates, certificates assigned to and used by the organization, and more.

Aggregating and maintaining local threat intelligence enables McAfee Threat Intelligence Exchange to reflect each threat in the context of the activities and the operational environment of each organization. The metadata collected from endpoints, gateways, and security components is combined, providing visibility and enabling protective actions attuned to the threat status of your organization.

Supercharge existing endpoint protection.
While traditional advanced forensics require specialized tools and training and a lot of manual effort, McAfee Threat Intelligence Exchange turns intelligence into automated protection driven by IT's rules. McAfee Threat Intelligence Exchange provides breakthrough endpoint protection by extending VirusScan Enterprise to make local, contextual file execution decisions.

When a host attempts to execute a file:

- VirusScan Enterprise looks at its local signatures.
- If the file is unknown, the McAfee Threat Intelligence Exchange module on the host queries the McAfee Threat Intelligence Exchange Server for metadata about the file.
- The McAfee Threat Intelligence Exchange Server will query the cloud-based McAfee GTI network when no record of this file is to be found, returning the global reputation to the querying host.

- The McAfee Threat Intelligence Exchange Server will serve the query using collected metadata it already stores about this file. Included with the reply are enterprise-specific values, such as enterprise reputation, enterprise prevalence, and enterprise age.
- The McAfee Threat Intelligence Exchange module then uses rules to combine the locally observed context (file, process, and environmental attributes) and the current available collective threat intelligence to create a risk score.
- The client module applies your policies to make a decision whether or not to execute the file.
- The McAfee Threat Intelligence Exchange Server records the event in its knowledgebase.
- Should an unknown file later be determined to be malicious, VirusScan Enterprise can also be told to clean the host, which would stop a running malicious process.

Policies let you customize the level of risk tolerance on the endpoint, defining various execution conditions. For example, your policy could be as rigid as zero-tolerance for unknown or "grey" files. This just requires setting a policy that "no file is accessed unless it has a known and acceptable reputation."

Each company may have different ideas as to where on the spectrum of risk it is appropriate to allow a file, versus quarantining or deleting it altogether. That tolerance typically varies based on the class and business criticality of different systems. If the administrator later decides the file is safe, the administrator can add the blocked application to a whitelist and move on. Administrators may also decide to let users allow the file based on a prompt.

Review rich data for clarity and rapid response.

The collective threat intelligence—global, local, third-party, and manually generated—stored using the McAfee Threat Intelligence Exchange Server enables visibility, answering key questions with instant, actionable intelligence. This clarity provides conclusive evidence in time so that you can act to protect your organization; there's no need to wait for a third-party conviction and leave your organization exposed.

For example, enterprise prevalence data shows every machine that has asked about a specific file. The list of affected systems helps reveal the attacker's tactics and intent and, most importantly, shortens the window of persistence available to the attacker. Are all the machines receiving the file from a single workgroup, such as finance or software development, which could indicate what sort of confidential data the attackers are seeking? Do the systems share an application profile that could indicate zero-day vulnerabilities?

Share intelligence everywhere, instantly.

McAfee Threat Intelligence Exchange helps enterprises adapt defenses and fully contain the threat. When a McAfee Threat Intelligence Exchange client on the host decides to either block or allow execution, its decision updates the McAfee Threat Intelligence Exchange Server's records. The intelligence gleaned from each decision can be applied in several ways. McAfee Threat Intelligence Exchange will instantly publish the reputation and specifics of certain decisions to all subscribing countermeasures within the organization, including endpoint protections, gateway defenses, such as the McAfee Network Security Platform, and third-party products. This way, the full range of security products can update instantly and learn from each other, providing consistent, locally tailored protection at a rate no vendor or outside organization can match.

Since the typical sophisticated attack looks for multiple vulnerable systems, this type of advanced intelligence sharing within the environment prevents other hosts from being compromised or targeted by a specific attack. Optionally, McAfee Threat Intelligence Exchange can also forward the newly gleaned local intelligence to the McAfee GTI cloud to help other subscribers in defending against similar attacks.

What Would You Like to Know?

When an initially unknown file is later convicted, by a cloud or local intelligence source or internal investigations, McAfee Threat Intelligence Exchange server offers up actionable details on adversarial behaviors to help incident responders with live situations:

- Is this file on any of my endpoints? (Prevalence.)
- Did it execute? (Critical for discerning between infected and non-infected endpoints.)
- Where did it execute (Prioritize list of at-risk systems.)
- What was the first system "infected"? (First occurrence.)
- Which machines are likely compromised because they have executed a file now known to be malicious?
- How is the malware spreading throughout my environment? (File trajectory.)
- Where are the files that other security products are not blocking?
- Which grey files can be marked black or white?
- What is the global reputation of a certain file versus the enterprise local reputation?

What Would You Like to Know? (continued)

- How many files in the last few hours have been identified as malicious?
- How many files found in my environments are categorized as white, black, or grey?
- What percentage of the overall file population is white, black, or grey by version of the Microsoft Windows operating system found in my environment?
- What are the least prevalent files in my environment (outliers, potentially malicious)?
- Is a certain Microsoft Windows OS being specifically targeted?

The following use cases show how McAfee Threat Intelligence Exchange and the data exchange layer change the dynamics of threat detection, enhancing actionable intelligence and proactive protection, from encounter to containment.

Scenario 1: Act on collective intelligence.

The first use case allows endpoints to protect based on locally optimized threat intelligence. This customization would have allowed merchants in the VISA network to quickly implement automated protection against the hashes VISA published in 2013 for a memory parser attack.[1]

Administrators at the company now receive a bulletin and enter the new hash files into McAfee Threat Intelligence Exchange through its administration interface. Later, when a host system encounters the suspicious file, the McAfee Threat Intelligence Exchange module prevents its execution based on the customized knowledge ("these hashes are malicious") provided through the collective threat intelligence.

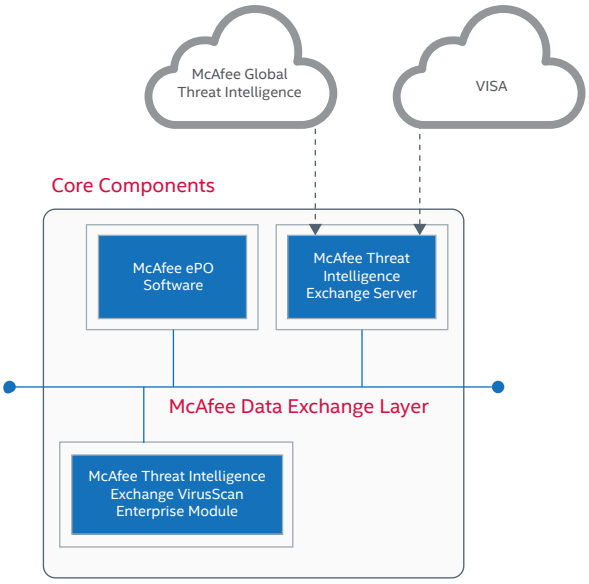

Figure 4. Third-party data can be a rich mine of intelligence.

Malware (or suspicious files) discovered by in-house teams can be blocked instantly, without submitting a sample and awaiting an antivirus signature update from the vendor. Incidents of any other endpoint encountering that file adds to a prevalence count stored in the McAfee Threat Intelligence Exchange server, knowledge that helps the administrators understand if they are under attack. The value to the organization is that an indication of compromise—a file hash in this case—can lead to a mountain of valuable intelligence that can be shared in real time.

In addition, the McAfee Threat Intelligence Exchange module will intercept on a file's attempt to execute, not simply on read or write operations. Execution protection guards against unusual behaviors. And this functionality allows McAfee Threat Intelligence Exchange to capture valuable indicators of attack (IoAs) that can be shared across the environment as they are seen. Unlike indicators of compromise (IoCs), which are individual, known bad static events, IoAs only become bad based on what they mean to you and the situation. An IoA is a unique construction of unknown attributes, IoCs, and contextual information (including organizational intelligence and risk) into a dynamic, situational picture that guides response. McAfee Threat Intelligence Exchange can detect and alert on new and unusual things in the environment that may not yet be associated with a known threat or compromise.

Scenario 2: Add McAfee Advanced Threat Defense for in-depth analysis.
An attacker who covets your enterprise data invests in subtle, obfuscating programming techniques and zero-day exploits. The resulting malware file may be unique or seen just a few times. This rarity may prevent traditional signature- or reputation-based countermeasures from accurately detecting the threat. However, if a suspicious file is not convicted through existing McAfee Threat Intelligence Exchange resources, the technology can eliminate any uncertainty by passing the file to **McAfee Advanced Threat Defense** for more in-depth analysis.

McAfee Advanced Threat Defense adds detection for advanced targeted attacks with a layered approach that leverages innovative real-time malware deconstruction capabilities, including strong unpacking that breaks through evasive techniques to expose the original executable code to determine intended behaviors. Where other sandbox providers can easily be tricked and bypassed by even simple malware coding tactics, McAfee Advanced Threat Defense combines several techniques into an industry-first: real-time static-code deconstruction with dynamic-sandboxing analysis to use attackers' obfuscation techniques against them in detection. This represents the strongest advanced anti-malware technology in the market, and effectively balances the need for security and performance.

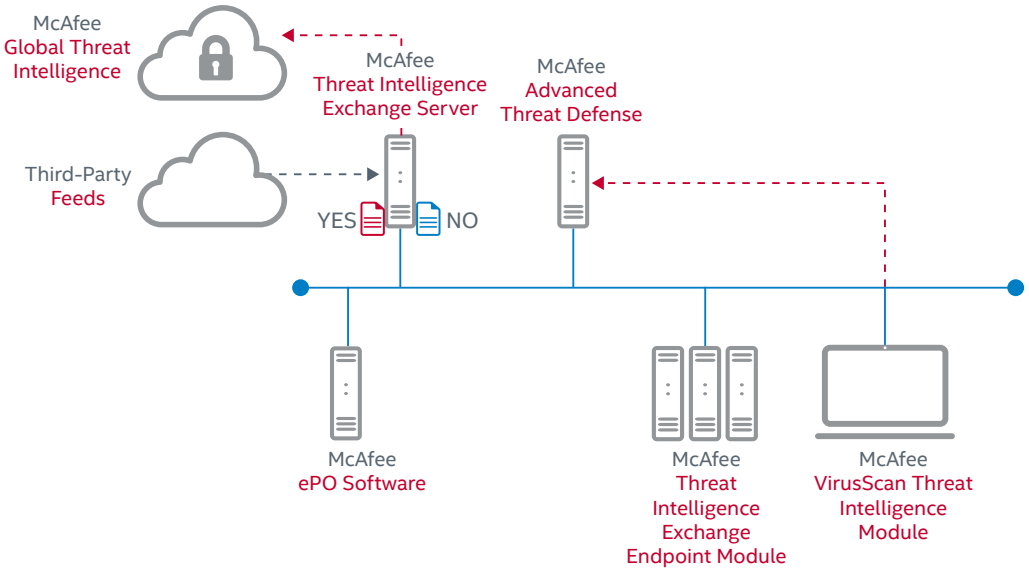

Figure 5. Intelligence and reputation synthesis from cloud, network, and endpoint.

Get endpoint-to-network and network-to-endpoint leverage.
When McAfee Threat Intelligence Exchange is used with McAfee Advanced Threat Defense, the immunization from advanced targeted attacks is more potent. You create modern threat defense in depth: a combination of behavioral, reputation, and signature-based assessment capabilities on both the network and endpoints.

McAfee endpoints can be told by policy to block payloads of "unknown" reputation, then pass the file to McAfee Advanced Threat Defense for examination and a verdict—innocent or guilty. If the file is convicted, the system publishes this conviction via a reputation update through the data exchange layer to all subscribing countermeasures within your organization. For example, McAfee

Threat Intelligence Exchange-enabled endpoints will gain proactive protection if the file attempts to execute in the future and network gateways can prevent the file from entering into the organization. Detections at network gateways cycle through this centralized analytics process and educate endpoints as well.

This intelligence and reputation sharing demonstrates the endpoint-to-network leverage of the unique Security Connected platform, such as eliminating blind spots from out-of-band payload delivery. Linking cross-vector McAfee security solutions drastically reduces the window of exposure to new malware, reduces the time to remediation, and reduces the need for network re-architecture.

Use VirusTotal integration to evaluate inputs and measurements from other anti-malware vendors to determine how you want to prosecute a given potential threat in your own environment.

Scenario 3: Detect attacks earlier with McAfee Enterprise Security Manager.
Finally, many enterprises want to harness the visibility and correlation provided by the McAfee Enterprise Security Manager for faster and better insight into the threat landscape within their environment. McAfee Enterprise Security Manager security information and event management (SIEM) can collect rich data from McAfee Threat Intelligence Exchange and McAfee Advanced Threat Defense and use its patented, high-performance database engine to correlate with log and event data from hundreds of data sources.

This expanded, fine-grained set of data lets you answer the question: "Which hosts in my environment are exhibiting behaviors that match our newly found intelligence?" as you work to understand and act against attacks. Every time McAfee Threat Intelligence Exchange identifies a new malicious event (a "first occurrence") and instructs clients to execute or block, McAfee Enterprise Security Manager can bring the event to the attention of administrators and activate mitigation workflows, such as updating endpoint policies in near real time. As they link the detect/respond/prevent processes in to a closed loop, McAfee Enterprise Security Manager workflows and watch lists turn McAfee Threat Intelligence Exchange and SIEM findings into better protection and risk management for your organization.

Replay the past, revise the future.
McAfee Enterprise Security Manager uses artifacts provided by McAfee Advanced Threat Defense and McAfee Threat Intelligence Exchange to hunt down events in McAfee Enterprise Security Manager archives and alert on related future events. This gives it the ability to turn back the clock and leverage today's newly found intelligence to identify any previous malicious interactions that may not have been known at the time.

For instance, the file hash resulting from any file-based conviction through either McAfee Threat Intelligence Exchange or McAfee Advanced Threat Defense can be loaded into an SIEM watch list. McAfee Enterprise Security Manager then uses the information stored in the watch list to compare against historical events that have been indexed or new real-time events. Because file hashes are generated by many products—not just McAfee Advanced Threat Defense, but also file integrity monitoring solutions like McAfee Change Control, host and network intrusion prevention systems, and web gateway anti-malware engines—the shared file hash increases sensitivity to activities throughout the organization. McAfee Threat Intelligence Exchange publishes the reputation out to these systems to enforce blocking, and McAfee Enterprise Security Manager provides an environment where each incident can be pieced together to create an overall, complete picture of malicious activities.

In addition to file hashes, McAfee Enterprise Security Manager leverages other IoAs generated by McAfee Advanced Threat Defense and McAfee Threat Intelligence Exchange. Both of these provide other intelligence associated with their findings, such as filenames, IP information, payload hashes, prevalence, and hostname.

Further, McAfee Advanced Threat Defense reports include even more information about files associated with the attack. When you have both McAfee Advanced Threat Defense and McAfee Enterprise Security Manager deployed, McAfee Enterprise Security Manager can filter based on bad files generated by McAfee Advanced Threat Defense and then analyze events looking for these files based on a number of characteristics. Having located the files, an investigator could then filter that subset of data further with the IP addresses and filenames also provided by McAfee Advanced Threat Defense. McAfee Enterprise Security Manager will report on all historic results specific to attributes generated by McAfee Advanced Threat Defense, and it will monitor for any subsequent events.

As McAfee Enterprise Security Manager identifies events in an attack sequence, it can trigger containment, remediation, and adaptation automatically. For instance, hosts determined to be involved could receive an immediate policy update, quarantine, or scan.

Changing the Dynamics of the Fight

These use cases show you ways to funnel the best, most complete, most actionable intelligence into your defenses and use this intelligence to drive protective action automatically. You can tie together your detection, analysis, and protections at the data and workflow layers to let them learn from each other to protect your organization better and in real time. And you can effectively understand, hunt, and eliminate threats throughout your environment—acting on live intelligence and looking into the past to protect the future.

By introducing this adaptive intelligence and real-time communications to its Security Connected Platform, McAfee changes the dynamics of the fight against advanced targeted attacks. McAfee Threat Intelligence Exchange enriches threat intelligence to construct and act on indicators of attack, while the data exchange layer adds context and orchestration to the Security Connected platform. With McAfee Advanced Threat Defense and McAfee Enterprise Security Manager, as well as the broad range of McAfee endpoint to network countermeasures, McAfee continues to deliver the industry's most comprehensive threat protection—an optimized system to achieve sustainable advantage against advanced targeted attacks.

For more information, visit:

www.mcafee.com/comprehensivethreatprotection

www.mcafee.com/incidentresponse

www.mcafee.com/exchange

www.mcafee.com/atd

www.mcafee.com/siem

About Intel Security

McAfee is now part of Intel Security. With its Security Connected strategy, innovative approach to hardware-enhanced security, and unique Global Threat Intelligence, Intel Security is intensely focused on developing proactive, proven security solutions and services that protect systems, networks, and mobile devices for business and personal use around the world. Intel Security combines the experience and expertise of McAfee with the innovation and proven performance of Intel to make security an essential ingredient in every architecture and on every computing platform. Intel Security's mission is to give everyone the confidence to live and work safely and securely in the digital world. **www.intelsecurity.com**.

1. **http://usa.visa.com/download/merchants/alert-prevent-grocer-malware-attacks-04112013.pdf**

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