



MANAGE SECURITY AND RISK



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.

Download the latest resources at mcafee.com/securityconnected.

Get Proactive About Managing Risk

Challenges

Compliance and financial risk used to be the driving concerns for security and risk management. Audits and governance processes were predictable events that IT attempted to minimize and automate. Risk was a fairly static concept. However, today the pace of threats—“low and slow” as targeted attacks or lightning fast as cyberactivism and malware outbreaks—demands that executives and IT administrators pay more attention to unfolding events and make rapid risk-based decisions on mitigation.

Of course, compliance and financial risk have become dynamic too. Consider that regulators independently refine more than 200 guidelines around the world as the surging economy reshapes business opportunity. That once static risk picture now fluctuates like a kaleidoscope.

Dig through Big Security Data

Managing risk today means making sense of more data: vulnerability scans, application and database logs, flows, access and session records, alerts, and trending analysis. Data streams originate from multiple systems protecting more users with more devices in more places.

Audits—whether internally or externally driven—showcase the pain of managing data from this plethora of sources. IT administrators must track down and collate data streams into the preferred format for the auditor’s consumption. Audits are by definition a backward-looking and static assessment of past risk. They sap organizational resources and detract from proactive risk management—the ability to look forward, to understand and mitigate changing risks before they do damage.


Evaluate risk

This world is a “Big Data” environment—big security data. Understanding subtle security threats can take days or months. Most security analysts experience comparable data issues to IT administrators fulfilling audits: that plethora of independent data streams makes it hard to form a concise and coherent picture of events. The bigger the mass of data being collected and analyzed, the more chaotic it seems and the longer it takes to reconstruct events. Only after the picture is complete—well after the event—can policies and protections be adjusted to prevent a repetition.

What if the attack is fast and furious—a denial-of-service attack or rapidly spreading worm? Taking days or months to diagnose the problem could permit a tremendous—potentially fatal—compliance and financial impact. Which assets are genuinely at risk to the threat and which have compensating controls or countermeasures? To answer this question, administrators need visibility into the security state of the full range of systems, including the expanding collection of mobile and personally owned devices accessing their networks.

Act on events

After understanding come triage and remediation. Which assets matter the most? Which can wait? Administrators often swivel between different management consoles to run scans, execute scripts, adjust policies, install updates, or quarantine systems. Each product that crowds the security market adds cost and complexity: another user interface, data format, policy standard, or report. Inevitably, there are coverage gaps and mistakes that expose the organization and its assets to unnecessary—and usually unrecognized—risk.



You can no longer manage risk from the rearview mirror. You must look forward—using a wide-angle lens—to identify and manage risk as it changes. Situational risk intelligence provides access to dynamic context about the global threat environment and your enterprise's assets and security posture. Automated risk management technologies use this context to help you continuously connect the dots to tune policies and protections.

Solutions

Big Security Data and its operational issues complicate security and risk management, but a comprehensive strategy coupled with modern technology will help make sense of the chaos. Within the context of compliance and financial risk management processes, you need to consider, in real time, the possible risks introduced by external and internal events. Unifying these efforts streamlines processes and supports automated responses that cut costs and response time. Executives gain visibility into the potential impact of security events on risk posture, while administrators gain the insight and control to mitigate risk proactively.

Modern security and information event management (SIEM) systems couple closely with security and compliance management of devices, servers, networks, applications, and databases. This security management platform can provide a command and control core that facilitates visibility and operational agility. The more closely these systems integrate with each other, with risk intelligence, and with security systems, the more easily you will be able to understand and manage risk. A platform approach aligns and unifies individual and fragmented processes, policies, workflows, and reports. Incorporating up-to-date intelligence places data in the context of changing risk and helps improve accuracy, relevance, and response time to lower risk.

Assess vulnerabilities

Most regulated entities scan for vulnerabilities in support of compliance mandates. However, scheduled scans routinely miss remote and hibernating systems or bypass business-critical assets like applications and databases. Rogue systems may go unnoticed, harboring exploitable vulnerabilities. A conscientious approach to managing vulnerabilities across networked assets can accommodate these diverse systems and eliminate compliance gaps. You can use dynamic risk intelligence, asset value, and relevant countermeasures to direct scans or implementation of compensating controls.

Enhance situational awareness

In the face of cyberattacks and porous perimeters, most organizations want to better comprehend and respond to changing risks. The key is finding the data that matters, while it still matters. With the speed and capacity to handle Big Security Data, SIEM tools can monitor applications and databases, manage logs, and normalize events into correlated dashboards. Some also integrate a real-time understanding of the threat landscape as well as users, systems, data, risks, and countermeasures. With this rich contextual picture, you can quickly understand security-related activity, including historical activity. Robust analytical tools help you forecast and pinpoint attacks and remediate threats in minutes instead of days.

Look inside network traffic

Networks represent both critical infrastructure and pipelines that can leak sensitive, regulated data. By monitoring and managing network traffic, including encrypted traffic, administrators can reduce undesirable or risky Internet and application use and ensure content policies are enforced. The integration of next-generation network security with SIEM and system security can help risk managers enforce policies, defend against zero-day threats, and monitor, analyze, and report on compliance.

Optimize log management

Logs provide a wealth of data that supports e-discovery, audits, and other compliance requirements—if you can absorb and cull data feeds to find the facts. With an integrated, secure, high-performance log management solution, you can collect data in real time from all relevant sources and preserve logs according to a secure chain of custody standard. Application control can ensure that attackers do not hijack logging systems to hide their actions. Connecting log management functions into other security and risk analytic functions helps get log data into the hands of those who can best use it to manage risk.

Best Practices Considerations

- Align and unify fragmented processes and controls
- Automate collection, correlation, assessment, response, and monitoring
- Leverage dynamic risk intelligence, what-if analysis, and policy-based response to proactively identify and block threats
- Ensure security and risk programs cover all devices, data, and IT infrastructure
- Pull together all security and risk information across the enterprise into one platform for more efficient and effective management
- Monitor the situation continuously and proactively to detect and respond to changing risk, maintain compliance, and prevent future security events

Manual security and risk processes have a higher likelihood of failure and are a primary driver of increased security and compliance costs.

Deliver Value

A comprehensive security and risk management strategy enabled by a risk-aware and automated management platform will help your organization:

- Achieve meaningful situational awareness through rich context and analysis
- Diagnose and respond to incidents in seconds, not hours, to reduce damage, prevent data breaches, and lower remediation costs
- Experience fewer security and compliance incidents and lower per-incident costs
- Simplify compliance policy processes and reporting to improve operational efficiency
- Reduce the number of vendor platforms, hardware, and software used for security management
- Reduce training time and operational cost

Related Material from the Security Connected Reference Architecture

Level II

- Controlling and Monitoring Change
- Protecting the Data Center
- Obtaining Benefit from PCI

Level III

- Assess Vulnerabilities
- Enhance Situational Awareness
- Look Inside Network Traffic
- Optimize Log Management
- Investigate Data Breaches
- Live with Social Media
- Protect Intellectual Property

For more information about the Security Connected Reference Architecture, visit:

www.mcafee.com/securityconnected.

About the Author



Barbara G. Kay, CISSP, is principal industry analyst at Secure By Design Group. She specializes in information protection for distributed and mobile enterprises and consumer education on safe Internet use. Prior to forming Secure By Design in 2006, Barbara was Director of Marketing for Sun's Security and Privacy Initiative. She is a graduate of Dartmouth College.

