



IT Collaboration Equals Success

Overview

Enterprise IT knows about continuous innovation. In a never-ending quest to adjust to a business environment changing at an accelerating rate, IT created specialized teams—the network operations center (NOC), the security operation center (SOC) and audit groups—to manage increasingly sophisticated threats, evolving regulations and new reporting mandates. These specialized teams continually deploy point solutions that are complemented by best practices within each focus area. While this approach may tactically meet the requirements of each area independently, it typically creates silos of incompatible data that hinder effective cross-functional business decision making.

A new challenge emerged as teams, whether accountable for network availability, information security, or compliance and risk management tasks, discover that day-to-day operational decisions have impact beyond any single functional area. Therefore, decision-making requires a broader perspective supported by consistent enterprise-wide data. Functional point solutions have become less efficient and effective as teams face growing complexity and interdependency. Today, IT's success depends upon solutions that improve cross-team communications and collaboration.

This challenge has led to a new set of cross-functional solution requirements based on enterprise-wide collaboration. These requirements define next-generation security information management (SIM)—with comprehensive solutions designed to extract, correlate and analyze actionable information from a mixture of log, vulnerability, configuration, asset, performance and network behavioral anomaly data from across the enterprise. In some cases, these solutions integrate IT governance, risk and compliance (GRC) management functionality to provide a more comprehensive platform that unifies security, risk and audit management. Such platforms complement traditional point solutions by providing a common foundation for team collaboration. They present IT teams with an integrated framework for effective decision making.

IT's Growing Interdependency of NOC, SOC and Audit Management

The technologies and architectures used to build and implement IT business services are increasingly sophisticated, interdependent and dynamic. The complexity of the infrastructure, applications, management and reporting demanded from NOC, SOC and audit teams also continues to expand and grow.

Data and information security is assuming a leading role in IT's portfolio of business services due to increasingly sophisticated attacks whose objectives extend beyond information and asset theft. For example, attempts may be made to disrupt order entry operations, to acquire and corrupt private customer data, to block proper use of expensive resources through denial of service attacks, and so forth. The recent Nugache Trojan with the ability to constantly change a network of distributed peer connections is indicative of the significant leap forward in malware quality. Secure operations and asset management have become major management issues. IT must not simply secure assets such as infrastructure and data, but also respond to and base operational decisions on business impact and risk assessment. This requires cross-functional coordination, communication and information sharing.

The NOC, key to IT Operations, is responsible for the network—the communications pathway within and outside the enterprise. A network failure or slowdown can have catastrophic consequences for the entire business. The NOC also makes decisions which broadly impact business operations as related to data and information security, service levels and repairs, transaction integrity, and customer response times and satisfaction.

The SOC, another key IT team, is responsible for analyzing and assessing risk as well as identifying and evaluating general security measures. After determining acceptable levels of security and risk, the SOC develops policies and procedures to manage to those acceptable levels. They must also define the action taken when violations occur. Their enterprise role and access to nearly all corporate data and assets, makes them the controlling authority for implementation, monitoring, management and reporting of these processes.

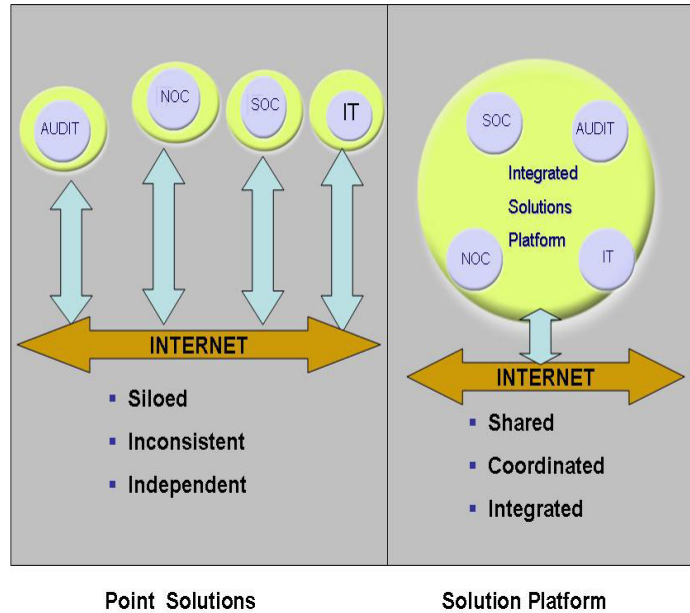
Concerns over corporate malfeasance, both real and perceived, have driven the creation of audit teams to manage the growing burden of operating, monitoring and reporting mandates. Directives from government, internal oversight and regulatory bodies require audit teams to define procedures for monitoring and reporting on compliance efforts. Non-compliance penalties can be harsh and applied both into and beyond the executive suite. Typically, audit teams establish policies, set procedures and create reports on the effectiveness of compliance efforts.

In summary, NOC teams set policy, and design and maintain the IT infrastructure for the business. SOC teams identify threats, and establish policies and procedures to address and manage security incidents as they evolve. Audit teams assure proper governance, quantify acceptable business risk levels, set policies to assure compliance, and report on implementation and effectiveness of such efforts. Each functional team is likely to significantly impact the others

with its decisions and programs related to information security, risk and audit management. Now let's look at what this means in terms of solution requirements.

A New Set of Security, Risk and Audit Management Requirements

NOC, SOC and audit teams began as siloed functions—a result of organizational dynamics and initial failure to recognize interdependencies and the need for collaboration. The majority of tools used by these teams are point solutions complete with their own individual data repositories, collecting mechanisms and analytics. Each team operates independently, creating policies and reports with little, if any, coordination or collaboration because they rely on their own tools.



While the necessity for the best and most current security technology for a specific focus—such as the best firewall, VPN or virus checker—remains paramount, today's security, risk and audit management challenges are generating a larger, more comprehensive set of solution requirements. The new requirements expand existing best-of-breed solution technology by adding a focus on team collaboration, consistent data that is correlated across the enterprise, and flexibility to adapt to automatically discovered changes across functions.

Best-of-Breed Technology

Currently, most solutions available to NOC, SOC and audit teams are point solutions designed to address only parts of the problem. Such solutions take a one-dimension view of the problem, the data and the operations. They solve problems in the context of a specific focus, but do not promote interdepartmental collaboration. They lack the ability to correlate across multiple silos of security data, thus resulting in a failure to detect critical security breaches, policy violations and data theft. Integrated security, risk and audit management solutions are now available to complement point technology. By correlating data across the enterprise, an integrated platform

facilitates team coordination and collaboration while minimizing inefficient, counter-productive decision making.

Enhanced Communication and Collaboration between Teams

IT must not only secure assets, but must also respond to and adjust operational decisions to consider business impact and risk assessment. This requires cross-functional coordination and communication as well as information sharing. A solution should allow the consolidation of management and operating tasks across organizational as well as functional boundaries while coordinating inter-team collaboration.

The solution acts as a platform for integrating infrastructure management functions as implemented and run by operations (security, asset, performance, events, problems, analytics, compliance and reporting), and as required by functions such as security (information collection, risk analysis, policy setting and process monitoring). These, in turn, support enterprise initiatives (compliance and controls measurement, monitoring and reporting).

Coordination and collaboration among the teams assures accurate information is available to serve as the basis for decision making. Data can be easily shared in real time and analysis performed. For instance, the NOC can be alerted when a configuration change violates a security policy. The SOC can be warned when a policy mandate violates Service Level Agreements, and the audit group can be informed when compliance is impacted.

Synchronized, Consolidated and Shared Data

To meet evolving security, risk and audit challenges, data must be accessible through a consistent interface with multiple silos consolidated into a single entity. Typically point solutions require significant customization to provide such coordination, and therefore, can lead to inefficiencies. Problems occur when decisions made by one team impact the task of another. For example, when two teams separately collect data using different tools in varying formats at different times, the resulting data stores cannot be synchronized, leading to inconsistencies. Such data, when analyzed, yields bad information, resulting in wrong conclusions and poor decisions. Implementing point solutions means having to build a separate correlation engine via system integration work that may not effectively identify problems. The end result is reduced efficiency, increased costs and frustrated staff.

Comprehensive, End-to-End View of Data

Information presented in a different way to each team decreases the benefits of data synchronization. A solution should permit comprehensive end-to-end viewing. This enables effective cross management of the infrastructure's operating environment and its constituent parts, providing a consistent portal for data collection, correlation, archiving, visualization, monitoring, forensics, reporting and process implementation. An adaptable interface can meet the viewing, analysis and reporting needs of different teams. This allows access to a common portal for specific functional information when creating and implementing new processes, while still enforcing the coordination of changes to existing processes.

Flexibility and Scalability to Adjust to Operational Growth

The technology infrastructure underlying the enterprise is far from static so a solution must be adaptable, extensible and scalable to satisfy both evolving technological complexity and the sophistication of its utilization in support of the business. For example, SOC and NOC teams require the integration of functions such as log management with analytics for performance, vulnerability, asset, configuration and network behavioral anomaly detection. Audit teams require definition and management capabilities for building control frameworks, integrating regulation changes, as well as extending and modifying policies and standards. Change will continue to accelerate, teams will be added and therefore, platform operations (discovery, analytics, reporting) must be automated and self-monitoring.

Dynamic Discovery of Changes

Not only is the infrastructure not static, but its rate of change accelerates as the business environment continually evolves. Therefore, a solution must also include a centralized, dynamic ability to discover changes in or near real time. Automated and timely discovery is essential to maintaining high-quality, cross-functional data and the interdependent team decisions that rely on such information.

Which Approach? Point or Integrated?

While these new requirements are nearly universal, the relative need for each varies from organization to organization. The right approach—point solution or integrated platform—for the best enterprise fit depends on enterprise culture and competitive environment. A well-developed and functioning culture of coordination, cooperation and communication can mold point products into effective tools—if IT is able to customize solutions. However, this can require intensive custom integration at a tool level. Additionally, as organizational complexity grows and

dependencies increase, adding siloed solutions can become expensive and labor intensive to implement and manage.

As a result, there has been a gradual shift away from point solutions to integrated security, risk and audit management platforms that complement existing technologies. Enterprises in rapidly evolving and highly competitive business and technology environments benefit the most from an integrated platform solution. Such solutions are designed for environments requiring prompt responses and fast adaptation to change in services, delivery mechanisms, reporting requirements or operations, whether driven by customer demand, security threats, business opportunity or risk.

An integrated platform solution allows the consolidation of management and operating tasks across organizational and functional boundaries. It provides a consistent, shared user-interface while permitting customization to meet user needs. Cross-group coordination and collaboration assures consistent data, the basis for accurate information for decision making.

Automatic data processing provides each team the information necessary to decide what and when to take action. An integrated platform allows IT to implement process changes dynamically to respond quickly to change requests, operational problems or new business priorities. As compliance reporting mandates change, report context also changes. A fully integrated solution with consistent analytics allows prompt generation of reports to meet new requirements.

Conclusion: An Optimal Solution

The role of IT in the enterprise is changing as NOC, SOC and audit teams face increasing demands to deliver and manage services to support new business functions. As IT gains more responsibility, their impact on and accountability for results grows. The complexity of next-generation security, risk and audit requirements will make today's demands appear trivial in comparison.

Siloed operations and point solutions are a blueprint for failure in an increasingly complex, connected and interdependent operating environment, where supporting sophisticated processes that extend across organizational and functional boundaries is the norm. New mandates in response to increasingly sophisticated security threats and identity theft require a comprehensive, detailed end-to-end view of what is happening anywhere, at anytime along with the ability to quickly respond to, remediate and report on the situation.

<i>Solution Requirement</i>	<i>Existing Point Solutions</i>	<i>Integrated Platform Solution</i>
Best-of-Breed Technology	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Enhanced Communication and Collaboration between Teams		<input checked="" type="checkbox"/>
Synchronized, Consolidated and Shared Data		<input checked="" type="checkbox"/>
Comprehensive, End-to-End View of Data		<input checked="" type="checkbox"/>
Flexibility and Scalability		<input checked="" type="checkbox"/>
Dynamic Discovery of Changes		<input checked="" type="checkbox"/>

**Table 1 - The New Cross-Functional Solution Requirement Matrix
(Courtesy of eIQnetworks, Inc.)**

Table 1 summarizes why an integrated platform approach provides the automation, collaboration and integration capabilities needed to meet new cross-functional solution requirements. Complex and changing business environments increase dependencies and the need for collaboration.

In summary, the integrated platform approach is not a replacement for point solutions; instead it complements existing technology by correlating data across the enterprise. Data unification across functional areas facilitates team coordination and collaboration while minimizing inefficient, counter-productive decision making. In so doing, this solution approach delivers enhanced competitive advantage through IT's management of information security, business operations support and regulatory compliance.

This Research Brief was sponsored by eIQnetworks, Inc.

This document is subject to copyright. No part of this publication may be reproduced by any method whatsoever without the prior written consent of Ptak, Noel & Associates LLC.

All trademarks are the property of their respective owners.

While every care has been taken during the preparation of this document to ensure accurate information, the publishers cannot accept responsibility for any errors or omissions.

About Ptak, Noel & Associates LLC

With a belief that business success and IT success are inseparable, Ptak, Noel & Associates LLC works with clients to identify, understand and respond to the implications of today's trends and innovations on the future of IT Operations.

www.ptaknoelassociates.com