SOLUTION BRIEF

McAfee and Swimlane for Security Operations

Security orchestration, automation, and response for advanced threat defense

Integration with Swimlane will allow customers using McAfee® products, including McAfee® Active Response, McAfee® Advanced Threat Defense, Data Exchange Layer (DXL), McAfee® Enterprise Security Manager, McAfee® ePolicy Orchestrator® (McAfee ePO™) software, McAfee® Network Security Manager, McAfee® Threat Intelligence Exchange, and McAfee® Web Gateway to automatically initiate and execute incident response workflows in response to any alarm. Importing security event data from McAfee products into Swimlane delivers consolidated event details from multiple platforms for rapid investigation and alarm triage in a single, dynamic case management view. Automated workflows initiate a broad range of actions at machine speeds in response to any potential threat. This ensures faster incident response and a greater return on investment from the entire security infrastructure.

McAfee Compatible Solution

- Swimlane Security Orchestration, Automation, and Response (SOAR)
- McAfee Active Response
- McAfee Advanced Threat Defense
- Data Exchange Layer
- McAfee ePolicy Orchestrator
- McAfee Enterprise Security Manager
- McAfee Network Security Manager
- McAfee Threat Intelligence Exchange
- McAfee Web Gateway

McAfee COMPATIBLE

SWIMLANE

Connect With Us

The Business Problem

Advanced attacks are more sophisticated than ever before, evolving rapidly to bypass your security infrastructure. And while organizations have deployed a broad range of security tools to defend against advanced attacks, the sheer volume of alarms they generate are overwhelming security operations teams with a constant barrage of potential threats. Compounding this risk is a growing shortage of trained security personnel required to keep up with the volume of threats targeting your network.

Swimlane helps organizations get the most out of existing resources by automating time-intensive, manual processes and operational workflows in real time. An application programming interface (API)-first architecture, extensive out-of-the-box integrations, and prepackaged templates allow organizations to quickly enable orchestration across their entire security infrastructure.

McAfee and Swimlane Joint Solution

By integrating Swimlane with McAfee products, organizations can automatically initiate incident response workflows in response to alarms. This is a two-way integration, leveraging either REST API or DXL.

For example, importing security event data from both McAfee Enterprise Security Manager and McAfee ePO software into Swimlane delivers consolidated event details from multiple platforms for rapid investigation and triage. In another use case, alarms from McAfee Enterprise Security Manager can trigger automated workflows within Swimlane, which can then apply tags using McAfee ePO software to specific endpoints for immediate policy enforcement. This ensures faster incident response and a greater ROI from the entire security infrastructure.

Together, McAfee and Swimlane deliver:

- Automated incident response to combat advanced threats at machine speeds
- Fully or partially automated workflows based on organizational requirements
- Interoperability with a broad range of security platforms
  - Greater event contextualization
  - More accurate threat detection and response

About Swimlane

Swimlane was founded to deliver innovative and practical security solutions to organizations struggling with alert fatigue, vendor proliferation, and chronic staffing shortages. Swimlane is at the forefront of the growing market for security automation and orchestration solutions that automate and organize security processes in repeatable ways to get the most out of available resources and accelerate incident response.

Challenges

- Accelerating attack volumes
- Overwhelming alert fatigue
- Time-consuming manual processes
- Antiquated and decentralized incident response (IR) tools
- Growing shortage in skilled security professionals

Swimlane and McAfee Solution

- Bidirectional integration using REST API and/or DXL
- Faster response times
- Consistent IR processes
- Orchestration across all security platforms

Results

Integrating Swimlane with McAfee products can deliver an immediate and quantifiable return on investment (ROI). It enables organizations to investigate and respond to all alarms without increasing operating overhead. Security operations teams are empowered to operate more efficiently and effectively, spending less time on manual tasks and more time on proactive, advanced security activities.

About McAfee ePolicy Orchestrator Software

McAfee ePO software is the industry-leading security and compliance management platform. With its single-agent and single-console architecture, McAfee ePO software provides intelligent protection that is automated and actionable, enabling organizations to reduce costs and improve threat protection and compliance.

About McAfee Enterprise Security Manager

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

Learn More

For more information or to start an evaluation of McAfee DLP, contact your McAfee representative or channel partner, or visit **www.mcafee.com**.

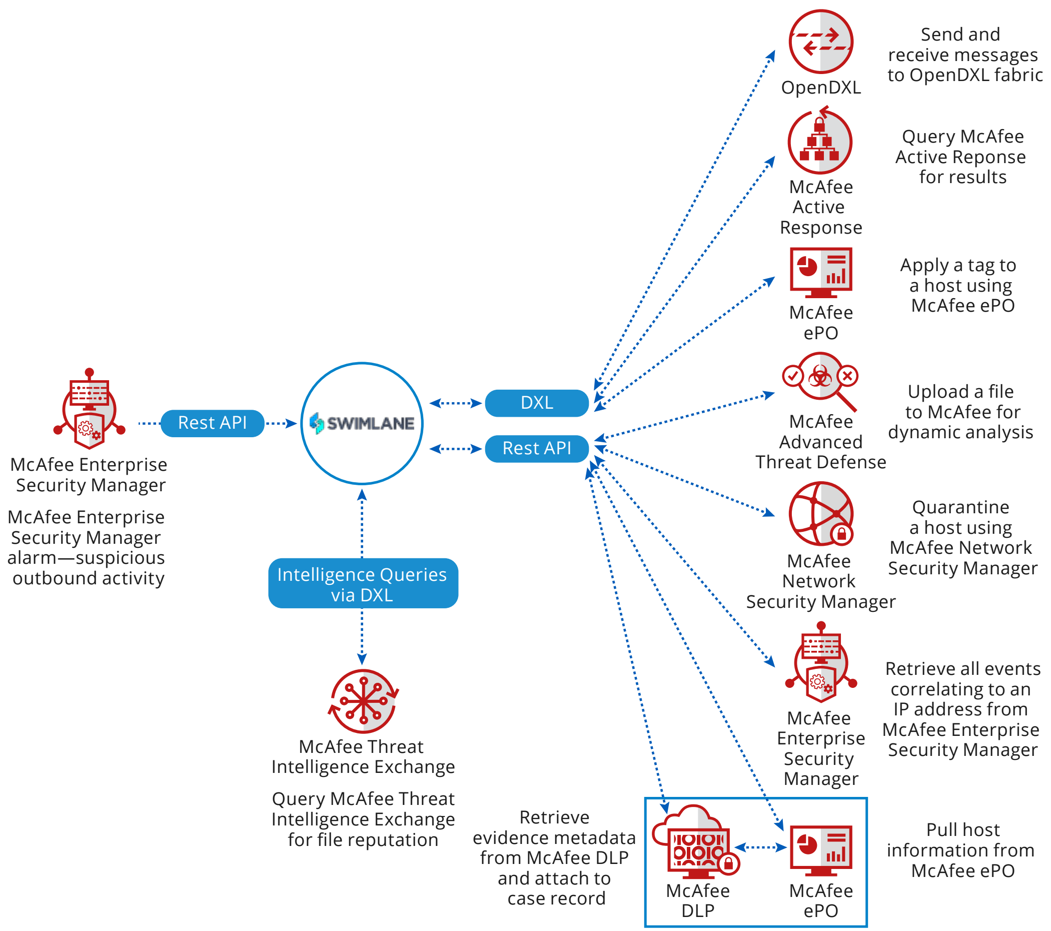
McAfee Enterprise Security Manager
McAfee Enterprise Security Manager alarm—suspicious outbound activity
Rest API
SWIMLANE
DXL
Rest API
Intelligence Queries via DXL
McAfee Threat Intelligence Exchange
Query McAfee Threat Intelligence Exchange for file reputation
OpenDXL
Send and receive messages to OpenDXL fabric
McAfee Active Response
Query McAfee Active Reponse for results
McAfee ePO
Apply a tag to a host using McAfee ePO
McAfee Advanced Threat Defense
Upload a file to McAfee for dynamic analysis
McAfee Network Security Manager
Quarantine a host using McAfee Network Security Manager
McAfee Enterprise Security Manager
Retrieve all events correlating to an IP address from McAfee Enterprise Security Manager
Retrieve evidence metadata from McAfee DLP and attach to case record
McAfee DLP
McAfee ePO
Pull host information from McAfee ePO

Figure 1. Swimlane workflow triggered by a McAfee Enterprise Security Manager alarm that includes automated response using a several McAfee products.

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