SOLUTION BRIEF

McAfee and Swimlane for Security Operations

Security automation and orchestration for advanced threat defense

Integration with Swimlane allows McAfee® Enterprise Security Manager and McAfee® ePolicy Orchestrator® software customers to automatically initiate and execute incident response workflows in response to any alarm. Importing security event data from McAfee Enterprise Security Manager/McAfee ePO software into Swimlane delivers consolidated event details from multiple platforms for rapid investigation and alarm triage. Automated workflows can enforce policy on endpoints leveraging McAfee ePO software 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 Automation and Orchestration (SAO)
- McAfee ePolicy Orchestrator
- McAfee Enterprise Security Manager

Connect With Us

The Business Problem

Advanced attacks are more sophisticated than ever, 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 labor-intensive, manual processes and operational workflows in real time. An applications 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 ePO software and McAfee Enterprise Security Manager technology, organizations can automatically initiate incident response workflows in response to alarms. This is a two-way integration.

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 return on investment from the entire security infrastructure.

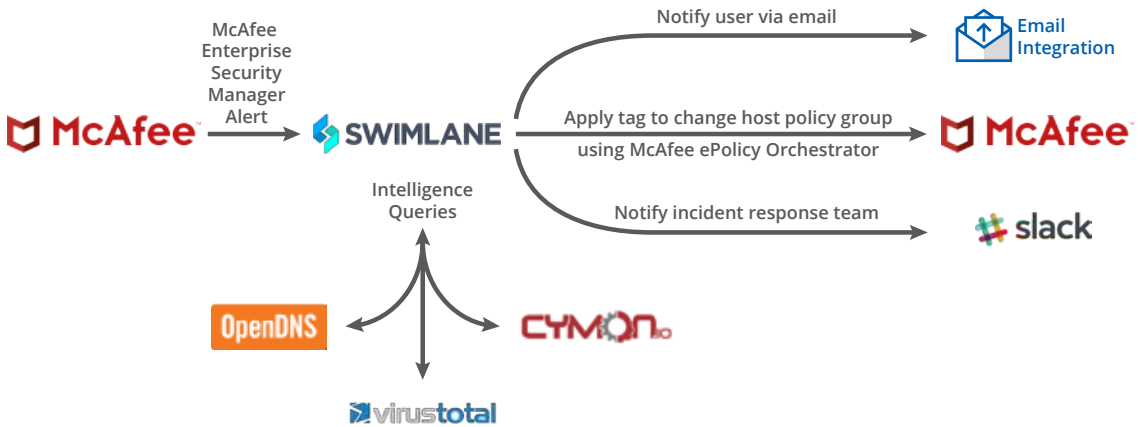

Figure 1. Use diagram depicting a Swimlane workflow triggered by a McAfee Enterprise Security Manager alarm that includes automated remediation using McAfee ePO software.

Challenges

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

Swimlane and McAfee Solution

- Bi-directional Integration
- Faster response times
- Consistent incident response processes
- Orchestration across all security platforms

Results

Integrating Swimlane with McAfee ePO software and/or McAfee Enterprise Security Manager can deliver an immediate and quantifiable return on investment (ROI). The joint solution enables organizations to investigate and respond to all alarms without increasing operating overhead. Security operations are empowered to operate more efficiently and effectively, spending less time on manual task and more time on proactive, advanced security activities.

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.

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.

McAfee Together is power.

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