Data Sheet

McAfee Threat Intelligence Exchange

Shared threat intelligence to fight targeted attacks

McAfee® Threat Intelligence Exchange enables adaptive threat detection and response by operationalizing intelligence across your endpoint, gateway, network, and data center security solutions in real time. Combining imported global threat information with locally collected intelligence and sharing it instantly, allows your security solutions to operate as one, exchanging and acting on shared intelligence. McAfee Threat Intelligence Exchange narrows the gap from encounter to containment from days, weeks, and months down to milliseconds.

Key Advantages

- Adaptive threat protection closes the gap from encounter to containment for advanced targeted attacks from days, weeks, and months down to milliseconds.
- Collaborative threat intelligence is built out of global intelligence data sources combined with local threat intelligence gathering.
- You get immediate visibility into the presence of advanced targeted attacks in your organization.
- Relevant security intelligence is shared in real time among endpoint, gateway, network, and data center security solutions.

Create a collaborative threat intelligence ecosystem

McAfee Threat Intelligence Exchange transmits over the McAfee Data Exchange Layer to share information and provide integrated security. Combined inputs from multiple threat information sources are instantly shared with all your connected security solutions, including third-party solutions.

When security components operate as one, relevant intelligence to aid in threat detection and protection is immediately shared between endpoint, gateway, data center, cloud, and other security control points in your environment. Integration simplicity, enabled by McAfee Data Exchange Layer, significantly reduces implementation and operational costs and provides unmatched security, operational efficiency, and effectiveness.

Designed as an open framework, McAfee Data Exchange Layer enables all security solutions to dynamically join the McAfee Threat Intelligence Exchange ecosystem, including third-party security products. Total cost of ownership decreases, and you are better equipped to leverage the value of your existing security products and solutions investments with your security components now in full communication with one another.

Collaborative and adaptive threat prevention is a radical new approach to enterprise IT security, joining together your disparate systems for true security coordination. Security teams need the ability to automate the sharing of security threat information and proactively apply prevention policies and protections to all points in their network, breaking the barriers of organizational and budgetary boundaries.

By transforming the security infrastructure into a collaborative system, security administrators are able to detect, share, and immunize their environment from threats. McAfee Threat Intelligence Exchange provides a significant increase in resiliency and control in the battle against emerging and targeted attacks.

Adapt and Immunize Against Threats

Every shared insight, detected from all locations on your network, encourages deeper awareness in the battle against targeted attacks. Since these threats are laser-focused attacks by

Key Advantages (continued)

- You are empowered to make decisions on never-before-seen files, based on endpoint context (file, process, and environmental attributes) blended with collective threat intelligence.
- Integration is simplified through the McAfee Data Exchange Layer. Implementation and operational costs are reduced by connecting together Intel Security and non-Intel Security security solutions to operationalize your threat intelligence in real time.

design, organizations need a local surveillance system to capture the trends and any unique assaults they encounter. This local contextual data gathered from the encounter, combined with global threat intelligence, enables better decision making on files that have never previously been seen, resulting in faster time to protection and detection.

An unidentified file, encountered anywhere on your network, is evaluated locally by McAfee Threat Intelligence Exchange. Based on convictions, protection is propagated back out to all your systems in real time. This local threat intelligence is stored for future encounters, meaning that if it is seen again on another device or server, it will no longer be an unknown, but will be immediately detected.

For example, information on a malicious file encountered at your gateway is sent via the McAfee Data Exchange Layer to McAfee Threat Intelligence Exchange, reaching your endpoints and data center in milliseconds, so they have the information required to proactively immunize against this threat. A blocked compromise attempt on an endpoint reveals malware, and this information is shared instantly, reaching gateway and other security components, sealing the perimeter against the threat.

Operationalize Threat Intelligence in Real Time

Now you can combine threat intelligence from imported global sources, such as McAfee Global Threat Intelligence (McAfee GTI), third-party threat information, and shared indicators of compromise (IoCs), such as Structured Threat Information eXpression (STIX) files. McAfee Global Threat Intelligence collects local real-time and historical data from endpoints, data center, gateways, your network, and the McAfee Advanced Threat Defense sandboxing solution. This combined global and local threat data is operationalized and shared across your entire security ecosystem in real time.

McAfee Threat Intelligence Exchange makes it possible for administrators to easily tailor comprehensive threat intelligence from global sources, such as McAfee GTI, third-party data and imported STIX files. This is combined with local threat intelligence sourced from real-time and historical event data delivered from endpoints, gateways, sandbox solutions, and other security components. Security administrators are empowered to assemble, override, augment, and tune the comprehensive intelligence information to customize protection for their environment and organization, including, blacklists and whitelists of files or certificates assigned to and used by the organization.

This locally prioritized and tuned threat information provides instant response to any future encounters. Descriptive metadata about key objects are maintained and reflected in the collective intelligence. Administrators and security information and event management (SIEM) products can collaborate based on insight gathered to instantly identify systems with a high chance of being compromised based on past malicious activity.

Get Cutting-Edge Endpoint Protection

McAfee Threat Intelligence Exchange provides innovative endpoint prevention through the use of a McAfee Threat Intelligence Exchange VirusScan® Enterprise Module. By using configurable rules, the module makes accurate file execution decisions and leverages the combined intelligence from local endpoint context (file, process, and environmental attributes) and the current available collective threat intelligence (for example, organizational prevalence, age, reputation, and more).

When you customize the McAfee Threat Intelligence Exchange VirusScan Enterprise Module based on your organization's level of risk tolerance at the endpoint, administrators get the flexibility to set execution conditions driven by their specific requirements. This can be as rigid as adhering to a zero-tolerance policy for unknown or "grey" files and by setting rules that no file is accessed unless it has a known and acceptable reputation.

Manage Endpoints Anytime, Anywhere

McAfee Threat Intelligence Exchange provides adaptive threat prevention and security manageability with a global reach. It reaches endpoints no matter where they are and provides the means for management of threat policy, detections, and security

Advanced Targeted Attacks Are a Real-World Challenge

Designed to thwart detection and to establish a lasting foothold in an organization that is exfiltrating high-value data, advanced targeted attacks continue to plague organizations. According to data recently released as part of the *Verizon 2015 Data Breach and Investigations Report,* 70% to 90% of malware samples are unique to a single organization, indicating that detection of unique threat indicators is today's biggest challenge.[1]

For more information, visit **mcafee.com/TIE.**

updates and remote investigation. Security components operate as one, regardless of physical boundaries. They immediately share relevant security data among endpoint, gateway, and other security products—regardless of location—enabling adaptive threat prevention.

Other security management solutions are unable to immediately push policy changes, content, and program updates to the endpoints. This leaves an open window when organizations are exposed to increased risk. By utilizing McAfee Data Exchange Layer, McAfee Threat Intelligence Exchange can maintain a persistent connection, regardless of network obstacles. It effectively closes this risk gap and ensures that no endpoint is left behind.

Benefit from Collaboration

One-click reputation query

Upon encountering an unknown file by any of the security components in your organization—gateway, endpoint, or network—reputation can be easily determined based on attributes and your composite threat intelligence.

Advanced threat analytics

If more information on a file is needed, it can be sent automatically from McAfee Threat Intelligence Exchange to McAfee Advanced Threat Defense to immediately gain additional insight to potential new threats. Together, they leverage the threat analytics from static and dynamic code analysis to determine the reputation of a file in question. All of this is automated, documented, and collectively shared via McAfee Data Exchange Layer to protect your entire security ecosystem.

Security event management

McAfee Enterprise Security Manager enables you to dig deeper when investigating IoCs identified by McAfee Threat Intelligence Exchange. Access to historical security information and the ability to create automated watch lists increase the security efficiency for organizations.

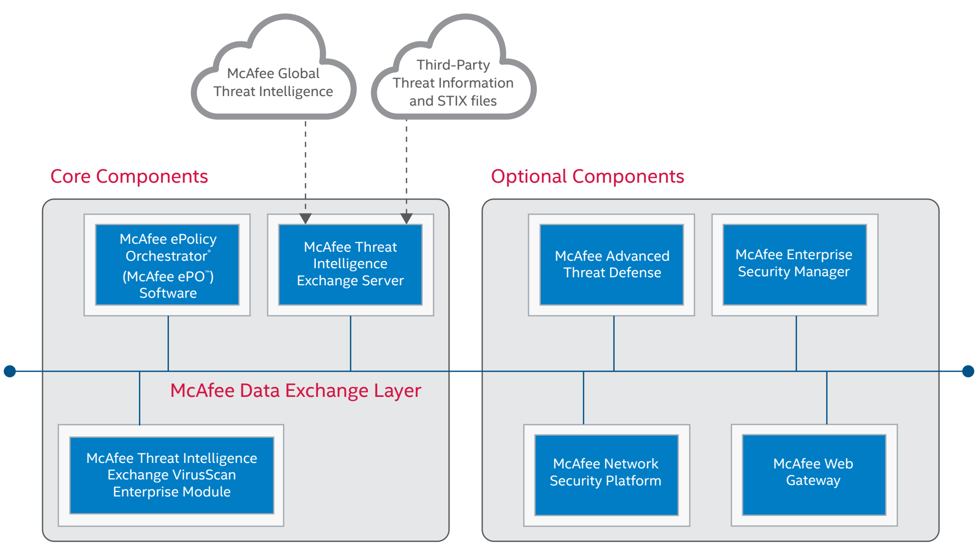

Figure 1. Integration simplicity through McAfee Data Exchange Layer reduces implementation and operational costs and enables unmatched operational effectiveness while advancing the Security Connected platform evolution.

1. http://www.verizonenterprise.com/DBIR/2015/

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