Prepared for

NETSCOUT

A Guide to NetOps and SecOps Collaboration

May 2021 EMA White Paper
By Shamus McGillicuddy

EMA™
IT & 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, perhaps now more than ever. Businesses are grappling with brand-new infrastructure demands brought on by the COVID-19 pandemic, which has caused an uptick in security attacks as more companies migrate to the cloud and millions of employees leave campus networks to work from home.

It's in the best interest of networking and security teams to collaborate, if not converge. Thirty-five percent of network operations teams say security system problems, such as bad policies and device failures, have led to complex and difficult to troubleshoot service performance issues. Another 35% reported that incidents originally presented themselves as complex service performance problems that required cross-silo collaboration.[1]

Suffice to say, security is a strategic priority for network teams. Security risk reduction is the second-most important organizational goal of NetSecOps, more so than operational cost efficiency. As enterprises deploy software-defined data centers and public and private cloud architecture, security becomes even more essential to the network team. According to EMA research, the top three goals of NetSecOps collaboration are improved network performance, security risk reduction, and accelerated security incident detection and response.

EMA found that the closer network and security teams work together, the more successful NetOps is. In fact, successful teams are very likely to have converged groups or integrated tools and processes between networking and security. Successful network operations teams are more likely to report significant increases in NetSecOps collaboration.

Network and Security Collaboration is Already Common

Seventy-eight percent of enterprises have at least some formal collaboration between their network and security groups. Forty-seven percent have fully converged these groups with shared tools and processes, although this is more common among small and midsized enterprises in which traditional organizational silos are less established. Another 31% of security groups enable collaboration by integrating the toolsets of network and security teams, and 16% of network and security teams collaborate on an ad hoc basis.

[1] All research cited in this paper was originally published by EMA in the April 2020 report "Network Management Megatrends 2020."

However, this collaboration isn't easy. Network managers have identified several key barriers to success. Network teams have told EMA that the top challenge to this collaboration is that the two teams 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 teams say that they struggle with a cross-team skills gap and a lack of tools that could help support NetSecOps collaboration.

Collaboration 101: From Infrastructure Design to Operational Tools

EMA recommends that IT leaders take a five-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.

Begin at the Design Stage

EMA research found that one of the most critical points 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 enterprises also struggle with data control conflicts because individual teams can be very protective of the data they extract from the network, both on the security side and the network side of the business. In some cases, EMA found that the data teams do share for collaboration is sometimes inconsistent, irrelevant, or out of date. At the same time, many network and security tools are already

leveraging the same data, such as packets and flows. 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 and security teams should find ways to unify their data collection and the tools they use for analysis wherever possible. Ninety percent of respondents reported that they already do or have plans to consolidate critical data, like logs and events, to help overcome data sharing issues.

Select the Right Tools for Collaboration

The vast majority (97%) of network teams are interested in using security capabilities provided by their network management vendors to support NetSecOps collaboration. Furthermore, network managers say network performance monitoring and network automation/orchestration 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 affects performance.

EMA also found network automation tools to be slightly more useful for this collaboration than other tools. Network automation tools allow enterprises to make quick changes to the network in response to a security event. Automation workflows in a network performance management solution can deliver a lot of value to network and security collaboration.

Formalize This Collaboration

Enterprises must institutionalize the collaboration between network and security groups. 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 set an agenda by documenting the processes established for collaboration, creating change controls where necessary, and leveraging 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. While network teams are beginning to make progress in working alongside their peers in the security group, 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) helps assure 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 Smart DDoS Protection by NETSCOUT products help protect against 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 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**. You can also follow EMA on **Twitter** or **LinkedIn**

1995 North 57th Court, Suite 120, Boulder, CO 80301 +1 303.543.9500 **www.enterprisemanagement.com**

4092.051121

BAKOTECH is an international group of companies, a flagship in focused Value Added IT Distribution that represents solutions of leading IT vendors. Positioning itself as a True Value Added IT distributor BAKOTECH provides professional pre-sales, post-sales, marketing and technical support for partners and end-customers.
BAKOTECH is the official distributor of Netscout in Ukraine, Georgia & CIS, Central Asia countries.

www.netscout.bakotech.com | netscout@bakotech.com | +380 44 273 3333