SOLUTION BRIEF

Syncurity SOAR Platform and McAfee MVISION in Action

Optimize incident response and triage through an integrated solution

Cyber alert triage and incident response require process agility and standards-based technology integration. Are your security operations able to match adversary speed? Fragmentation of security solutions has created operating environments plagued with patchwork technologies. These technologies are not collective in their defense capabilities, and they are not cohesively managed for maximum incident response efficiency and efficacy. This means there is no common lens for evaluating and mitigating risk. Many organizations are not bringing to bear the full capabilities of even their existing defensive technologies. In fact, 55% of organizations currently struggle to rationalize data when three or more consoles are present.[1]

McAfee Compatible Solution

Syncurity

- IR-Flow SOAR software platform (VMware ESX-based deployed on premises or in the private cloud)

McAfee

- McAfee® ePolicy Orchestrator® (McAfee ePO™ (pending certification)
- McAfee® Active Response
- McAfee® Active Threat Defense
- McAfee® Enterprise Security Manager
- McAfee® Web Gateway
- Data Exchange Layer (DXL) (pending certification)

Connect With Us

McAfee® technologies and Syncurity IR-Flow accelerate security operations cyber-risk identification, containment, and remediation using a comprehensive array of McAfee, third-party, and even operating systems (OS)-native technologies through a single integration framework to offer maximum defense against relentlessly innovative adversaries by delivering a solution that is:

- **Open:** Using a standards-based integration framework and REST application programming interfaces (APIs), the McAfee solution suite and the Syncurity IR-Flow SOAR platform allow enterprises to improve immediately using their existing investments versus "rip-and-replace."
- **Adaptive:** With dynamic process workflows for alert triage and incident response, the combined McAfee-Syncurity solution enables device-native, third-party, and McAfee products to enrich investigations with context and implement containment countermeasures for your best collective defense—this is not just a collection of separate, unintegrated defenses.
- **Comprehensive:** Defend your entire digital terrain, not just traditional operating system-based endpoints, including laptops, servers, containers, mobile, and embedded Internet of Things (IoT) devices.

Traditional IR Cycle Time Drives Up Cyber Risk

Defending against cyber risk is a never-ending game of "Whac-a-Mole," where techniques to identify, stop, and eradicate adversaries must continuously assess risk and adapt accordingly. Delays in properly identifying, prioritizing and eradicating risks can lead to costly security breaches.

There are three key factors that make comprehensive incident response so difficult:

- **Technology diversity:** Today's enterprises deploy hundreds of applications across multiple on-premises, private/public cloud, and SaaS infrastructures. In support of this, they also deploy dozens of security technologies, often from multiple vendors. The inability to easily define investigative workflows with systematic access to the context needed results in tedious, manual efforts that increase dwell time for true positives.
- **Lack of a common language:** Technology compatibility goes beyond the simple techniques of exchanging electronic information. Most security tools today maintain their own taxonomy for risk (score, "Critical, High, Medium, or Low" rating, and more), and use different names and attributes for common information ("source IP," "source address," or "originating IP"). For many enterprises, this requires teams to write code that normalizes these values in an attempt to assess risk across their diverse technology spectrum, which complicates efforts to quickly enable new tools to reduce risk.
- **Point solution detection and response:** In order to expedite the IR process, many security point solutions have added functions that enable automated response (assess an IP address, and block it at the firewall based on some criteria). However, to truly assess cyber risk, a comprehensive view of the extended enterprise is needed. Otherwise, measures taken may not fully thwart the adversary or may miss critical forensic data that could be used to improve

Challenges
- Alert overload
- Manual processes
- Long dwell times

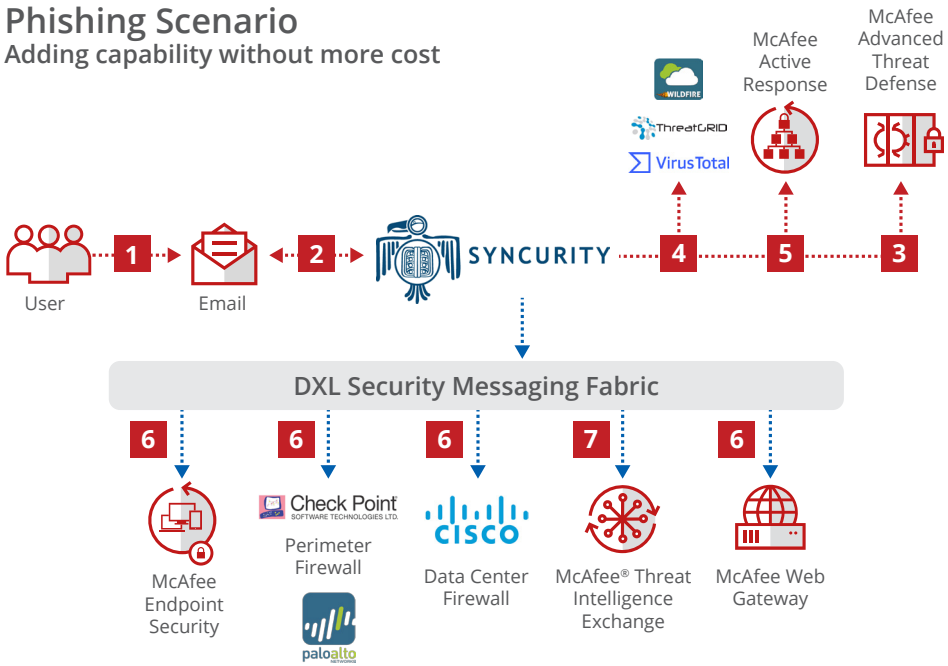
McAfee Solution
- McAfee® intelligent security operations solutions

Results
- Increased number of alerts evaluated daily per analyst
- Decreased alert dwell time, time-to-containment, and time-to-remediation
- Improved patching and security update practices
- Delivered granular audit data and reporting for alert and incident handling

defenses comprehensively versus only one threat vector. In addition, these tools often lack the additional context needed to determine risk severity of risk and to support/justify the recommended containment and remediation actions. They also don't easily incorporate the human element of review/approval typically necessary to make IT changes outside a pre-approved change control process.

The McAfee Platform and the Syncurity SOAR Solution Solve the Challenge

McAfee and Syncurity solve the security operations challenge with a comprehensive solution that delivers rapid response and reduced cyber risk. The combination of industry-leading McAfee solutions orchestrated with certified integrations by the Syncurity IR-Flow SOAR platform, enable real-time evaluation of cyber risk and the automated deployment of containment and remediation actions through an open integration framework that supports McAfee and third-party technologies.



Scenario Description

Incident Identification

1. User forwards a suspicious email with an attachment to SOC for investigation.
2. Syncurity automatically ingests this email and extracts artifacts.

Incident Investigation

3. Syncurity detonates file in McAfee Advanced Threat Defense.
4. Syncurity validates suspicious C2 IP addresses with Cisco Threatgrid, VirusTotal, or Palo Alto Networks Wildfire.
5. Syncurity launches AR queries to find infected systems.

Incident Containment

6. Syncurity updates customer McAfee Threat Intelligence Exchange server with malicious hashes.
7. Syncurity updates McAfee Web Gateway and Palo Alto Networks firewalls with malicious IPs.

Figure 1. How McAfee and Syncurity work together to add capability to the incident response process when a phishing incident occurs.

Gartner has defined **Security Orchestration, Automation and Response** (SOAR) as a technology that enables organizations to collect security threat data and alerts from different sources, where incident analysis and triage can be performed leveraging a combination of human and machine power to help define, prioritize, and drive standardized incident response activities according to a standard workflow. SOAR tools allow an organization to define incident analysis and response procedures (plays in a security operations playbook) in a digital workflow format, so that a range of machine-driven activities can be automated.

By codifying the steps necessary to effectively identify threats, assess potential risk, and—when appropriate—remediate that risk, enterprises are able to implement repeatable, auditable security operations workflows that can be executed consistently, regardless of the skill level of the available analysts, application owners, or IT resources supporting the infrastructure. The Data Exchange Layer (DXL) platform provides the means to standardize communications across McAfee and third-party products, while the Syncurity IR-Flow platform enables dynamic workflows for alert triage and incident response. The combination enables enterprises to more quickly and accurately assess risk, prioritize those risks, and, if necessary, orchestrate containment and remediation actions across the McAfee and third-party tool landscape.

- **Software:** The McAfee-Syncurity solution is comprised of multiple software components, including McAfee ePO software (pending certification), McAfee Web Gateway, McAfee Enterprise Security Manager, McAfee Advanced Threat Defense (pending certification), and the DXL framework for the execution of orchestration capabilities across the McAfee and third-party vendor technologies. The entire process is orchestrated and automated using the IR-Flow SOAR platform's playbooks.
- **Services:** McAfee and its solution partners provide a range of services to ensure success. McAfee experts provide security assessments to analyze your current environment and data landscape, focusing on risk to sensitive data. Certified delivery partners manage the hardware and software deployment, installing the security operations components within your environment. Once deployment is complete, the partner oversees integration, which includes connecting the various components using DXL to the SOAR platform. McAfee and Syncurity have identified several high-value reports, which can be tailored to specific industry or business requirements, as well as optimize and model the data capture needed to support those reports. The solution includes reports in the IR-Flow Business Intelligence engine to demonstrate performance improvement and serve as the basis for continuous improvement.

Summary

The diversity and limited interoperability of today's enterprise IT and security infrastructure creates increased cyber risk due to alert dwell time and delayed response. McAfee and Syncurity have combined their industry-leading solutions to create a comprehensive platform for assessing, prioritizing, and executing containment and remediation for threats against the entire ecosystem, including third-party products. The solution uses DXL as a common translation and execution layer whose actions are orchestrated and automated by the Syncurity IR-Flow platform with key McAfee solutions, as well as third-party technologies.

KEY BENEFITS

- Quick "time-to-value" with integrated solution and services
- Rapid insight into a consistent evaluation of cyber risks
- Access, analyze, and execute cyber risk containment and remediation in real time
- Reduce cyber risk associated with alert dwell time
- Optimize performance of limited security operations resources

About Syncurity

Syncurity optimizes and integrates people, process, and technology to realize better cybersecurity outcomes and accelerate security operations teams by delivering an agile incident response platform. Syncurity's IR-Flow platform uniquely allows "on-the-fly" customization to speed deployment, separates alert handling from incident management processes to increase efficiency, incorporates human analysts for more accuracy, and generates a detailed security "system of record" that enables reporting and measurement, process improvement, and compliance demonstration. With pre-built integrations that enable context enrichment and automated action across the security stack, IR-Flow empowers security teams to reduce alert triage and escalation time by over 80% and implement consistent, repeatable, and auditable processes for incident handling.

For more information, visit https://www.syncurity.net.

About McAfee

McAfee is the device-to-cloud cybersecurity company. Inspired by the power of working together, McAfee creates business and consumer solutions that make our 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.

Learn More

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

1. Source: MSA Research commissioned by McAfee on Security Management, January 2018

McAfee Together is power.

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