A Guide to NetOps and SecOps Collaboration

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Written by Shamus McGillicuddy, Q1 2019

Prepared for NETSCOUT

EMA™
IT AND DATA MANAGEMENT
RESEARCH | INDUSTRY ANALYSIS | CONSULTING

EXECUTIVE SUMMARY

This white paper draws on EMA research to offer a step-by-step guide for building partnerships and collaboration between enterprise network and security teams. It explores why this collaboration is essential, and how enterprises can reap rewards from NetOps and SecOps partnerships. In particular, it reviews how tools, data, and processes are essential to success.

NETWORK AND SECURITY TEAMS NEED TO COLLABORATE

IT executives need to bring their network and security teams together. The reality of today's digital infrastructure demands the collaboration, if not convergence, of these groups. For instance, it is increasingly difficult to discern whether an IT service event is a performance issue or a security incident. Enterprise Management Associates (EMA) research found that the two most common root causes of complex IT service problems that drive cross-domain responses are network infrastructure issues (40 percent) and security events (37 percent).[1]

Security is also a strategic priority for network teams. Security risk reduction has emerged as the fastest-rising measure of success for network teams, more so than service quality, network visibility, and end-user experience. As enterprises deploy software-defined data centers and public and private cloud architecture, security becomes even more essential to the network team. For instance, network managers who support public cloud initiatives say supporting cloud access is the most challenging aspect of cloud enablement.

Network and Security Collaboration is Already Common

Ninety-one percent of enterprises have at least some formal collaboration between their network and security groups. Forty percent have fully converged these groups with shared tools and processes, although this is more common among small and midsized enterprises where traditional organizational silos are less established. Another 35 percent of security groups enable collaboration by integrating the toolsets of network and security teams, and 16 percent have deployed tools that the network and security teams share.

EMA research identified three leading drivers of network and security team collaboration. First, it engenders cost efficiencies in operational expenses. Second, it reduces overall risk. Third, it shortens the mean time to insight or mean time to resolution of security incidents and security problems.

However, this collaboration isn't easy. Network managers have identified several key barriers to success. The top challenge is that the industry hasn't established a set of defined processes or best practices for such collaboration. Network teams and security teams also typically have different goals in mind when they come together. A mandate to lock things down drives the security team, while the network team is charged with connecting people to data and services. Additionally, network and security teams say they lack a shared data store that is consistent, current, and relevant to the task of collaboration.

COLLABORATION 101: FROM INFRASTRUCTURE DESIGN TO OPERATIONAL TOOLS

EMA recommends that IT leaders take a four-pronged approach to fostering network and security team collaboration. First, these groups should take a transformational view of this collaboration. It's not only about operations, but also about infrastructure. Second, enterprises should build a data store that both teams can use. Next, they should adopt the right toolset for collaborative workflows. Finally, enterprises should formalize this collaboration every step of the way with documented policies, controls, and best practices.

[1] EMA first published all the research data cited in this paper in "Network Management Megatrends 2018: Exploring NetSecOps Convergence, Network Automation, and Cloud Networking," April 2018.

Begin at the Design Stage

EMA research found that the most critical point of collaboration between network and security groups is at the infrastructure design and deployment stage, while incident monitoring and incident response are secondary. Digital transformation demands collaboration at the design stage. Cloud, software-defined WAN solutions, virtualization, the Internet of Things, and mobility are all combining to destroy the security perimeter. Communications infrastructure must deliver security natively.

Find a Single Source of Truth in Your Data

Collaboration will require a single source of truth, specifically regarding data. Network teams and security teams need to share data to ensure their analysis is based on the same set of basic truths. If one team is working with outdated information, they won't be on the same page as the other team. If one team has too many blind spots, they won't be able to partner effectively with the other team. Many network and security tools already leverage the same data, such as packets and flows. Choosing the right data is essential for successful collaboration. Smart data must be able to support workflows without requiring management tool architects to cobble together multiple secondary data stores to prop it up.

Network visibility fabrics (taps, network packet brokers, etc.) are a good place to start. In fact, 51 percent of enterprises that use these fabrics have formal processes and best practices that govern how network and security teams collaborate on data collection. This collaboration leads to better data. Organizations with formal collaboration on these fabrics tend to monitor a larger percentage of network segments, ensuring there are fewer blind spots for security and network operations.

Select the Right Tools for Collaboration

Network managers say network performance monitoring and advanced network analytics are the two most essential tools for collaboration. EMA has observed network performance management solution vendors leveraging their core technology to deliver security solutions or to add security features in their products. Given that network performance and security incidents are often intertwined (one might cause the other, and vice versa), performance management tools can identify possible security incidents and they can help analysts understand how a security incident is affecting performance.

People often look at advanced network analytics tools as a separate product, but EMA research found that many enterprises prefer to consume advanced analytics technology as features embedded in their existing network operations tools, particularly network performance management tools. Network managers also say that integrated, security-related insights are the most valuable product features in network management solutions. Furthermore, 33 percent of network managers require their network management tools to integrate with their company's security monitoring solutions. Forty-two percent of network managers provide the security team with custom views or role-based access to their network management tools.

Enterprises should also leverage automation for this collaboration. Ninety-two percent of network managers are expanding network automation, and 70 percent say it's a top priority. Their number-two target for network automation is security incident response. They are seeking tools that can detect suspicious activity, automatically mitigate security incidents, and make analytically-derived recommendations on further action. These forms of automation will make the network team a valuable partner with the security group.

Formalize This Collaboration

Enterprises must formalize this collaboration. While network teams and security teams can derive significant benefits from working together, they are not natural partners. They need a roadmap for success. IT leaders should document the processes established for collaboration, create change controls where necessary, and leverage industry best practices where relevant. The IT service management group may be a valuable partner for this process.

IT leaders should encourage network and security teams to share resources, including tools, data, people, and budget. Leaders should encourage these groups to reveal their value and expertise to each other and should not leave them to solve this challenge on their own. Without the full support of executive leadership, these two groups will drift apart, fighting individual fires. Formalize this collaboration and maintain strong top-down leadership.

ABOUT NETSCOUT

NETSCOUT Systems, Inc. (NASDAQ: NTCT) assures digital business services against disruptions in availability, performance, and security. Our market and technology leadership stems from combining our patented smart data technology with smart analytics. We provide real-time, pervasive visibility and insights customers need to accelerate and secure their digital transformation. Our approach transforms the way organizations plan, deliver, integrate, test, and deploy services and applications. Our nGenius service assurance solutions provide real-time, contextual analysis of service, network, and application performance. Arbor security solutions protect against DDoS attacks that threaten availability and advanced threats that infiltrate networks to steal critical business assets. To learn more about improving service, network, and application performance in physical or virtual data centers, or in the cloud, and how NETSCOUT's performance and security solutions (powered by service intelligence) can help you move forward with confidence, visit www.netscout.com or follow @NETSCOUT and @ArborNetworks on Twitter, Facebook, or LinkedIn.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at www.enterprisemanagement.com or blog.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook, or LinkedIn.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com

3812.022619

IT AND DATA MANAGEMENT
RESEARCH | INDUSTRY ANALYSIS | CONSULTING