McAfee
An Intel Company

McAfee Threat Intelligence Exchange

Delivering adaptive threat prevention in real time

McAfee® Threat Intelligence Exchange enables adaptive threat prevention by sharing relevant security data across endpoints, gateways, and other security products. Sharing of data allows these products to operate as one, exchanging and acting on collective threat intelligence. By delivering a cohesive framework where security products collectively pinpoint threats and expose threat trends within an organization, McAfee Threat Intelligence Exchange significantly optimizes threat prevention. McAfee 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.
- Provides collective threat intelligence built out of global intelligence data sources combined with local threat intelligence and customized organizational knowledge.
- Brings immediate visibility into the presence of advanced targeted attacks in your organization.
- Security components operate as one, sharing relevant security data in real time between endpoint, gateway, and other security products enabling adaptive security.
- Cutting-edge endpoint protection technology determines file-execution decisions with rule-based logic based on endpoint context (file, process, and environmental attributes) blended with collective threat intelligence.
- Integration simplicity through the McAfee data-exchange layer reduces implementation and operational costs and enables unmatched operation effectiveness advancing the evolution of the McAfee Security Connected Platform.

With McAfee Threat Intelligence Exchange, security teams gain actionable insights and security management efficiencies through the real-time exchange of threat intelligence. We know that revealing a threat is most useful if you can take actions against it. McAfee Threat Intelligence Exchange automatically blocks threats that are determined to be risky to your organization. Leveraging your security detection, prevention, and analytics technology, an investment in McAfee allows the orchestration of adaptive threat prevention across the entire organization while significantly reducing total cost of ownership. The result is a unified threat defense system that is customizable and easily deployed, providing resilience and immunity to infections.

If You See Something, Say Something

McAfee Threat Intelligence Exchange is the first solution to make use of the McAfee data-exchange layer that promotes security intelligence and adaptive security through product integration and context sharing. When components operate as one, they immediately share relevant data between endpoint, network, security applications, and other security components. Integration simplicity, enabled by the data-exchange layer, significantly reduces implementation and operational costs and provides unmatched security, operational efficiency, and effectiveness.

Designed as an open framework, the data-exchange layer enables security components to dynamically join the McAfee Threat Intelligence Exchange. Every shared insight encourages deeper awareness of the battle against targeted threats. 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.

Apply the Power of Knowledge

McAfee Threat Intelligence Exchange makes it possible for administrators to easily tailor comprehensive threat intelligence from global intelligence data sources. These can be McAfee Global Threat Intelligence (McAfee GTI) or third-party feeds, with local threat intelligence sourced from real-time and historical event data delivered via endpoints, gateways, and other security components. Customers are empowered to assemble, override, augment, and tune the intelligence source information so that they can customize data for their environment and organization (for example, blacklists and whitelists of files and certificates or certificates assigned to and used by the organization).

The Threat Intelligence Exchange Server reflects the current threat state across your organization. Descriptive metadata about key objects are maintained and reflected in the collective intelligence

Advanced Targeted Attacks: 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 2013 Data Breach and Investigations Report*, in 80% of cases a breach went undetected for weeks. Once a detection was made, it took days to contain the threat in 79% of the cases.

For more information, visit mcafee.com/TIE

gathered. 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.

McAfee Threat Intelligence Exchange brings immediate visibility into the presence of advanced targeted attacks by automatically assembling events and valuable context as communicated from the endpoints, gateways, and other security components. Every new event is transformed into actionable intelligence guiding investigations and timelines. Protection effectiveness, detection, and analysis capabilities are increased when multiple intelligence sources are used.

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, etc.).

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 by setting rules that no file is accessed unless it has a known and acceptable reputation.

Endpoint Protection and Management Anywhere, Anytime

McAfee Threat Intelligence Exchange provides adaptive threat prevention and security manageability with a global reach. McAfee Threat Intelligence Exchange reaches endpoints no matter where they are and provides the means for management of threat policy, detections, and security updates and remote investigation. Security components operate as one, regardless of physical boundaries. They immediately share relevant security data between 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 the McAfee data-exchange layer, McAfee Threat Intelligence Exchange has the ability to maintain a persistent connection regardless of network obstacles. It effectively closes this risk gap and ensures that no endpoint is left behind.

Adapt and Immunize Against Threats

Adaptive threat prevention is a technology breakthrough, leapfrogging beyond loose integrations as a means for security coordination. Security teams need the ability to automate security threat information and proactively apply prevention policies and protections if they want to break the barriers of organizational and budgetary boundaries. By joining 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 threats. From a security standpoint, the total cost of ownership decreases and you're better able to leverage the value of your existing McAfee security detection, prevention, and analytics technology investment. Plus, your security components now operate as one.

Now, an encounter of recently-identified malware at a network gateway can propagate through the data exchange layer in milliseconds, reaching all of the endpoints so they have the information needed to proactively immunize against this threat. A blocked compromise attempt on an endpoint that reveals malware can be shared through the data-exchange layer, reaching gateway and other security components sealing the perimeter against the threat. Endpoints are protected based on malware detected by network gateways, while network gateways block access based on endpoint convictions.

Collaboration Benefits

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. Single-click integration to VirusTotal and McAfee GTI will return immediate results.

Advanced threat analytics

McAfee Threat Intelligence Exchange coordinates with 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 through the data exchange so you can extend the depth of threat prevention by adding advanced threat analytics to comprehensive threat intelligence.

Security event management

McAfee Enterprise Security Manager provides the additional tool to dig deeper when investigating indicators of compromise determined from McAfee Threat Intelligence Exchange. Access to historical security information and the ability to create automated watch lists increase the security efficiency for organizations.

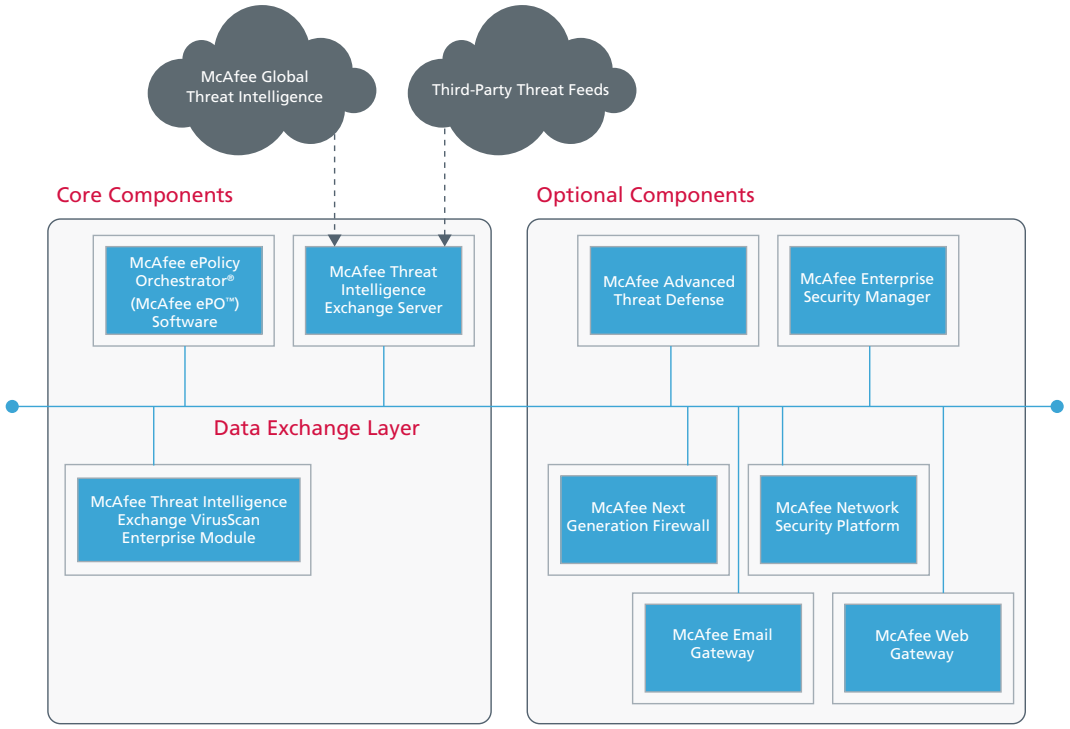

Figure 1. Integration simplicity, through the McAfee data-exchange layer, reduces implementation and operational costs and enables unmatched operational effectiveness while advancing the McAfee Security Connected Platform evolution.

McAfee
An Intel Company

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

60943ds_threat-intelligence-exchange_0214_fnl_ETMG