SOLUTION BRIEF

Gaining a Full View of Network Scope and Risk

Assess accurately. Investigate efficiently. Work effectively.

Compiling the dynamic puzzle of an indicator of attack (IoA) requires a comprehensive view of your network and a meaningful way to combine your security data and analytics capabilities. Issues of data and analytics diversity, scale, and trust often keep the puzzle pieces scattered and your resources from operating at peak productivity.

The integration of SAS® Cybersecurity security analytics software with Data Exchange Layer (DXL) enables McAfee® ePolicy Orchestrator® (McAfee ePO™) software to gain broader and deeper visibility into your network environment and enterprise risk. Automated, multidimensional network device risk scoring driven by machine learning provides the constant awareness required to speed IoA identification, management, and response.

McAfee Compatible Solution

- SAS Cybersecurity version 2.1 and above
- Data Exchange Layer version 3.1.0 and above

Connect With Us

The Business Problem

It's critical, yet increasingly difficult to know your network. The explosion of Internet of Things (IoT) devices, virtual machines, and cloud services has left organizations struggling to understand the scope of what connects, when, how, and why. This added network size and complexity means more security risk. Despite the increased risk, most organizations are unable to keep up. They can't get enough value from siloed security data and analytics capabilities to drive insights and priorities. Without clear network knowledge, they are challenged to identify high-risk areas warranting enhanced protection.

These organizations exist in a reactive circle of threat containment, eradication, and recovery. Focus on "known bad" static indicators of compromise (IoCs) are the norm.

What if you could simultaneously improve your network visibility and become more proactive in your security focus? With rapid and easy detection and analysis of IoAs. How much would that increase your security resource effectiveness and posture?

Security analytics from SAS provides that accurate and detailed network insight at scale, increasing your security visibility, efficiency, and productivity. Security analytics capabilities from SAS are built on the SAS Platform, a software foundation engineered to generate insights and impact from data in any computing environment. The SAS Platform supports diversity, enables scale, and empowers trust in your security data, analytics, and results.

McAfee and SAS Joint Solution

As the leader in analytics, SAS brings decades of experience, scaling to meet Fortune 500 customer data and analytics challenges. By leveraging the power of the SAS Platform—combined with the integrative capabilities of DXL—customers get a new security perspective on network devices to help them stay ahead of emerging threats with existing resources.

SAS Cybersecurity unifies streaming data from data silos and analytics from technology silos. Network traffic data is collected and enriched in-stream with endpoint, identity, asset, network, and threat data in real time, resulting in a cross-dimensional behavioral feed for every network device. Machine learning algorithms compare this enhanced behavioral record for each device to the behavior of similar devices in its individual peer group.

The solution then delivers continuously updated and prioritized device risk scores based on the composite score across multiple behavioral measures. This approach creates a holistic view of risk for each device. Organizations are alerted to subtle and potential IoAs and are provided with valuable investigational context. Further contextual enhancement is driven by ingesting DXL data from supported DXL-compatible partners. Prioritized results can then be complemented by institutional knowledge.

Challenges
Existing security applications have limited ability to see network activity contextualized against other security data to proactively identify threats and IoAs.

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.

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 instead of solely responding to IoCs. The alerts and analytically enriched data are available for subscription from any DXL-compatible solution.

Publishing/Subscribing to DXL Information with SAS Cybersecurity Software

1. SAS Cybersecurity ingests supported DXL-compatible partner data and correlates the data against its rich device risk profiles.
2. Acting as an aggregation point, SAS Cybersecurity performs advanced analytics on the combined data.
3. The composite risk scores plus the underlying analytically enriched data are published to DXL.
4. These high-value threat insights are sent to DXL via the {/open/threat/v1/nip/SAS/SCS} topic for consumption. DXL data subscribers can take these results to McAfee ePO software, McAfee Active Response, McAfee Enterprise Security Manager, and third-party DXL-compatible solutions to better understand their security postures and prioritize remediation activities.

High level dataflow

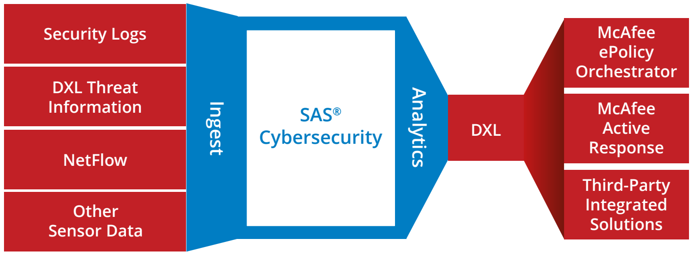

Figure 1. SAS Cybersecurity working in concert with supported DXL-compatible solutions.

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 allows organizations to identify, define, and act on IoAs accurately across all network-connected devices, including IoT and the cloud. Applying powerful machine learning capabilities to network data enriched with endpoint, identity and threat information, SAS drives security operations efficiency and focus for fast investigation and disposition of critical security risks.

About SAS

SAS addresses the issues of security data and technology diversity, resource scalability, and analytics trust that prevent organizations from gaining an integrated picture of their security posture. Whether your organization is exploring data or expanding established security analytics efforts, SAS can help you ask the right questions, find the right answers, and take the next step toward getting the most value from your analytics.

Learn More

For more information or to start an evaluation of DXL, 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