WHITE PAPER

McAfee
Together is power.

Security that Plays Well with Others

Table of Contents

Security that Plays Well with Others

In a threat landscape replete with sophisticated attacks that are rapidly increasing in volume and frequency, organizations are finding that their isolated security controls are largely ineffective. Adversaries are outmaneuvering defenses, and resource-constrained security teams struggle to keep up. Typically, the security industry has responded by tracking attackers' tools and techniques in an attempt to anticipate the next threat wave and push out solutions that promise to be the ultimate "silver bullet." Barraged by complex threats, enterprise security organizations have responded by acquiring the most current innovative solutions, which they hope will address specific attacks and get the job done. But this "best-of-breed" approach has resulted in fragmented security where security data is entrenched in silos, making it difficult for security practitioners to fully understand threats and act on them appropriately and swiftly.

Organizations need a way to orchestrate security components so that they to work together and present a unified coordinated defense. McAfee's open, integrated architecture can help legacy point products play well together, optimize the effectiveness of your entire security infrastructure, and simplify, unify, and advance the threat defense lifecycle.

Achieving a Coordinated, Integrated Response

McAfee can help your enterprise move up the security maturity ladder and mount a truly coordinated, integrated response that can be easily adapted to your security operations. McAfee provides an open architecture that embraces not only solutions from McAfee and its partners, but also your current security defenses from multiple vendors. McAfee offers several integration options that can be adapted to your unique environment. These integration models are based on interconnecting tools, security data, and threat response processes. Reliable and scalable to accommodate future expansion, this open architecture also facilitates intake of new sources of threat intelligence—both global and local—and helps distribute it across all your defenses.

There are four methods by which you can integrate your security components into the McAfee architecture:

- **Point-to-point integration:** Use application programming interfaces (APIs) to improve the effectiveness of your combined security tools.
- **Many-to-one or one-to-many framework integrations:** Enable multiple downstream consumers and scale security information exchange in use.
- **Data integration:** Use standardized languages with common semantics to exchange threat intelligence.
- **Process and scripting via SIEM:** Automate your immediate orchestration needs.

Integration Using Application Programming Interfaces (APIs)

A common integration method is through an API (application program interface), a machine interface that opens a door directly into the security application and allows other tools to execute application processes or extract data. The interaction and exchange of data is usually made possible by a custom "catalyst" application that retrieves information from one tool and transmits it to another. Several McAfee applications provide an API, including McAfee® ePolicy Orchestrator® (McAfee ePO™) software, McAfee Advanced Threat Defense, and McAfee Enterprise Security Manager.

Methods	McAfee ePolicy Orchestrator	McAfee Threat Intelligence Exchange	McAfee Advanced Threat Defense	McAfee Enterprise Security Manager
Point-to-Point Integration	Web API		RESTful API	RESTful API
Common Framework Integration		Data Exchange Layer	Data Exchange Layer	Data Exchange Layer
Data Integration		STIX import	STIX export, file FTP import	STIX, TAXII, Data Exchange Layer, Netflow/IPFIX, File Pull/FTP, WMI, HTTP, OpSec, eStreamer, and more
Process and Scripting	Trigger scripts via automated responses			Trigger scripts via alarm actions

Table 1. Integration Methods and McAfee Product Interfaces

Use case 1: Leveraging the McAfee ePO software API for endpoint tagging and agent updates

McAfee ePO software provides policy-based management of a wide range of endpoint, data center, and network security countermeasures, including antivirus, host intrusion prevention, whitelisting, activity monitoring, and data loss prevention. Through the McAfee ePO management console, users or security tools can tag assets, such as desktop computers or other networked client systems. Once a system is tagged, other security tools can perform actions on the tagged asset, such as scanning, cleaning out the registry settings, or deploying a new control.

This use case provides an overview of how users can dynamically update endpoints that lack proper disk encryption software by leveraging the McAfee ePO software API and the Microsoft PowerShell command shell/scripting language. For other examples, visit: **https://community.mcafee.com/community/business/toolexchange**.

Integration requirements: Extract endpoint asset information status and deploy a disk encryption agent where needed.

Methodology:

- **Step 1:** Trace endpoint disk encryption status by interrogating McAfee ePO software via the API.
- **Step 2:** Deploy new disk encryption on required endpoints. Modify client properties through McAfee ePO software.
- **Step 3:** Report on the endpoint encryption status of all assets. Restart step 2 where required.

Figure 1. Leveraging the McAfee ePO software API for endpoint tagging.

Use case 2: Automated detonation of potential malware via the McAfee Advanced Threat Defense API

McAfee Advanced Threat Defense sandboxing technology offers unmatched analysis and detection for today's advanced targeted attacks, producing threat information for immediate action and protection. When security analysts observe suspicious network activity, they can validate high-risk files through McAfee Advanced Threat Defense to determine if a suspicious file is clean or infected with malware. This validation process can be automated by using the McAfee Advanced Threat Defense API to verify if and where potential malware may be present in the environment.

Integration requirements: Automate forwarding of high-risk files from a variety of security sources, such as web gateways, public FTP sites, web uploads, and more to McAfee Advanced Threat Defense for detonation. Centralize analysis results as critical information for analyst investigation.

Methodology:

- **Step 1:** Upload the suspicious file for detonation.
- **Step 2:** Report the results to your security information and event management (SIEM) solution and add it to the McAfee Advanced Threat Defense catalog.

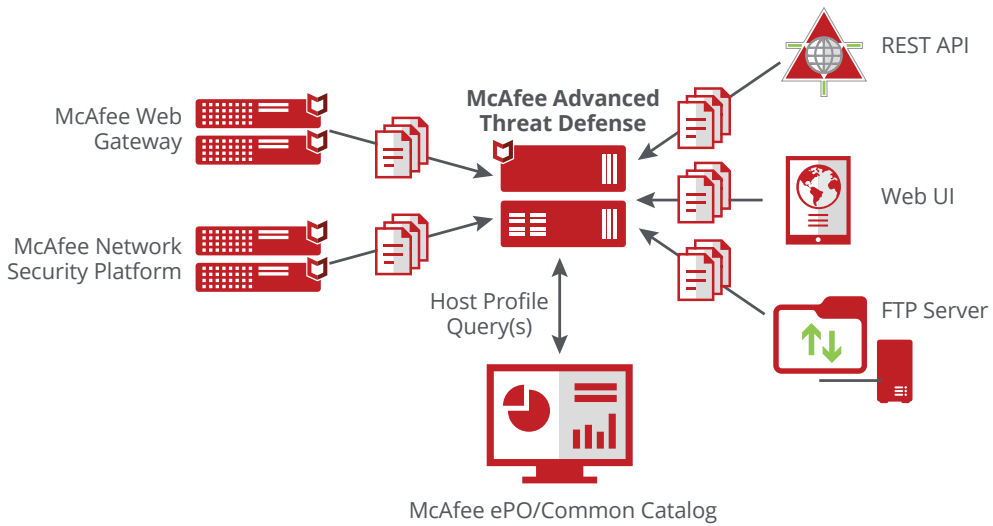

Figure 2. Automatic detonation of potential malware via the McAfee Advanced Threat Defense API.

Use case 3: Automated case management via the McAfee Enterprise Security Manager (SIEM) API

McAfee Enterprise Security Manager—the foundation of the security information and event management (SIEM) solution family from McAfee—delivers intelligence, actionable insights, and integration at the speed and scale required for security organizations to identify, understand, and respond to threats, while the embedded compliance framework simplifies compliance.

As events flow into McAfee Enterprise Security Manager and alerts are generated, the case management feature allows security operations to share alert investigations and streamline the workflow among security analysts. The information in the SIEM case management database may also be of value for IT operations team members who are involved in cleaning up endpoints, deploying new IT policy changes, or closing an IT service ticket when the issue has been resolved. Automated exchange of case management information helps streamline operations among security and IT teams—this is accomplished by way of the McAfee Enterprise Security Manager API. This use case leverages the McAfee Enterprise Security Manager structured representational state transfer (REST) API to accomplish any single task or combination of tasks (see "Methdology").

Integration requirements: Retrieve alarm and investigation information from McAfee Enterprise Security Manager case management and forward the data to the IT service management ticketing tool.

Methodology:

- **Step 1:** Forward McAfee Enterprise Security Manager cases to IT operations service desk tool.
- **Step 2:** Automatically transfer critical SIEM alarms to the service desk.
- **Step 3:** Enrich existing service desk tickets with McAfee Enterprise Security Manager event queries.
- **Step 4:** Transfer watchlists of known critical endpoints from the service desk to McAfee Enterprise Security Manager.

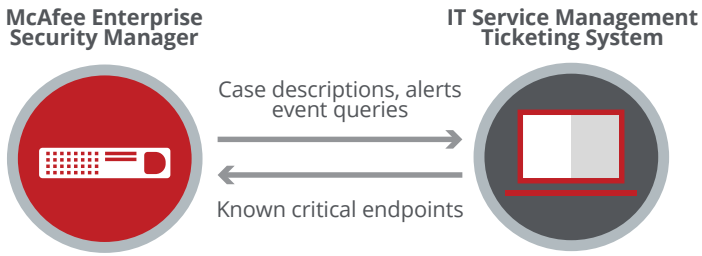

Figure 3. Automated case management through the McAfee Enterprise Security Manager API.

Common framework integration using Data Exchange Layer

Data Exchange Layer's API enables you to create a global framework for security integration. Unlike individual product APIs, which are tied to a specific application, Data Exchange Layer leverages a single API that can interface with multiple security tools. This unique API acts as a common communication fabric among all Data Exchange Layer participants, enabling one-to-one or one-to-many data flows that broadcast threat intelligence to a single tool or many across the security infrastructure. This integration is especially valuable when multiple downstream security components require instant updates about emerging adversarial activity.

Use case 4: Automated quarantining via Data Exchange Layer

Data Exchange Layer is an innovative, real-time, bi-directional communications fabric providing product integration simplicity and allowing security components to operate as one by sharing relevant data among endpoints, gateways, and other security products. For instance, by integrating threat detection and network access tools over Data Exchange Layer, users can automate quarantining of infected or noncompliant devices and reduce malware dwell time.

Integration requirements: Inform network access control solution when endpoint intrusion is detected.

Methodology:

- **Step 1:** Deploy and activate endpoint intrusion through McAfee ePO software.
- **Step 2:** When anomalous or suspicious activity is detected on the endpoint, endpoint intrusion security informs the network access solution to quarantine the infected endpoint.

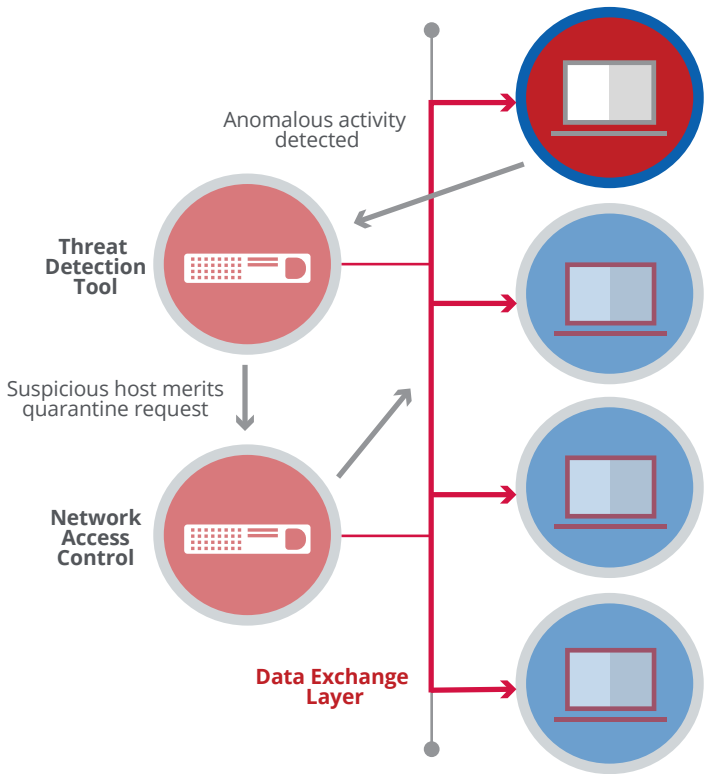

Figure 4. Automated quarantining via Data Exchange Layer.

Data-Level Integration

Once communication among security tools has been established, the need for common semantics arises. For instance, when a security device detects a threat, how do you share contextual information about the adversary, the exploit technique, or details about the impacted system so that various security controls can take appropriate action and stop the attack? Over the past several years, common threat context frameworks have emerged as accepted standards for threat data exchange. These include Structured Threat Information eXpression (STIX), Open Source malware Identification tool YARA, and Interface for Metadata Access Points (IF-MAP). All of these consist of structured representations of threat information that are expressive, flexible, extensible, capable of being automated, and as human-readable as possible.

STIX, for example, can describe the behavior of adversaries, including tactics, techniques, and processes. STIX has especially seen wide adoption by security vendors, including McAfee. Additionally, Trusted Automated eXchange of Indicator Information (TAXII) is a platform that enables sharing of STIX-formatted intelligence across organizations and products. These standards have been adopted by industry organizations like the Financial Services Information Sharing and Analysis Center (FS-ISAC) and other Internet community groups to facilitate sharing of cyberthreat intelligence among peers, partners, and other trusted organizations. (Visit the STIX website: **http://stixproject.github.io/supporters/**.) The McAfee architecture allows you to take full advantage of these community-driven initiatives to expand the breadth of threat intelligence your infrastructure can ingest to accelerate incident response. STIX is supported by several McAfee solutions in its product portfolio, including McAfee Advanced Threat Defense, McAfee Threat Intelligence Exchange, and McAfee Enterprise Security Manager (SIEM), all of which also leverage TAXII.

Use case 5: Importing STIX-formatted data into McAfee Threat Intelligence Exchange

McAfee Threat Intelligence Exchange significantly optimizes threat prevention by sharing intelligence across your infrastructure, closing the gap from encounter to containment for advanced targeted attacks from days, weeks, and months down to milliseconds. McAfee Threat Intelligence Exchange can combine threat intelligence from multiple sources, such as McAfee GTI, third-party threat information, and shared indicators of compromise (IoCs) formatted as STIX files.

Today, security practitioners can easily get access to threat intelligence (such as STIX-formatted data) that provides insights on adversaries, their methods, and system fingerprints. Continuous consumption and digestion of threat information can, however, become a complex and time-consuming task. By automating ingestion and propagation of STIX-formatted threat intelligence, security practitioners can obtain near-instant protection against rapidly emerging threats.

Integration requirements: Inform protection tools about STIX-reported threat intelligence using McAfee Threat Intelligence Exchange.

Methodology:

- **Step 1:** Import STIX threat data into McAfee Threat Intelligence Exchange.
- **Step 2:** Push the STIX threat intelligence out to your security components through Data Exchange Layer.

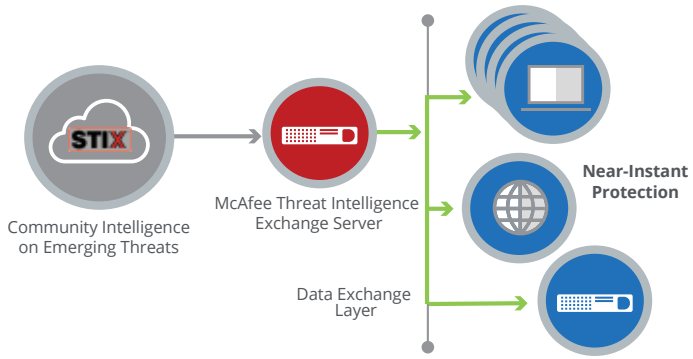

Figure 5. Importing STIX-formatted data into McAfee Threat Intelligence Exchange.

Use case 6: Importing STIX-formatted data to uncover suspicious activities

McAfee Enterprise Security Manager collects activity and event data from systems, databases, networks, and applications. It also imports global threat feeds and consumes threat intelligence in standard formats and transports, such as STIX/ TAXII; automated imports via CIFS, NFS, FTP, SCP, SFTP; and manual imports.

STIX-formatted IoCs contain facts and information about adversaries and the techniques they use. Security analysts can leverage this information to detect recently reported threats and especially to find out if the adversary has already been active in their environments. By automating the importation of STIX-formatted data over TAXII, security analysts can uncover new or previous suspicious activity and initiate the appropriate response actions.

Integration requirements: Import STIX-reported threat data and correlate it against real-time or historical event evidence.

Methodology:

- **Step 1:** Automate import STIX-reported threat data into McAfee Enterprise Security Manager using the cyberthreat manager.
- **Step 2:** Detect STIX-reported adversarial activity by correlating events with newly received STIX and TAXII threat intelligence.
- **Step 3:** Execute a backtrace against historical event evidence to validate past activity by specific adversaries.
- **Step 4:** Generate a report of all impacted systems for timely incident response.

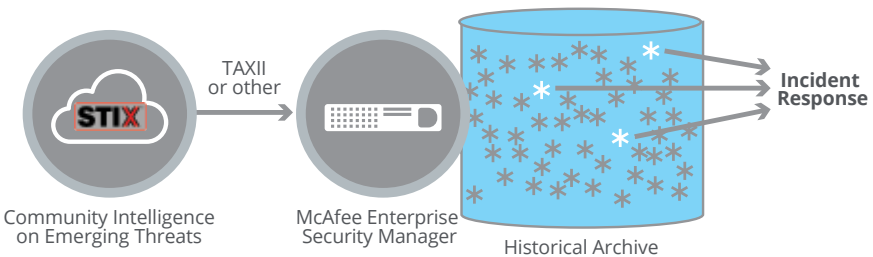

Figure 6. Importing STIX-formatted data to uncover suspicious activities.

SIEM as a Universal Gateway

In an enterprise security scenario where security data formats and interfaces are diverse, a skilled translator is immensely valuable during the threat response process. This is where SIEM comes into play. McAfee Enterprise Security Manager is designed from the ground up to consume any type of threat information in real time. It parses the information, categorizes and prioritizes it, and then leverages that data for analytics, global visibility, or orchestration across your security infrastructure to help your security team spring into action.

With its rich set of ingress and egress interfaces, McAfee Enterprise Security Manager can ingest a variety of event formats, such as Syslog, Netflow/IPFIX, File Pull/FTP, WMI, HTTP, OpSec, eStreamer, and more. It also can consume intelligence feeds from threat lists or STIX/TAXII, within your organization or externally. McAfee Enterprise Security Manager acts as an orchestration framework capable of collecting security event data while applying security semantics and enrichment. It analyzes this data via correlation rules and imports context data, such as adversarial threat intelligence, geolocation, reputation data, and user names. It quickly transforms these feeds into local stored security intelligence that can be used for analytics and better decision-making during the IR process. The SIEM system can also help the user automate post-alert actions, reducing exposure time when threats are active and helping security teams orchestrate response.

Use case 7: Interconnecting an advanced malware sandbox, McAfee Enterprise Security Manager, and McAfee Threat Intelligence Exchange for coordinated response

Today's threats require a coordinated response, where multiple technologies, such as malware sandboxing, SIEM, and protection tools work in concert and share information. In this scenario, convictions from a sandbox are collected by McAfee Enterprise Security Manager, interpreted, and forwarded to various tools to launch a coordinated response that will help neutralize the recently discovered adversary.

Integration requirements: Propagate malware threat details to all protection and remediation tools.

Methodology:

- **Step 1:** Import recently discovered threat details into McAfee Enterprise Security Manager through the standard event transport process.
- **Step 2:** Normalize and analyze the event details via McAfee Enterprise Security Manager.
- **Step 3:** Inform your network access control tool so that it can quarantine the affected assets and feed the details about the malicious file to McAfee Threat Intelligence Exchange for publication in the McAfee ePO management console.

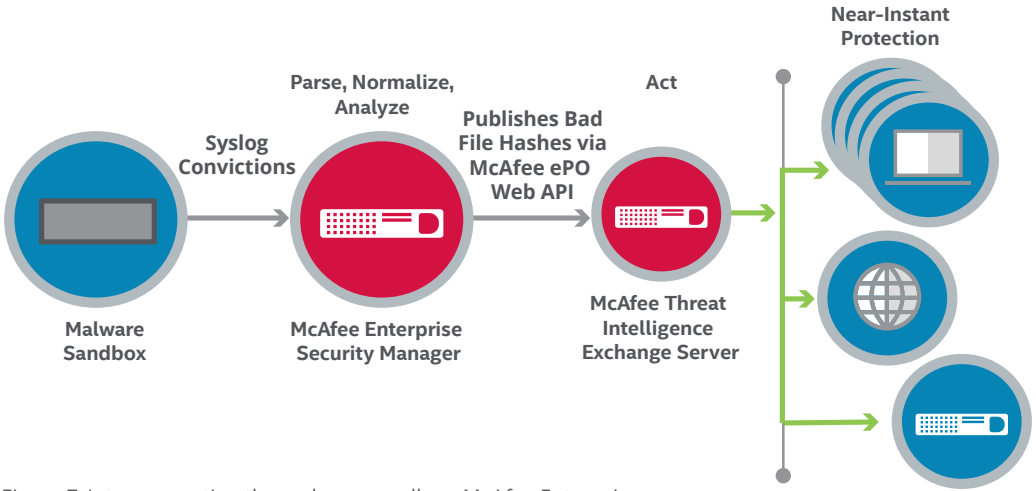

Figure 7. Interconnecting the malware sandbox, McAfee Enterprise Security Manager, and McAfee Threat Intelligence Exchange.

Use case 8: Script-based interactions

McAfee Enterprise Security Manager also allows for script-based orchestrations. When alerts fire, administrators can trigger any script and forward critical data from the alert into the custom script. In this example, network access is prevented when McAfee Enterprise Security Manager detects suspicious activity.

Integration requirements: Execute a custom script after an alert to disable the user account and filter the remote IP address.

Methodology:

- **Step 1:** Deactivate the user on Active Directory through the script.
- **Step 2:** Block the offensive external IP addresses by activating the access control filter on the firewall.

Figure 8. Script-based interactions.

Summary

In today's threat landscape, where both the sophistication and volume of threats are increasing at an unprecedented rate, organizations are becoming aware that a "silver bullet" approach to security is no longer viable. To gain the advantage over attackers, they need a way to coordinate their siloed legacy security products. McAfee's open, integrated security architecture facilitates the intake and distribution of threat data from a variety of sources, which helps build a stronger defense across the entire security infrastructure. Enterprises can choose the methods and integration strategies that are right for their environments and that will yield desired outcomes. Both McAfee products and legacy point products from multiple vendors play well together to simplify, unify, and advance the threat defense lifecycle.

Learn More

For additional information on how McAfee solutions integrate with other security technologies, visit:

- **McAfee Global Threat Intelligence**
- **McAfee Threat Intelligence Exchange**
- **McAfee Advanced Threat Defense**
- **McAfee Enterprise Security Manager**
- **McAfee ePolicy Orchestrator**
- **How to Use a TAXII Feed with McAfee Enterprise Security Manager**

About McAfee

McAfee is one of the world's leading independent cybersecurity companies. Inspired by the power of working together, McAfee creates business and consumer solutions that make the world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.

www.mcafee.com.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com