Solution Brief

Security in Unison

Adaptive intelligence enables you to respond immediately to emerging threats.

Organizations face multiple security and operational challenges as they attempt to mount an effective defense against today's emerging threats. Zero-day and advanced targeted attacks use payloads that have never been seen before. Polymorphic malware threats also pose similar challenges. On their own, traditional, signature-based countermeasures have difficulty detecting advanced malware payloads.

To effectively combat emerging threats, organizations need a security system that provides a combination of behavioral, reputation, and signature-based assessment capabilities on both the network and endpoints. While each of these technology layers might do a good job identifying threats individually, it's important that they work together to share insights, gain knowledge, and adapt in unison to address evolving threats. Time-consuming manual communications between network and endpoint solutions simply aren't fast enough to counteract today's threats.

McAfee® Threat Intelligence Exchange and McAfee Advanced Threat Defense work collaboratively to deliver automated, adaptive protection from emerging threats. Regardless of the first point of contact from an unknown malware file, once it is convicted, the entire connected environment is updated immediately. If a file is convicted by McAfee Advanced Threat Defense, McAfee Threat Intelligence Exchange will publish this conviction via a reputation update through the data exchange layer to all countermeasures within the organization. McAfee Threat Intelligence Exchange-enabled endpoints will have proactive protection if the file appears in the future. McAfee Threat Intelligence Exchange-enabled gateways prevent the file from entering the organization. Additionally, when McAfee Threat Intelligence Exchange-enabled endpoints encounter files with unknown reputations, they are submitted to McAfee Advanced Threat Defense to determine whether the object is malicious, eliminating blind spots from out-of-band payload delivery.

Close the Exposure Gap

Identify stealthy malware payloads.

McAfee Threat Intelligence Exchange and McAfee Advanced Threat Defense work collaboratively to analyze suspect objects, regardless of the point of first contact. As new files attempt to execute, they are subject to the combined endpoint rules, environmental and global reputation knowledge, and in-depth static and dynamic interrogation from the connected components in this collaborative solution. This connected approach to threat analysis yields more precise identification of stealthy malware that could otherwise go undetected.

Key Benefits

- Dramatically reduce time to containment through automated, adaptive threat response.
- Achieve greater visibility, agility, and control via network-to-endpoint collaboration.
- Respond intelligently to encounters with conclusive file reputation and execution knowledge.
- Improve security while optimizing TCO, thanks to simplified integration and implementation.

intel Security

Boost threat detection with behavior-based threat analysis.
McAfee Advanced Threat Defense provides reputation classification with innovative malware deconstruction capabilities, including strong unpacking that breaks through evasive techniques to expose the original executable code to determine intended behaviors. Together, static code and dynamic analysis provide a complete evaluation and represent the strongest advanced threat detection technology in the market.

Get visibility and control, from the endpoint to the network.
McAfee Advanced Threat Defense also receives malware samples collected at network ingress points by other products in your environment. In turn, these network components can share the newly found intelligence that is gleaned from these samples over the McAfee Threat Intelligence Exchange. This intelligence and reputation sharing demonstrates the endpoint-to-network leverage of the Security Connected platform from McAfee. Additionally, McAfee Threat Intelligence Exchange maintains a knowledgebase that indicates where the last objects in the endpoint environment have executed to deliver conclusive visibility of encounters.

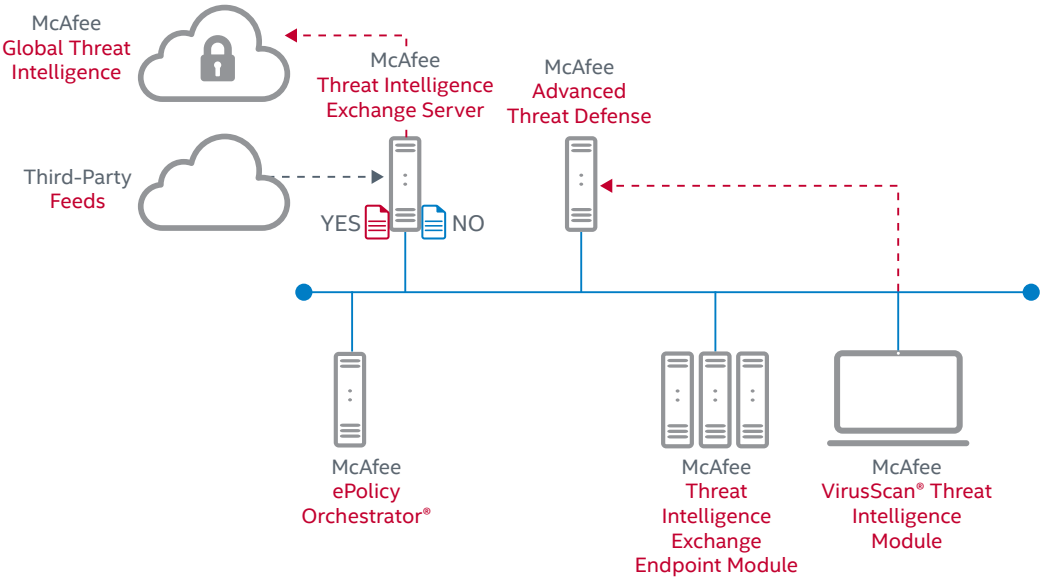

Figure 1. Intelligence and reputation synthesis from cloud, network, and endpoint.

Adaptive Response

Once McAfee Advanced Threat Defense analyzes and classifies a file, the results are sent to McAfee Threat Intelligence Exchange. The new file reputation, whether good or bad, is published instantly to all of the McAfee Threat Intelligence Exchange-enabled countermeasures in the environment. Any future instance of the file will be understood, and all McAfee Threat Intelligence Exchange-enabled components take action according to policy to allow, block, or clean. This adaptive response provides instant protection across the entire environment, including network, gateway, and endpoint components. Responsive agility is increased, while the time-to-containment and remediation are dramatically reduced, all without the need to re-architect the network.

Enabling Security Connected with the McAfee Data Exchange Layer

McAfee Threat Intelligence Exchange is the first solution to use the McAfee data exchange layer, an ultra-fast, lightweight bidirectional communications fabric that enables security intelligence and adaptive security through product integration and context sharing. McAfee data exchange layer-connected products simply subscribe and publish to the fabric without the need for complex application programming interface (API)-based integration efforts or burdensome configurations. It marks a new era in security–where all components come together to work as one cohesive system.

Easy Deployment and Management

Integration between McAfee Threat Intelligence Exchange and McAfee Advanced Threat Defense is seamless across the data exchange layer. Designed as an open framework, the data exchange layer enables security components to dynamically join the McAfee Threat Intelligence Exchange without the need for extensive APIs or complex product configurations, reducing errors and eliminating extensive manual effort.

CONNECT
Easily integrate network devices and endpoints to work cohesively and share security insights.

PROTECT
Use all connected capabilities to analyze suspect objects, regardless of first contact point.

RESPOND
Investigate encounters and retrospect with unparalleled visibility, via a centralized intelligence database to take control of the IT environment.

ADAPT
Automated, immediate and unified response across endpoints and network devices to emerging threats.

Figure 2. Seamless integration across the data exchange layer through Security Connected.

Learn More

McAfee Threat Intelligence Exchange and McAfee Advanced Threat Defense are essential to connecting disparate security components, protecting your environment, responding to encounters, and automatically adapting to emerging threats. Providing a security ecosystem that integrates advanced threat analysis, network products, and endpoint solutions, McAfee enables organization-wide visibility and context for threats while reducing response time and simplifying remediation.

- **http://www.mcafee.com/TIE**
- **http://www.mcafee.com/ATD**
- **http://www.mcafee.com/securityconnected**

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