McAfee
Together is power.

SWIMLANE

SOLUTION BRIEF

Swimlane and McAfee MVISION

Accelerating alert response

WHY WE WORK BETTER TOGETHER

Throughout the last decade, cybersecurity budgets have grown as more tools are needed to keep organizations protected. Attackers have continued to evolve, driving this need for more protective tools. The attackers have created and share a powerful arsenal of tools and automations purpose-built to conduct cyberattacks. Security Operation Centers (SOCs) and analysts find themselves with more to do to repel these advances, most of which is unfortunately coupled with increasing urgency. To continue to fight this battle effectively, they need some sort of force multiplier to keep up. McAfee and Swimlane provide a powerful solution to efficiently and effectively defend the enterprise.

BUSINESS CHALLENGE

With more powerful attackers on the prowl, the sheer number of alerts security teams are expected to investigate has increased dramatically. Infosecurity Magazine reported that, "alerts are on the rise, leaving today's security teams bombarded with 174,000 per week." These issues are compounded by the proliferation of security tools that need to be monitored, triaged, or updated. Security teams spend too much time switching back and forth and searching through tools for answers. Building a case requires cutting and pasting indicators, intelligence and other details to understand the big picture and provide full documentation. For alerts that need to be triaged, analysts also have to manually update rules and systems to address the issue and prevent it from reoccurring. All of this can be tedious, time-consuming, and prone to errors and omissions.

BENEFITS

- Enables the automation of alert triage, saving time
- Provides greater interoperability between products and threat intelligence correlation
- Standardized workflows ensure accurate triage

SOLUTION AT A GLANCE

Automated incident response to combat advanced threats at machine speeds

Flexible automated workflows based on organizational requirements

More efficient incident response and threat intelligence management

Centralized management of all integrated products (less time wasted moving back and forth between tools)

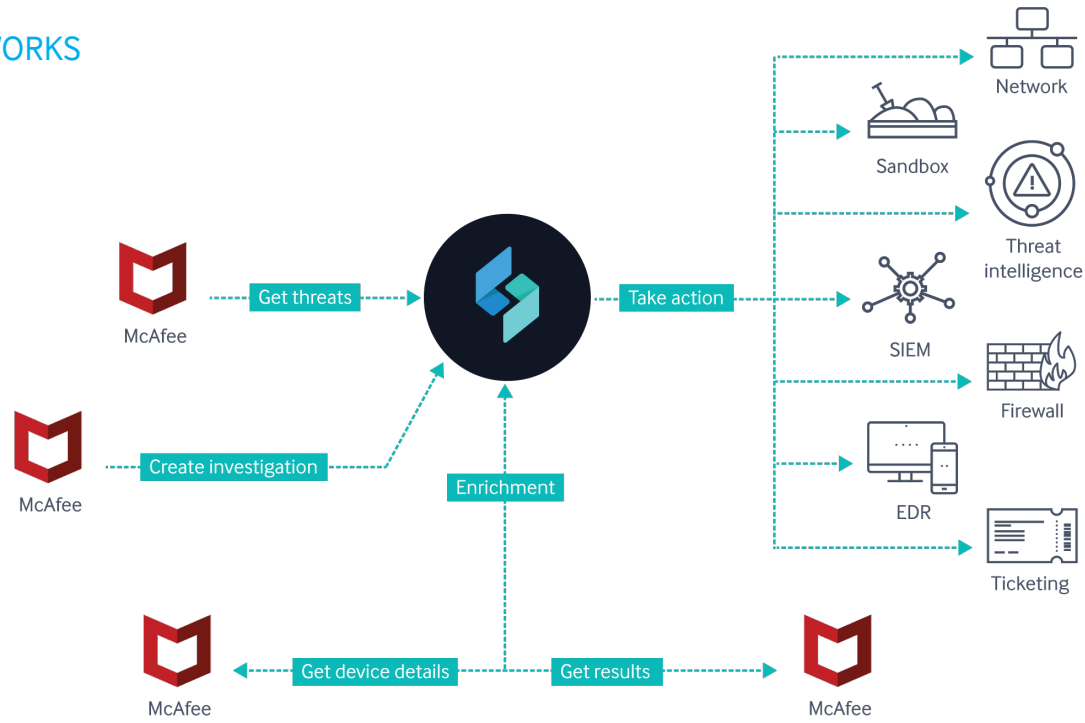
Swimlane ©2020

SOLUTION OVERVIEW

With so much for security teams to do, integrating security tools can really cut down on many SOC challenges, like time spent per alert. Swimlane and McAfee have teamed up to integrate our products so that they can, together, orchestrate a faster, more effective incident response and threat management solution. This solution not only connects disparate tools, but also enables teams to automate many of the alerts they would normally have to resolve manually.

The Swimlane McAfee MVISION integration enables the ingestion of McAfee MVISION ePO Events and Devices into the Swimlane platform. In addition, the MVISION EDR investigations are also brought into Swimlane. This helps security teams by preventing time wasted switching between security products or waiting for their results. Swimlane, coupled with MVISION's robust offerings, helps organizations accelerate and streamline incident response processes by centralizing all relevant event data in one platform and automating alerts with standardized workflows.

HOW IT WORKS



Using Swimlane's workflows, alerts from McAfee MVISION can be pulled into Swimlane to kick off a wide range of potential actions. Users have immediate access to information on associated devices, and workflows can add or remove tags and create investigations as needed.

BETTER TOGETHER

About McAfee

McAfee is a global organization with a 30-year history and a brand known the world over for innovation, collaboration and trust. McAfee's historical accomplishments are founded upon decades of threat and vulnerability research, product innovation, practical application and a brand which individuals, organizations and governments have come to trust.

About Swimlane

Swimlane is at the forefront of the security orchestration, automation and response (SOAR) solution market and was founded to deliver scalable security solutions to organizations struggling with alert fatigue, vendor proliferation and chronic staffing shortages.

Swimlane ©2020