Solution Brief

McAfee Threat Intelligence Exchange and Endpoint Protection

Get cutting-edge endpoint visibility, control, and protection.

Organizations face a variety of security and operational challenges in the face of today's emerging threats. Effective protection from ultra-low prevalence attacks, conclusive visibility on file executions, and the ability to investigate and respond to encounters are increasingly difficult endeavors. While traditionally layered, defense-in-depth endpoint protection approaches help disrupt the attack lifecycle, individual security components typically work alone in operational silos. This produces a fragmented security picture with limited contextual knowledge that ultimately leads to incomplete visibility, less effective protection, slower responses, and excessive demands on already taxed IT resources.

Effective protection against emerging threats requires security solutions that cohesively work together to identify stealthy attacks and to immediately respond—without requiring manual correlation, time-intensive policy changes, or traditional endpoint update mechanisms. The key is the ability to separate ongoing background noise of legitimate new files from stealthy, low-prevalence attack payloads executing in the environment. Also key is the ability to then share learned insights to adapt immediately across the IT infrastructure. To achieve this, security solutions must not only filter out known good and bad objects but also evaluate unknown executable files to determine an overall reputation risk score. Through understanding a file's reputation, appropriate actions can be made to thwart threats.

McAfee® Threat Intelligence Exchange delivers this innovative endpoint protection with a system that adapts and learns from encounters and immediately neutralizes emerging threats. With it, you can easily tailor comprehensive threat intelligence from multiple data sources. Plus, systems now share intelligence, learn from each other, and get collectively stronger. Local customization empowers you to assemble, override, and tune the intelligence source information, so you can modify protection for your environment and organization.

Key Advantages

Instant, adaptive protection
Neutralize emerging threats in milliseconds through a self-updating security infrastructure that shares learned insights instantly for faster, more effective protection.

The power of knowledge
Accurately determine a file's reputation through diversified global and local intelligence analysis from multiple sources including McAfee Global Threat Intelligence (McAfee GTI), VirusTotal, and locally-derived reputation insights specific to your environment.

Visibility and control
Gain insight into every executable that runs in your environment to understand where threats are attempting to gain a foothold, investigate point of origin, and isolate exposure with precision and speed.

intel Security

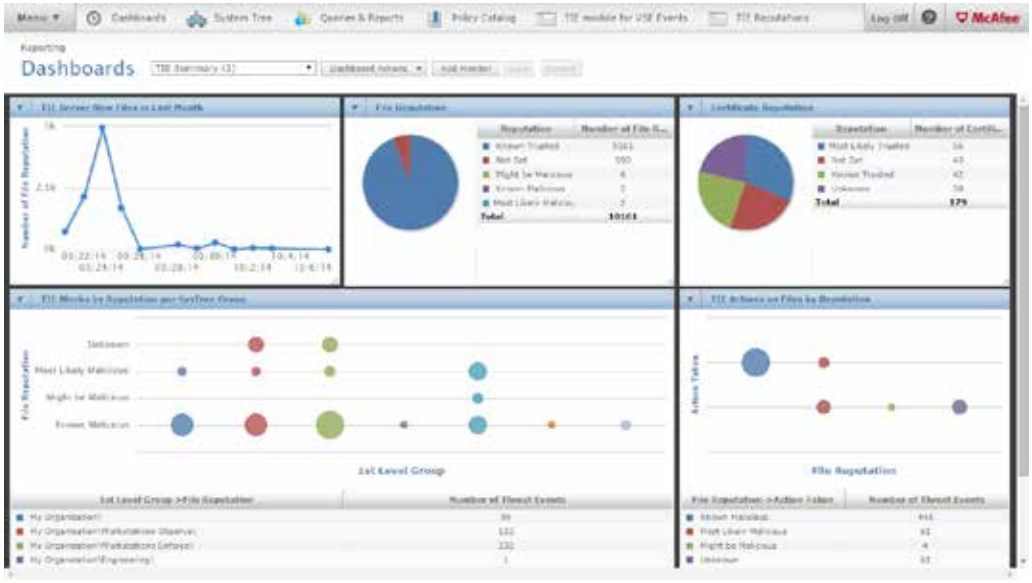

Figure 1. McAfee Threat Intelligence Exchange actionable dashboard.

Close the Exposure Gap

Advanced protection

McAfee Threat Intelligence Exchange delivers a new kind of endpoint protection that identifies potential risks from the background noise of known good and bad files. Performing an in-depth analysis of suspect files using local, global, and enterprise-level intelligence, smart execution-time decisions are made to identify and convict both low-prevalence attacks and stealthy malware. Conviction precision is further refined through advanced logic that analyzes an array of execution and file characteristics, such as the location a file is executing, suspicious metadata, or if the file has been packed in an attempt to obfuscate it.

Comprehensive threat intelligence

McAfee Threat Intelligence Exchange integrates multiple threat data sources, including McAfee Global Threat Intelligence, third-party vendor results from VirusTotal, and local knowledge specific to your environment to accurately determine a file's reputation risk score.

Instantaneous architecture

Instantly adapt to threats as the insights from a single encounter are propagated to all endpoints through the data exchange layer, without the need to submit a sample or wait for an antivirus signature update. Completely automate the adaptive response for a closed-loop process or use it interactively to protect against malware, high-risk files, or simply unwanted applications. The end result drastically reduces the time to contain and remediate emerging threats.

Incident response knowledgebase

McAfee Threat Intelligence Exchange stores historic details on file reputation and execution to investigate and respond to low prevalence attacks, suspicious files, and general threats. Quickly identify where a threat exists in your environment and how it has spread, as well as identify the first or only instance of a payload "patient zero."

Key Advantages Continued

Dramatically reduced TCO

Disparate collections of security technologies are transformed by McAfee Threat Intelligence Exchange into a single coordinated system with decreased complexity, instantaneous speed, and illuminated knowledge to drive lower operating costs, streamline protection and response, and shift valuable security team resources away from tactical fire drills towards strategic priorities.

Enabling Security Connected—Data Exchange Layer

McAfee Threat Intelligence Exchange leverages the data exchange layer (DXL), an ultra-fast, bidirectional communications fabric that enables information and context sharing between any connected security technologies. The DXL fabric is highly scalable and provides low-latency transactions via persistent network connectivity, allowing instantaneous communication and action across any enabled device. Products connected on the data exchange layer simply subscribe and publish to the fabric without the need for complex API-based integration efforts or burdensome configurations. It marks a new era in security where all components come together to work as a single cohesive system, regardless of vendor or underlying architecture.

Flexible control
Easily tune, override, and import reputation results and conviction actions to take complete control of your environment. For example, file reputations can be classified locally to immediately override and adjust how files are treated. Policies can be tailored across groups and systems to provide a broad spectrum of enforcement that is aligned with asset criticality. Additionally, insights from third-party tools can be easily imported to take action across the entire environment.

Simplified deployment and management
Integration between McAfee Threat Intelligence Exchange, McAfee VirusScan® Enterprise Module software, and McAfee ePolicy Orchestrator® (McAfee ePO™) software is seamless. The data-exchange layer supports automatic product configuration, thereby reducing errors and eliminating extensive manual effort.

Security connected ecosystem
McAfee Threat Intelligence Exchange connects your disparate security components to share contextual insights and deliver adaptive threat protection. Providing an extendable security connected ecosystem that integrates advanced threat analysis with network, gateway, and endpoint solutions, McAfee Threat Intelligence Exchange leverages all available countermeasures to neutralize threats.

Figure 2. McAfee Threat Intelligence Exchange solution process.

Learn More

McAfee Threat Intelligence Exchange provides greater scrutiny of grey files and local endpoint administrative control to quickly make decisions on how to handle them. Providing a security ecosystem that integrates advanced threat analysis, network products, and endpoint solutions, McAfee provides organization-wide visibility and context for threats, while reducing response time and simplifying remediation.

- **http://www.mcafee.com/TIE**
- **http://www.mcafee.com/us/products/virusscan-enterprise.aspx**

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