McAfee Threat Intelligence Exchange

Shared threat intelligence across security solutions

McAfee® Threat Intelligence Exchange acts as a reputation broker to enable adaptive threat detection and response. It combines local intelligence from security solutions across your organization, with external, global threat data, and instantly shares this collective intelligence across your security ecosystem, enabling solutions to exchange and act on shared intelligence.

Create a Collaborative Threat Intelligence Ecosystem

A reputation broker, McAfee Threat Intelligence Exchange combines threat intelligence from imported global sources, such as McAfee Global Threat Intelligence (McAfee GTI) and third-party threat information (such as VirusTotal) with intelligence from local sources, including endpoints, gateways, and advanced analysis solutions. Using Data Exchange Layer (DXL), it instantly shares this collective intelligence across your security ecosystem, allowing security solutions to operate as one to enhance protection throughout the organization.

Integration simplicity, enabled by DXL, significantly reduces implementation and operational costs of numerous direct application programming interface (API) integrations and provides unmatched security, operational efficiency, and effectiveness. Designed as an open framework, DXL enables all security solutions to dynamically join the McAfee Threat Intelligence Exchange ecosystem, including third-party security products.

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 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.

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.
- Relevant security intelligence is shared in real time among endpoint, gateway, network, and data center security solutions.
- 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 DXL. Implementation and operational costs are reduced by connecting together McAfee and non-McAfee security solutions to operationalize your threat intelligence in real time.

When an unidentified file is encountered anywhere on your network, McAfee Threat Intelligence Exchange is contacted to determine if a reputation exists on the file. Descriptive metadata, such as organizational prevalence and age, are also maintained and reflected in the collective intelligence. In addition to requesting reputations, integrated security solutions can also contribute reputation updates to McAfee Threat Intelligence Exchange based on local convictions. Updated reputations are then propagated 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.

McAfee Threat Intelligence Exchange makes it possible for administrators to easily tailor threat intelligence. Security administrators are empowered to assemble, override, augment, and tune the comprehensive intelligence information to customize protection for their environment and organization. This locally prioritized and tuned threat information provides instant response to any future encounters.

Enforcement Points Enhance Protection

Integrated solutions throughout the network—from endpoint to network edge—apply policy based on available reputation, metadata, or a combination of data points. One tightly integrated solution, McAfee Endpoint Security, leverages the combined local intelligence (file metatdata, such as organizational prevalence and age, along with local reputation delivered from other security components) and the current available global threat intelligence to make accurate decisions. For example, a custom application with no global reputation but high organizational prevalence would not generate a malicious composite reputation and most likely would be allowed to run. On the other hand, a file not seen before in the organization, with no global or local reputation and packed suspiciously, would most likely generate a low trust level, initiating a possible block or requiring further investigation through additional McAfee Endpoint Security engines or sandboxing through McAfee Advanced Threat Defense or McAfee Cloud Threat Detection.

Real Protect, the machine-learning capability of McAfee Endpoint Security, and Dynamic Application Containment further enhance endpoint detection and protection. Real Protect performs cloud lookups of the latest threat intelligence with pre- and post-execution analysis, while Dynamic Application Containment prevents malicious activity on the endpoint, protecting the first machine exposed to a new threat, while additional analysis is performed.

Advanced Targeted Attacks Are a Real-World Challenge

Designed to thwart detection and to establish a lasting foothold in an organization, advanced targeted attacks continue to plague organizations and exfiltrate high-value data. 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**.

Benefit from Collaboration

Advanced threat analytics

If more information on a file is needed, it can be sent automatically from McAfee Threat Intelligence Exchange to McAfee advanced analysis solutions—like McAfee Advanced Threat Defense or McAfee Cloud Threat Detection—to immediately gain additional insight to potential new threats and determine the reputation of a file in question. All of this is automated, documented, and collectively shared via DXL to protect your entire security ecosystem.

Security event management

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

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

McAfee
Together is power.

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