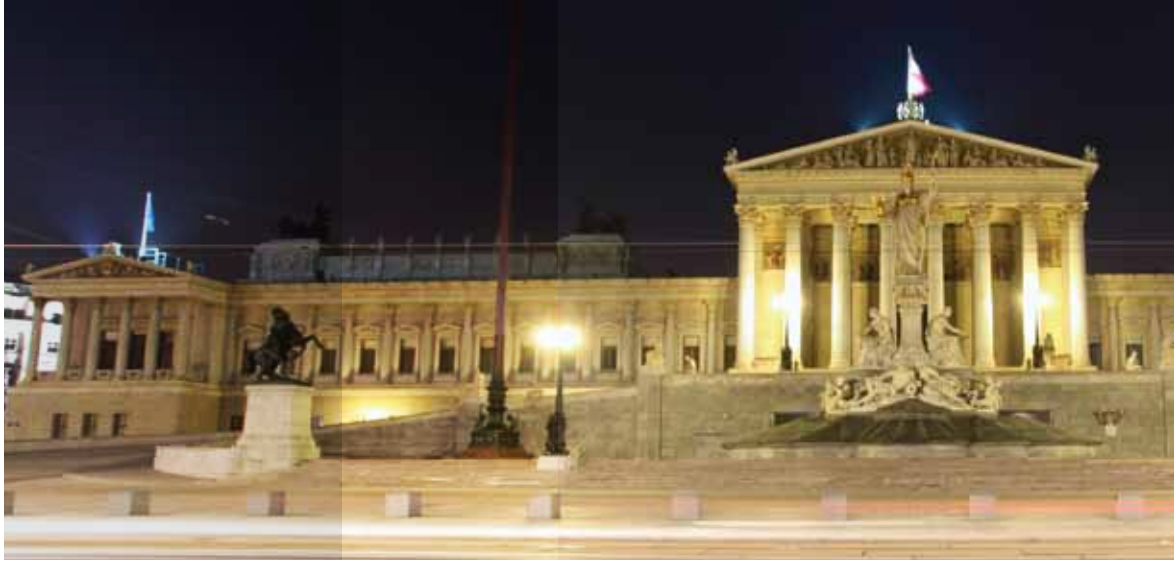
McAfee
An Intel Company

ACHIEVE CONTINUOUS MONITORING

Solution Guide

SECURITY CONNECTED REFERENCE ARCHITECTURE

LEVEL 1 **2** 3 4 5



Security Connected

The Security Connected framework from McAfee enables integration of multiple products, services, and partnerships for centralized, efficient, and effective risk mitigation. Built on more than two decades of proven security practices, the Security Connected approach helps organizations of all sizes and segments—across all geographies—improve security postures, optimize security for greater cost effectiveness, and align security strategically with business initiatives. The Security Connected Reference Architecture provides a concrete path from ideas to implementation. Use it to adapt the Security Connected concepts to your unique risks, infrastructure, and business objectives. McAfee is relentlessly focused on finding new ways to keep our customers safe.

Real-Time Risk Management as a Lifestyle

Challenges

Recognizing the shortcomings of FISMA and the need for a practical risk management process, the US Department of Homeland Security (DHS) created the Continuous Asset Evaluation, Situational Awareness, and Risk Scoring (CAESARS) Reference Architecture and Framework Extension (FE). CAESARS shifts the focus of security efforts from compliance reporting to effective and resilient cybersecurity. Support for CAESARS does not mean a rip-and-replacement of all security and compliance controls. Instead, it asks each organization to enhance its abilities to detect and evaluate vulnerabilities and anomalies and respond to incidents based on risk.

Continuous monitoring is a network lifestyle for greater resilience. It requires a shift in mindset, from reaction and documentation to proactive, data-centric, risk-based action.

Continuous monitoring also requires a shift in security infrastructure. Process and data integrations must cross organizational, data, and system boundaries. The biggest procedural changes affect pace and frequency—data collection, asset management, and risk management processes happen continually, not periodically, across sensor environments. The biggest technical changes affect integration and correlation of granular data across data domains: live threat intelligence and multiple data streams—including risk scores—are synthesized into automatic and human-assisted incident mitigation. As new data emerges, the system learns and responds, elevating thresholds and adapting network policies and control responses in a perpetual feedback loop.

The CAESARS architecture encourages multiple vendors, new sources of intelligence, and flexible, modular implementations. It calls for standard interfaces to link the key functional components and provide ways to plug in global and local threat intelligence from any available sources. This common, standards-based information framework ensures maximum compatibility, agility, and ROI. But few security vendors have a track record of leadership in standards and integration. Historically, point product vendors competed on features, not integration. Now, success requires support for an open, manageable, and unified security and compliance environment.

Solutions

Continuous monitoring streamlines costly security operations to help senior federal officials gain greater visibility into their organization's security health and precise information for continuous risk management. An effective implementation collects data from ongoing processes, correlates against multiple contextual factors, takes action automatically where appropriate, and presents the remaining issues in priority order. The most important and at-risk assets receive the most immediate and significant resources.

Most organizations have baseline capabilities in antivirus, operating system, and application patching assessment, along with SCAP-enabled products to evaluate FDCC/USGCB compliance. To embrace continuous monitoring, organizations typically invest first in real-time asset discovery and vulnerability management, intelligence-driven response, and continuous feedback. Open interfaces and standard protocols help agencies integrate these systems with each other and with existing infrastructure at minimal cost.

"The Risk Management Framework (RMF) developed by NIST describes a disciplined and structured process that integrates information security and risk management activities into the system development life cycle. Ongoing monitoring is a critical part of that risk management process. In addition, an organization's overall security architecture and accompanying security program are monitored to ensure that organization-wide operations remain within an acceptable level of risk, despite any changes that occur. Timely, relevant, and accurate information is vital, particularly when resources are limited and agencies must prioritize their efforts."

—NIST SP 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations

Real-Time Asset Discovery and Vulnerability Management

Effective asset management systems combine passive and active discovery and monitoring to detect and profile every system using the network, independent of operating system or form factor. Passive scanning monitors traffic to see which devices are alive. Active scanning probes the network to track down idle devices. Together you achieve full and constant visibility into network usage. As soon as a user installs or reconfigures a device on the network, the change is visible and the device can be assessed.

Effective vulnerability management solutions will expose how devices are configured, what vulnerabilities they have, if they are compliant with policies, and what risk they pose. Since applications are common targets for exploitation, this assessment must look beyond the OS, up the software stack and across different vectors to see web and database vulnerabilities. As vulnerabilities and threats change, the system should automatically update relevant checks to detect the latest issues and guide improvements.

Intelligence-Driven Response

The system should then translate this security state into quantified risk scores that factor in current threat intelligence and other context. Some low-impact events become high impact when viewed in conjunction with other activities.

Administrators invest up front in determining asset value and policies, and then risk-based scoring guides the system to the appropriate response. Where possible, the system acts instantly, leaving a verifiable audit trail. Where necessary, the system triggers rapid human intervention. Fixes like a new software .DAT or patch deploy automatically to remediate devices that are at risk—at machine speed. Anomalies in behavior trigger an alert for administrators to investigate.

This ongoing process correlates all the data collected on assets and vulnerabilities with live events taken from global and local intelligence feeds, such as vulnerability research and CERT alerts on government-specific events. Two other factors come into play: the countermeasures that could nullify a threat or vulnerability, and the value of the asset at risk. The right response to each incident should factor in true risk and potential impact on the mission.

Continuous Feedback

A command and control center manages these processes in a feedback loop. With integrated systems acting at machine speed to address the bulk of events, government staff can focus on monitoring what they know are the high-impact factors; fine-tuning policies, processes, and controls based on results; and investigating subtle and anomalous events. Flexible dashboards display information, automate response workflows, and facilitate communication among team members. The larger and more distributed the team, the greater the operational value from an accurate, contextual picture of risk and a centralized monitoring and management system that can scale, adapt, and overcome new risks—continuously.

Through integration of real-time system assessment, up-to-date threat intelligence, effective controls, and ongoing feedback, a continuous monitoring program saves government resources and reduces the chance of a disruptive network event. This perpetual feedback loop is the first step toward actually utilizing the output from CyberScope. As agencies engage in continuous monitoring, they may choose further analysis and correlation with the data they report that may even simplify FISMA reporting and other requirements that traditionally have a high time to utility ratio. These processes become the core of a healthy risk management lifestyle.

Best Practice Considerations

- Compliance with and reporting against CIS, DISA STIG, NIST, USGCB/FDCC standards, as well as FISMA, FedRAMP, and CyberScope
- Support for the standard content adaptation protocol (SCAP)
- Plug and play interoperability among task management, collection sensors, databases, presentation/reporting systems, and analysis/risk scoring systems for the CAESARS data domains
- Flexible automation that streamlines workflows across these subsystems and helps guide systemic and human-assisted incident response
- Open APIs to extend CAESARS to enterprise and coalition partners and support multitier networks
- Real-time threat and vulnerability feeds that drive dynamic vulnerability and risk assessment and make the system smarter
- Capacity to handle the speed, scope, and scale of security data feeds and reporting requirements

Value Drivers

Solutions for continuous monitoring need to provide security and compliance controls, but they also need to reduce complexity and maximize ROI. These solutions should:

- Support open standards and open platforms to leverage existing technologies and minimize integration and maintenance costs
- Reduce administrative staff, helpdesk calls, audit costs, errors, and manual compliance tasks
- Improve detection, increase the frequency with which attacks are thwarted, and reduce the volume and impact of events that must be responded to, investigated, and remediated
- Improve resilience through feedback loop incorporating state of the art detection and real-time remediation
- Enhance flexibility to respond to economic, political, and technological requirements
- Deliver an efficient IT architecture that reduces platform hardware and software usage, power and HVAC consumption, and rack and floor space

Related Material from the Security Connected Reference Architecture

Level II—Solution Guides

- Achieve Resilient Cyber-Readiness
- Operationalize Intelligence Driven Response
- Protect Critical Infrastructure
- Protect Your Information

Level III—Technology Blueprints

- Assess Your Vulnerabilities
- Achieve Situational Awareness
- Deliver Continuous Compliance
- Optimize Log Management
- Investigate Data Breaches
- Look Inside Network Traffic

For more information about the Security Connected Reference Architecture, visit: www.mcafee.com/securityconnected.

About the Author

Dr. Phyllis Schneck is Chief Technology Officer for Global Public Sector at McAfee. In this role, she is responsible for the technical vision for products and service for public sector as well as global threat intelligence, industrial control system security, and telecommunications strategy. She is also driving strategic thought leadership around technology and policy in cybersecurity and leading McAfee initiatives in adaptive security and intelligence in networks for critical infrastructure protection and cross-sector cybersecurity. For more than 14 years, Schneck has had a distinguished presence in the security and infrastructure protection community, most recently as a commissioner and a working group co-chair on public-private partnership and a working group chair on network situational awareness for the CSIS Commission to Advise the forty-fourth President on cybersecurity. Schneck recently co-chaired the Critical Infrastructure Protection (CIP) Congress and is leading the follow-up effort for the first global strategic plan for CIP. Schneck is also the chairman of the board of directors of the National Cyber Forensics and Training Alliance, a partnership among corporations, government, and law enforcement for cyberanalysis to combat international cybercrime. Schneck also serves on the NIST Information Security and Privacy Advisory Board. Schneck was recently named the Loyola University Maryland David D. Lattanze Center 2012 Executive of the Year.

McAfee
An Intel Company

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

54801sg_continuous-monitoring-L2_1112_wh