SOLUTION BRIEF

McAfee and IBM Resilient Incident Response Platform

Identify and intelligently respond to threats with enhanced accuracy and speed

Security teams face complex challenges as they try to keep pace with the cybersecurity threats of today and prepare for the attacks of tomorrow. The integration between IBM Resilient's Incident Response Platform (IRP) and the McAfee® product portfolio ensures that security analysts can operationalize threat intelligence data in real time, allowing them to focus their energy on investigation and response, rather than pivoting between tools.

McAfee Compatible Solution

- Resilient Incident Response Platform
- McAfee® ePolicy Orchestrator®
- McAfee® Threat Intelligence Exchange
- Data Exchange Layer

IBM Resilient

Connect With Us

Hurdles to Effective Response

Responding effectively to cyberattacks is more difficult than ever before. Security teams are struggling to dynamically and intelligently respond to sophisticated actors and complex attacks. Security teams face these challenges while dealing with a shortage of skilled cybersecurity professionals, lack of time and resources, and a disjointed suite of tools. As security incidents continue to increase every year, organizations need to increase the productivity and effectiveness of their current analysts in order to fight back.

McAfee and IBM Resilient Joint Integrations

IBM Resilient IRP empowers incident response (IR) teams to investigate incidents and act faster and more accurately. IBM Resilient IRP with Intelligent Orchestration dramatically accelerates and sharpens response by seamlessly combining incident case management, orchestration, automation, and intelligence into a single platform. IBM Resilient also provides an Intelligent Orchestration Ecosystem that is made up of enterprise-grade, bi-directional integrations with drag-and-drop function capability. This allows security analysts the ability to easily create, customize, and update dynamic playbooks as your organization's needs change.

IBM Resilient and McAfee have released a number of pre-built, bi-directional integrations to make it easier than ever to coordinate between solutions, minimizing the need to switch between platforms. By integrating IBM Resilient IRP with Data Exchange Layer (DXL), McAfee Threat Intelligence Exchange, McAfee ePolicy Orchestrator (McAfee ePO™), and McAfee Advanced Threat Defense via IBM Security App Exchange, IR teams can include individual McAfee functions within their IBM Resilient workflows to dynamically orchestrate security incident response activities.

McAfee Threat Intelligence Exchange threat Lookup and function

Automatically search your organization's McAfee Threat Intelligence Exchange reputation data when file or hash artifacts are tracked within IBM Resilient, rapidly alerting the IR team to significant threats. For deeper investigation, a function for custom workflows allows security teams to search for information on a file hash within McAfee Threat Intelligence Exchange in response to dynamic playbook events and update the incident data with the results.

McAfee Advanced Threat Defense Integration for IBM Resilient

Enhance incident response workflows by uploading a file or URL for detonation within McAfee Advanced Threat Defense, returning the results to IBM Resilient IRP to provide greater context around potential threats to prioritize response. The analysis is visible as a report or as structured data that can determine further courses of action in dynamic playbooks.

Challenges

- Organizations face a variety of security and operational challenges in the face of today's emerging threats.
- The cybersecurity industry remains fragmented, with some enterprises having as many as 85 tools from 45 different vendors.
- The skills gap is an ongoing challenge for security and incident response (IR) teams.

McAfee Solution

- McAfee ePolicy Orchestrator
- McAfee Threat Intelligence Exchange
- DXL

Results

- Respond smarter with Resilient's dynamic incident response playbooks.
- IR analysts save time by automating lookup in McAfee Threat Intelligence Exchange to streamline response activities.

McAfee ePO Integration for IBM Resilient

Take action on endpoints managed by McAfee ePO software directly from the IBM Resilient platform. When using the McAfee ePO software function in IR workflows, security analysts can automatically or manually trigger McAfee ePO software to act on the systems that are tracked in IBM Resilient artifacts by using tagging to initiate quarantine or other actions for remediation.

Open DXL integration for IBM Resilient

Listen for alerts published to OpenDXL topics by McAfee and other applications and immediately escalate into the IBM Resilient IRP. Both synchronous and asynchronous messages from IBM Resilient can be published to different topics within DXL using a service or an event. Analysts can take action on these events without switching between platforms. The full OpenDXL message request and response functions are available, such as adding McAfee Threat Intelligence Exchange results from an action to IBM Resilient as an incident note.

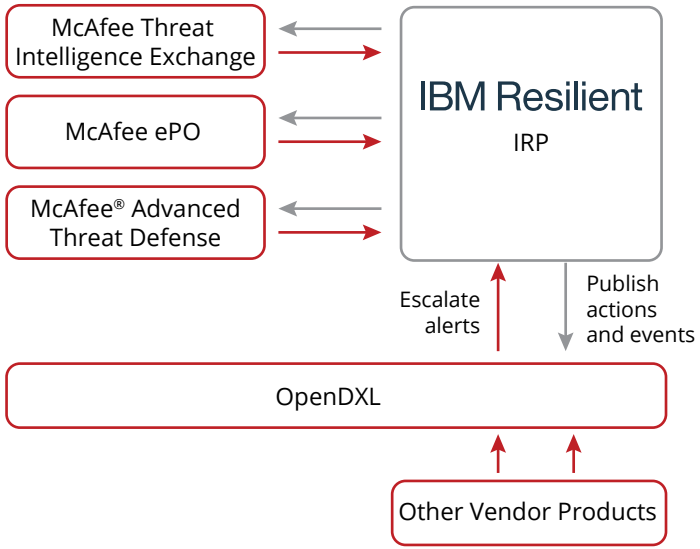

Figure 1. McAfee and IBM Resilient integration.

About IBM Resilient

IBM Resilient's mission is to help organizations thrive in the face of a cyberattack or business crisis. The industry's leading incident response platform (IRP) empowers security teams to analyze, respond to, and mitigate incidents faster, more intelligently, and more efficiently. IBM Resilient IRP is the industry's only complete IR orchestration and automation platform, enabling teams to integrate and align people, processes, and technologies into a single incident response hub. With IBM Resilient, security teams can have best-in-class response capabilities. IBM Resilient, part of IBM Security, has more than 300 partners, including 60 of the Fortune 500, and hundreds of other partners globally. To learn more, visit: ibm.com/security/intelligent-orchestration.

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 Data Exchange Layer

The Data Exchange Layer communication fabric connects and optimizes security actions across multiple vendor products, as well as McAfee-developed solutions. Enterprises gain secure, real-time access to new data and lightweight, instant interactions with other products.

Learn More

For more information, contact your McAfee representative or channel partner, or visit **www.mcafee.com**.

McAfee
Together is power.

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

McAfee and the McAfee logo, ePolicy Orchestrator, and McAfee ePO are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others. Copyright © 2018 McAfee, LLC. 4204_1218
DECEMBER 2018