White Paper

Advanced Targeted Attacks: It Takes a System

Adaptive intelligence and real-time communications orchestrate protection in the McAfee Security Connected Platform

Table of Contents

Executive summary

At Black Hat 2013, McAfee polled attendees to see where they struggled with the advanced malware used in low-prevalence and targeted attacks. While detection led the list of challenges, false positives, protection, and timely response and repair represented huge frustrations—and huge costs as well.

These challenges can be laid at the door of traditional, unintegrated, defense-in-depth designs. While you may have multiple antivirus engines and protection for each threat vector, too often these products operate in functional silos. This situation creates two problems: Cost and risk.

Unintegrated security operations remain reactive and complex, unautomated, and unoptimized. This inefficiency creates a high ongoing operational cost for security while leaving data and networks exposed to determined attackers. Unintegrated security products and operations give sophisticated attackers ample space and white noise in which to enter, hide, and persist within your organization.

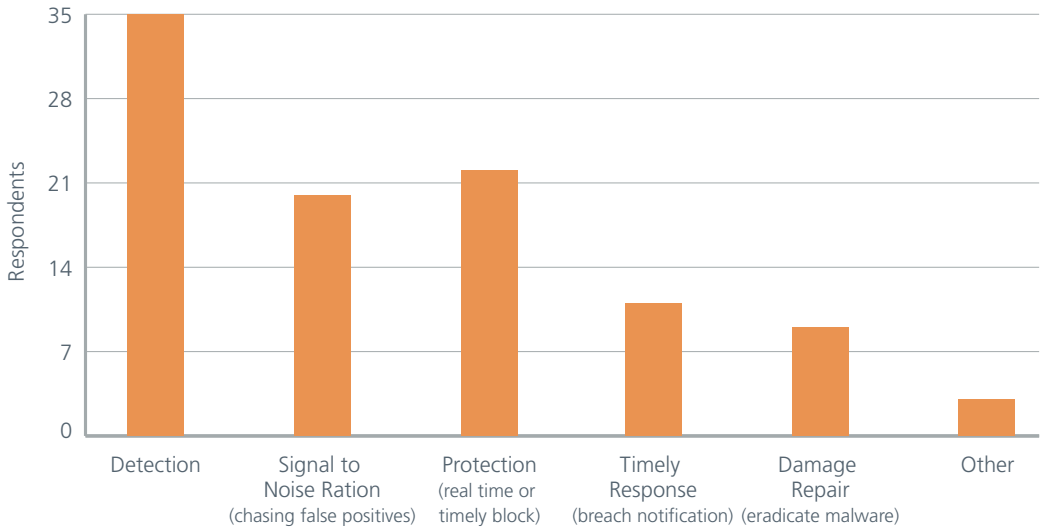

Figure 1. Advanced Malware Challenges as reported by Black Hat 2013 attendees.

Tailor collective intelligence

However, with McAfee® Threat Intelligence Exchange and the McAfee Security Connected Platform, security professionals now have a high-performance system that integrates workflows and data to overcome siloed operations and shift the model to agile, intelligent threat prevention. Integrated analysis of suspicious files from every ingress point and the inclusion of global, local, third-party, and manually entered threat intelligence provide complete, cross-vector detection, containment, and remediation of advanced targeted attacks. By building on and integrating real-time communications into existing security investments in McAfee solutions, your organization can cost-effectively prevent compromises and close the coverage gap between encounter and containment.

This paper describes three use cases for capturing the protection and cost savings offered by this cutting-edge approach:

- Take action on optimized collective threat intelligence within the endpoint environment for improving and automating cross-vector defenses and expanding endpoint effectiveness.
- Deploy with McAfee Advanced Threat Defense to add dynamic sandboxing and static analytics and connect to network components for more detection, deeper insights, and greater visibility.
- Use the McAfee Enterprise Security Manager security and information event management (SIEM) system to place the collective threat intelligence in the context of historic and unfolding attack sequences to see if your organization has been attacked in the past or is still under attack.

Building Blocks for Adaptive Threat Prevention

McAfee Threat Intelligence Exchange is the first solution to use the McAfee data-exchange layer, a bidirectional communications fabric enabling security intelligence and adaptive security through product integration simplicity and context sharing. McAfee Threat Intelligence Exchange collects and shares forensic-quality information and makes protective decisions over the wire in real time. The McAfee Security Connected strategy has always included automation and integration. McAfee Threat Intelligence Exchange with the data-exchange layer 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 can share their analyses of samples instantly and upgrade their enforcement accordingly. When added to the other comprehensive threat protection offerings in the McAfee Security Connected Platform, McAfee Threat Intelligence Exchange takes advantage of 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 optimize and elevate protections against future attacks. And you can 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 actionable intelligence in the McAfee Security Connected platform.

McAfee Threat Intelligence Exchange components operate as one to immediately share relevant data between network, endpoint, data, application, and other security solutions, enabling security intelligence and implementing adaptive security. The 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 1:1 basis, the data-exchange layer communications fabric allows products to integrate via a single API supporting a variety of communications methodologies, such as publish-subscribe, push notifications, and query-response. 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 are always on. Through an abstraction layer, a connection persists between 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 NAT'd devices, 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.

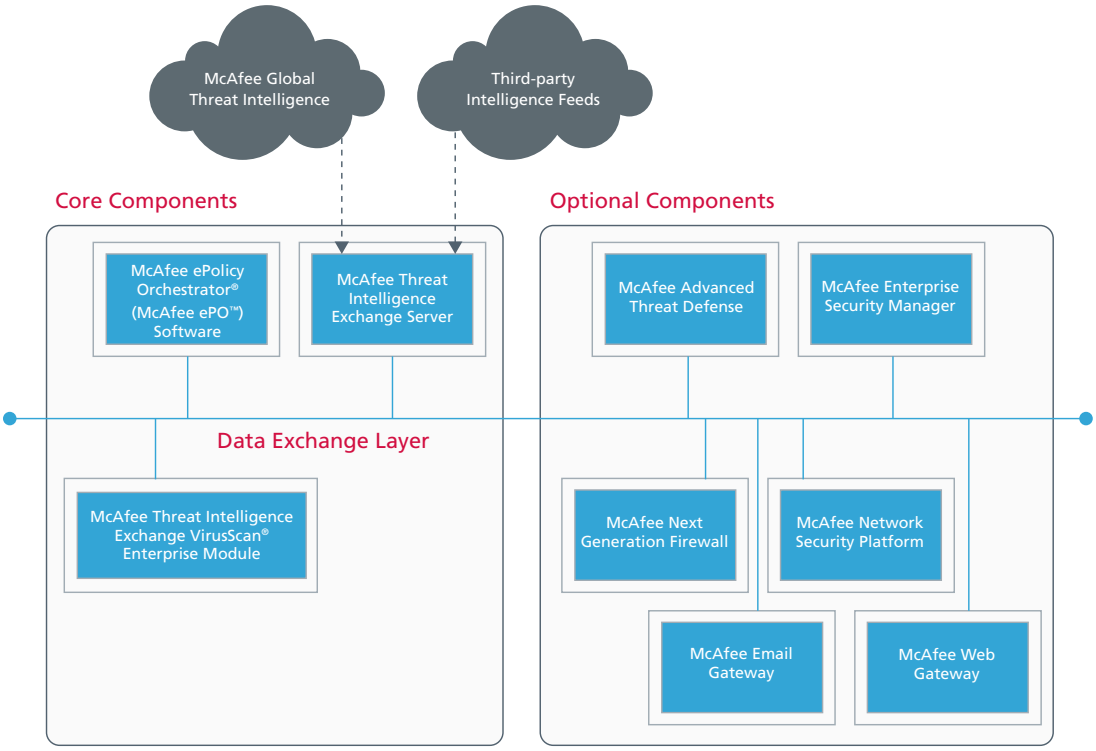

Figure 3. The data-exchange layer provides a real-time communications framework that will allow security components to act as one.

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 from global intelligence data sources, such as McAfee Global Threat Intelligence (McAfee GTI) 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. You will also be able to add custom preferences to the certificate reputation feature available in McAfee Global Threat Intelligence.

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, using a VirusScan Enterprise Threat Intelligence Exchange module to make accurate file execution decisions. A configurable rules engine provides the flexibility for variable levels of risk-tolerance based on the combined intelligence coming from local endpoint context (file, process, and environmental attributes) and the current available collective threat intelligence (organizational prevalence, age, and reputation). Endpoint defenses now have access to a rich set of security details to guide detection and protection decisions.

When a file is to be executed:

- The McAfee Threat Intelligence Exchange module queries the 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, using a configurable rules engine, would then combine the locally observed context (file, process, and environmental attributes) and the current available collective threat intelligence to make a decision whether or not to execute the file.

Rules let you customize the level of risk tolerance on the endpoint, defining various execution conditions. For example, your rule could be as rigid as zero-tolerance for unknown or "grey" files. This rule 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, later, the administrator decides the file is safe, the administrator can add the blocked app to a whitelist and move on. Administrators may also decide to let end users allow the file based on a prompt.

Review rich data for rapid response

The collective—global, local, third-party, and manually generated—threat intelligence stored using the McAfee Threat Intelligence Exchange Server enables clear visibility, answering key questions with instant, actionable intelligence. This clarity can provide conclusive evidence in time to act and protect your organization, rather than waiting for a third-party conviction and leaving the organization exposed.

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

What Would You Like to Know?

When an initially unknown file is later convicted, by a cloud or local intelligence source or internal investigations, the McAfee Threat Intelligence Exchange server can offer 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)
- What was the first system "infected"? (First occurrence)
- What other files were changed during the time close to the execution of the malware?
- 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)
- How many endpoints on my environment had elected to execute a certain file?
- Where are the files that other security products are not blocking?
- Which grey files can be marked black or white?
- Which hosts in my environment are exhibiting behaviors that match our newly found intelligence?
- What is the global reputation of a certain file vs. the enterprise local reputation?
- 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?
- What percentage of the overall file population is white, black, or grey by version of the Microsoft Windows operating system found in my environment?
- Is a certain Microsoft Windows OS being specifically targeted?

Share intelligence everywhere, instantly

McAfee Threat Intelligence Exchange helps enterprises adapt defenses and fully contain the threat. When a McAfee Threat Intelligence Exchange client 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. In this way, all security products 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, the McAfee Threat Intelligence Exchange can also forward the newly gleaned local intelligence to the McAfee GTI cloud to further help others in defending against similar attacks.

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: Customize 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 would have received the bulletin and entered the three hash files into McAfee Threat Intelligence Exchange through its administration interface. Later, when a host system encountered the suspicious file, the McAfee Threat Intelligence Exchange module would have prevented its execution based on the customized knowledge ("these hashes are malicious") provided through the collective threat intelligence.

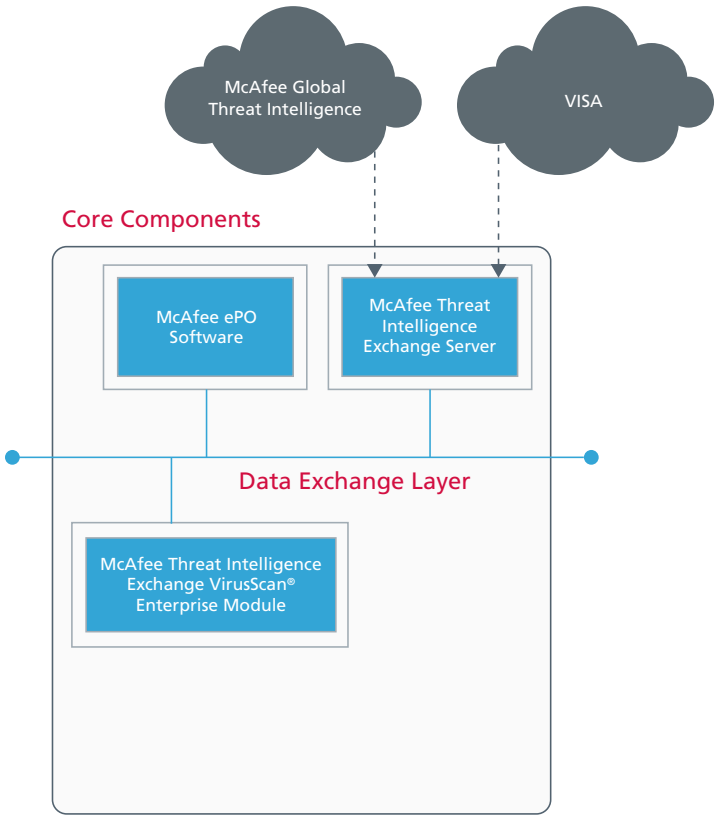

Figure 4. Third-party data can be a rich mine of intelligence.

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 would add 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, unlike standard antivirus, 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 indicator-of-compromise (IOC) information that can be shared across the environment as it is seen.

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. Therefore, where other sandbox providers can easily be tricked and bypassed by even simple malware coding tactics, McAfee Advanced Threat Defense combines an industry-first, real-time static-code deconstruction with dynamic-sandboxing analysis to use the attacker's obfuscation techniques against them in detection. Combined, this represents the strongest advanced anti-malware technology in the market, and effectively balances the need for both security and performance.

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. McAfee endpoints can delay payload delivery to prevent "patient-zero" infections while bidirectional integration with McAfee Advanced Threat Defense delivers a verdict—innocent or guilty—in real time. If the file is convicted, the system can publish this conviction via a reputation update through the data-exchange layer to all countermeasures within your organization. For example, McAfee Threat Intelligence Exchange-enabled endpoints will now have proactive protection if the file executes in the future, and McAfee Threat Intelligence Exchange-enabled gateways can prevent the file from entering into the organization.

McAfee Advanced Threat Defense also receives malware samples collected at network ingress points by other McAfee products, including McAfee Web Gateway, McAfee Email Gateway, and McAfee Network Security Platform. In turn, these network components, can share the newly-found intelligence that is gleaned from these samples over the McAfee Threat Intelligence Exchange across the environment. This intelligence and reputation sharing demonstrates the endpoint-to-network leverage of McAfee's unique Security Connected Platform. 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.

Scenario 3: Add situational awareness with McAfee Enterprise Security Manager

Finally, many enterprises will want to harness the visibility and correlation provided by the McAfee Enterprise Security Manager for gaining visual insight into the threat landscape within their environment. The McAfee Enterprise Security Manager uses a patented, high-performance database engine to collect and correlate log and event data from hundreds of data sources, including McAfee Threat Intelligence Exchange and McAfee Advanced Threat Defense. Workflows and watchlists can turn McAfee Threat Intelligence Exchange and security information and event management (SIEM) findings into better protection and risk management for your organization.

Replay the past, revise the future

The McAfee SIEM could use artifacts and IOC information provided by McAfee Advanced Threat Defense and McAfee Threat Intelligence Exchange to hunt down events in the SIEM archives and alert on future, related events. This would give 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 could be loaded into a SIEM watchlist. The SIEM could then use the information stored in the watchlist 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 could publish the reputation out to these systems to enforce blocking, and the SIEM would provide an environment where each incident can be pieced together to create an overall, complete picture of malicious activities.

In addition to file hashes, the SIEM could leverage other critical information generated by McAfee Advanced Threat Defense and McAfee Threat Intelligence Exchange. Both of these could 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 the SIEM deployed, the SIEM could 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. The SIEM will report out all historic results specific to IOCs generated by McAfee Advanced Threat Defense, and it will monitor for any subsequent events.

Change the Dynamics of the Fight

These three 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, while the data-exchange layer adds context and orchestration to the McAfee 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 fight advanced targeted attacks.

For more information, visit:

www.mcafee.com/comprehensivethreatprotection

www.mcafee.com/exchange

www.mcafee.com/atd

www.mcafee.com/siem

McAfee
An Intel Company

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

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

60945wp_it-takes-a-system_0214_ETMG