



BUYER CASE STUDY

Fashion Retailer Employs McAfee Risk Advisor to Automate Compliance and Risk Management Requirements

Vivian Tero

IDC OPINION

Using a risk-based approach to address vulnerabilities and threats as well as meet compliance obligations is useful for aligning IT operations with security. In more detail:

- ☒ A risk-based approach allows for more intelligent prioritization of the risk mitigation and remediation activities.
- ☒ To achieve this approach, organizations should consider solutions that highlight the relationship between the threats and vulnerabilities with the assets, the technical controls, and the compensating controls. Exposing the criticality of the data and application and the existence of countermeasures allows for effective allocation of resources, supports continuous improvement (thus fewer surprises), and mitigates hyper-enforcement.

IN THIS BUYER CASE STUDY

This IDC Buyer Case Study highlights the selection process and implementation of McAfee Risk Advisor by a United States-based fashion retailer. The organization employed this application to facilitate its security compliance, system uptime, and risk management operations.

SITUATION OVERVIEW

Organization Overview

In December 2010, IDC interviewed the security engineer for IT risk and compliance of Corp. A (name withheld upon request), a U.S. fashion clothing and accessories retailer. Corp. A is listed in the NYSE and reported revenue of \$1.8 billion in 2010. The retailer operates 590 stores and offers online shopping. A private equity firm owns a significant majority (75%) of the organization. Prior to its 2007 sale to a private equity firm and its eventual IPO in spring 2010, Corp. A was owned by High Street Fashions (name also withheld upon request). High Street Fashions is a global fashion retailer and has annual sales of over \$9 billion. Its portfolio includes high-end department stores, lingerie, skin care, cosmetics, and home accessories.

Challenges and Solution

Challenges

The following external developments prompted the update of Corp. A's IT security and compliance operations and the subsequent acquisition of McAfee Risk Advisor:

- ☒ Prior to the sale of Corp. A to a private equity firm in 2007, IT operations, security, and PCI compliance were provided by High Street Fashions' internal IT infrastructure.
- ☒ A planned IPO for spring 2010 required that Corp. A have the processes and technical protocols in place to address IT security operations and uptime system requirements, as well as PCI-DSS compliance objectives.

Corp. A's IT organization had at least 25TB of data to secure and manage between two datacenters, 590 stores, and over 250 servers across Windows and Unix environments. Postsale and prior to its planned IPO, Corp. A had 18 months to decouple its IT and security operations from High Street Fashions' IT infrastructure and build its own IT organization and service operations. The IT organization's primary objectives were to identify its IT vulnerabilities and threats, define and deploy the appropriate detective and preventive controls across discrete functional operations (such as endpoint security management, log management, threat management, patch management, and change and configuration management), and effectively correlate reports on risk feeds and threats to Corp. A's network and countermeasures.

Solution

In the run-up to completely decoupling its IT operations from High Street Fashions' IT network, Corp. A's IT organization spent several weeks with its business managers and IT admin functions to identify the critical assets (processes, data, applications, and people) and the associated operational security and compliance requirements such as system uptime and availability, business criticality, confidentiality, and compliance auditing and reporting. The team also took this opportunity to define the risk levels and control objectives, technical controls, and compensating controls. To address PCI-DSS compliance, for example, the team broke down the 220 subrequirements into discrete projects. (Note: To be PCI compliant, merchants and retailers need to demonstrate compliance to the 6 PCI-DSS control objectives and 12 major requirements, which are further broken down into approximately 220 individual subrequirements. For more on this, see www.pcisecuritystandards.org/security_standards/index.php.) The team identified the assets and tools needed to meet those objectives and subrequirements. Projects were prioritized according to the mandated audit and reporting deadlines, the criticality of the assets and/or processes, and the absence of countermeasures. The Corp. A IT team also used this opportunity to identify the areas for automating mundane, everyday IT ops tasks and for cutting down time for event and incident analysis and correlation.

Corp. A evaluated the McAfee and Symantec security operations, endpoint protection, and compliance products as well as the product offerings from Qualys. In

the end, the organization selected the McAfee portfolio, including ePolicy Orchestrator (ePO), McAfee Risk Advisor, McAfee Endpoint Protection, and McAfee Vulnerability Manager. Corp. A noted the ease with which McAfee Risk Advisor enabled the organization to correlate threats and vulnerabilities to existing countermeasures. Given Corp A's operational and time constraints, the organization viewed McAfee Risk Advisor's ability to prioritize and focus its remediation, configuration, and patch management efforts as a critical differentiator.

McAfee Risk Advisor

McAfee Risk Advisor is an optional module offered under McAfee's Total Protection for Compliance suite. This solution uses agent-based and agentless technologies to assess and report the operational security and compliance postures across networks, endpoints, applications, and databases. McAfee Risk Advisor integrates with McAfee ePolicy Orchestrator, McAfee Policy Auditor, McAfee Host Intrusion Prevention, McAfee Vulnerability Manager, McAfee Network Security Manager, and McAfee Labs' Global Threat Intelligence service. By taking advantage of the preexisting integration of Risk Advisor with the ePO platform, organizations are able to automate the audit process and correlate threat information with vulnerabilities and deployed countermeasures.

Results

Corp. A's IT operations and security team identified the following benefits from the McAfee Risk Advisor deployment:

- ☒ Enable the team to conduct a first PCI-DSS assessment as a discrete entity (with some initial assistance from the High Street Fashions infrastructure) prior to Corp. A's IPO.
- ☒ Prioritize patch management and endpoint security management and remediation efforts. Since the analysis highlighted the relationship between the threats, the vulnerabilities, the business criticality of the assets and processes, and the existence of compensating measures, the Corp. A team did not have to scramble and immediately issue a patch for every red flag or alert that appeared on the security management console. For example, patches for less critical assets with known countermeasures were done during scheduled operations, while critical assets and vulnerabilities were addressed immediately. Risk Advisor provided the foundation for creating the appropriate risk remediation and mitigation workflows.
- ☒ With Risk Advisor, Corp. A enhanced productivity; it was able to effectively tweak operations and test patches on a tiered basis resulting in less break-fix. Corp. A estimates that this risk management approach saved the company at least one dedicated FTE for patch and vulnerability management.
- ☒ Set the foundation and technology strategy for introducing new technologies and IT services securely.

- ☒ Solicit buy-in from business owners by allowing them to expose the dependencies between the business assets, the security controls, and the state of compliance or noncompliance of those assets.

ESSENTIAL GUIDANCE

IDC offers the following essential guidance for organizations looking to deploy an IT GRC management application:

- ☒ Understand the short- to long-term GRC objectives of the IT organization. Key questions to ask include: What are the critical IT and business assets? What is the level of IT and process integration required to manage risk and compliance? Where are the areas that would benefit most from automation? How do security, compliance, and privacy requirements impact future plans for introducing new applications, technologies, and services into the organization?
- ☒ Identify the security and compliance deadlines as well as audit and reporting requirements. Organize requirements and deadlines into discrete, incremental projects. This will help the organization prioritize projects, identify gaps, and map out the road map for the deployment and scale out of the GRC solution. It would also serve as a foundation for mapping out its GRC technology strategy for future upgrades, application decommissioning, and the introduction of new IT services and applications. In Corp. A's case, the road map included plans for automating key SOX assessment, audit, and reporting activities; addressing third-party risk management, audits, and assessments; and integrating with a GRC management platform in support of its enterprise GRC program.
- ☒ Understand the GRC "challenge" that you are trying to address. In this Buyer Case Study, Corp. A's initial priorities were to meet PCI and data and application availability objectives. Automation, risk prioritization, and intelligent remediation were key requirements. As a result, they gravitated to solutions that facilitated the continuous and integrated controls of IT operations and security processes. Corp. A indicated its intent to acquire and eventually integrate with a compliance management platform and employ McAfee Risk Advisor for SOX compliance. Failure to understand the motivation would oftentimes end up with buyers comparing enterprise GRC management platform applications with those that focus on the testing and audit of specific IT controls.

LEARN MORE

Related Research

- ☒ *McAfee FOCUS 2010: "Security Connected" Strategy Would Enable Continuous Control of IT GRC from Silicon to Satellite* (IDC #225455, October 2010)

Copyright Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/offices. Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or Web rights.

Copyright 2011 IDC. Reproduction is forbidden unless authorized. All rights reserved.