SOLUTION BRIEF

Gaining Advanced Analytic Insights into Your Network

Triage accurately. Investigate efficiently. Work effectively.

Through the integration of continuously updated and contextually enhanced risk scores for each of your network devices, your organization can achieve previously unknown visibility into network, identity, access, endpoint, and threat behavior for all network-connected devices. This automated multidimensional visibility helps you neutralize emerging threats and improve investigational efficiency and response.

Composite risk scores across data dimensions and the underlying analytically enriched data from SAS Cybersecurity are available for subscription from any Data Exchange Layer (DXL)-compatible solution. McAfee® ePolicy Orchestrator® (McAfee ePO™) console customers can subscribe to receive this information, further enhancing automated capabilities to identify, manage, and respond to security issues and threats.

McAfee Compatible Solution

- SAS Cybersecurity version 2.1 and above
- Data Exchange Layer version 3.1.0 and above
- McAfee ePolicy Orchestrator version 5.9.0 and above

The Business Problem

It's increasingly difficult to know your network. The explosion of IoT devices, virtual machines, and cloud services has left IT organizations struggling to understand the scope of what is connecting, when, how, and why. This added size and complexity means more security risk, more alerts, and more tuning. Despite the increased risk, most organizations remain understaffed and unable to keep up.

Not all adversaries in your network trigger an alert. Some hide in the technology and data silos. How can you determine whether suspicious activity is occurring? What if you could automatically break down these silos, to increase your visibility and awareness? What if you could scale the observation and decision-making power of your security operations center (SOC) to see risky activity more clearly?

Security analytics from SAS provides accurate and detailed network insight at scale, increased SOC efficiency and greater productivity.

McAfee and SAS Joint Solution

Leveraging the power of SAS Cybersecurity with the integrative capabilities of DXL, customers can now gain a new security perspective on the devices connecting to their networks and stay one step ahead of emerging threats.

SAS Cybersecurity collects streaming data from disparate data silos, starting with network traffic data. This data is analytically enriched with endpoint, identity, asset, other network information, and threat data in real time, resulting in a combined, cross-dimensional feed for every device on a network. Machine learning algorithms compare this enhanced behavioral record for each device to the behavior of other devices in the peer group.

The solution then delivers continuously updated risk scores from composite scoring against multiple behavioral measures. This approach allows the data to identify where risks exist. Prioritized results can then be complemented by institutional knowledge via the McAfee integration, but are not completely dependent upon it.

How the McAfee and SAS Joint Solution Works

1. To publish SAS Cybersecurity results, the events, alerts, and contextual data generated from SAS Cybersecurity are extracted via the applicable application programming interface (API).
2. The preformatted results are then parsed and formatted according to the McAfee open threat schema designed for both DXL and McAfee ePO software event ingestion in order to share as much common functionality as possible.
3. The formatted results are sent by DXL via the {/open/threat/v1/nip/SAS/SCS} topic for consumption by mutually-deployed, DXL-compatible solutions.

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

Challenges

- Existing security applications have limited ability to see network activity contextualized against other security data that can be analyzed to proactively identify threats and indicators of attack (IoAs) that need to be addressed.

McAfee Solution

- DXL is a secure, high-speed communication fabric that facilitates real-time exchange of high-value security data, thereby enabling security actions based on real-time intelligence across a multivendor ecosystem.
- McAfee ePO software unifies the way you manage endpoints, network, data, and compliance solutions.

Results

- SAS Cybersecurity publishes alerts and analytically enriched data to DXL, providing access to continuous, prioritized risk scores and security context. This allows security organizations to proactively identify IoAs versus responding to IoCs. It is available for subscription from any DXL-compatible solution.

Figure 1. SAS Cybersecurity working in concert with DXL and McAfee ePO software.

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.

About SAS Cybersecurity

SAS Cybersecurity is a security analytics software solution that reveals cyber adversaries in your network across the entire kill chain. Blending advanced behavioral analytics and machine learning, the solution automatically identifies threats missed by existing security investments. Continuous, prioritized risk scoring of network entities focuses investigations, while the underlying risk context enables fast action. The result? Unprecedented network visibility, reduced adversary dwell time, and SOC effort well spent.

About SAS

SAS provides customers with a full lifecycle approach to analytics that breaks down silos, transforms data, delivers fast and accurate results, and continuously integrates analytic insights and feedback into their operations.

The results? SAS improves operational efficiency, enhances decision-making and optimizes the value of data. With SAS, organizations can unify and grow their analytic capabilities so they are ready to solve today's and tomorrow's challenges.

Analytics must be more than a bolt-on capability to a security product. We know, because we have more than 40 years of experience establishing foundational analytic approaches that are sustainable for the long term.

Learn More

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

McAfee Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com