Prepared for

riverbed

The Convergence of Network and Security Operations

April 2021 EMA White Paper
By Shamus McGillicuddy

EMA™
IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Executive Summary

When network operations and security operations teams collaborate, good things happen to the business. EMA research found that many enterprises are pursuing this collaboration, even going as far as fully converging the two groups. Such collaboration can reduce risk, cut costs, boost productivity, and make the IT organization more responsive to the business. This white paper offers guidance on how to pursue this collaboration and identifies some pitfalls to avoid.

Enterprise Network Operations Teams are Partnering with IT Security

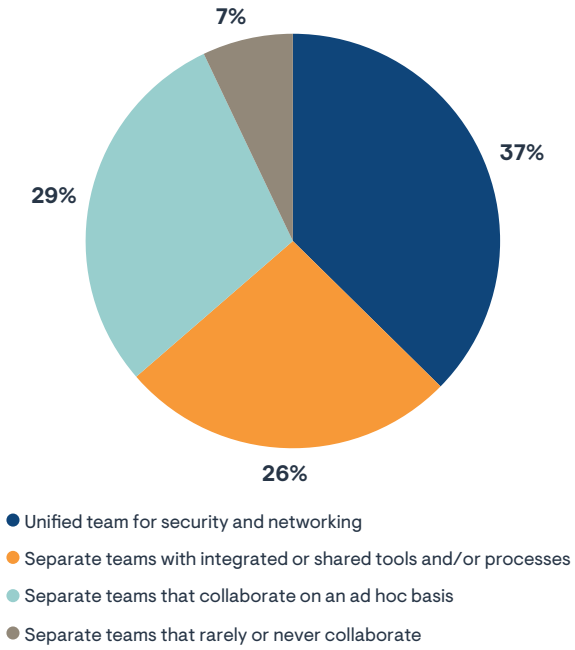
Security is something that no network manager can ignore today. For instance, security is often a factor in complex IT service issues and outages that require a cross-domain troubleshooting response. Security systems (i.e., device failure or bad policy) are the third-most common cause of such complex problems, and security incidents (attacks or breaches) are the fourth-most common root cause, according to Enterprise Management Associates (EMA) research (network infrastructure is first and end-client system or user error is second).[1] If for no other reason, the network team needs security awareness to prove its own innocence, since the network is often the first to be blamed for any service problem.

Security is a major strategic driver of network management. For instance, network security has been locked into the number-one spot for network technology initiatives that influence network management priorities for more than a decade. 2020 was no different. When EMA asked network managers to identify the concepts that are becoming increasingly important to measuring network operations success, security risk reduction was more prominently featured than service quality, improved network visibility, and application performance.

Thus, it's no surprise that network management teams are moving closer to security groups to enhance collaboration and improve overall visibility and responsiveness. In fact, 89% of network managers say they have increased their level of collaboration with their organizations' security teams over the last two years compared to 42% in 2018. This drive for collaboration is resulting in organizational change. Thirty-seven percent of enterprises claim to have fully converged their network management and security management teams, outfitting them with shared tools and processes. Another 26% maintain separate network and security teams, but they have integrated tools or processes to facilitate collaboration.

[1] All data cited in this paper is from the EMA research study, "Network Management Megatrends 2020: Enterprises Embrace NetSecOps, the Internet of Things, and Streaming Telemetry," April 2020.

Figure 1. Relationships between today's network management and information security teams



This collaboration is far-reaching. Enterprises see it as an opportunity to build security into the DNA of their networks. Network managers say their most critical point of collaboration with the security team is in improving network performance, followed by risk reduction and accelerated security incident detection and response.

Tool Strategies for Collaboration with IT Security

The network management team must develop a tool strategy to address its mandate for collaboration with the security group. EMA recommends an integrated approach. The network team should look for ways to extend their existing toolkits rather than add a new standalone tool that they will have to install, maintain, and learn how to use, with limited integration into their existing workflows and network datasets. Network managers will benefit from a security monitoring or management tool that shares datasets with existing network operations tools and offers integrated views of network performance and security monitoring.

EMA recommends this approach in part because network management toolkits are already crowded and fragmented. Large management toolsets add complexity and administrative overhead, which can have a negative impact on overall effectiveness. Every year, enterprises indicate an interest in reducing the number of tools they use, but EMA hadn't see any progress on this front until 2020. While there was a reduction in the number of tools when compared to 2018's results, the 2020 survey found that 64% of network operations teams still use four to ten tools to monitor and troubleshoot their networks. Another 17% use eleven or more.

A large toolset isn't necessarily going to render the network operations team ineffective. Often, those overcrowded toolsets are necessary. Many organizations acquire large sets of tools because they are managing hefty, complex networks that are inherently more difficult to operate. In fact, enterprises with eleven or more network management tools are the most likely (54%) to say they are successful with network operations, compared to 28% of those with 1-3 tools and 29% of those with 4-5 tools. However, EMA continues to recommend consolidation and integration wherever possible.

Network Management Tools That Support Security Collaboration

EMA research identified three kinds of network management tools that are important to enabling collaboration with security groups. The first is network infrastructure monitoring, which can collect device metrics via SNMP, device APIs, etc., and can detect unusual activity on a network device, such as saturation of an interface by an attack. Network infrastructure monitoring is a more popular enabler of collaboration for network teams that have fully unified with security teams, but less popular for teams that collaborate on an ad hoc basis, EMA found.

The second leading tool for security collaboration is network automation/orchestration. Network automation tools allow enterprises to make quick changes to the network in response to a security event. They also help enforce change control policies, which reduce the risk of vulnerabilities being introduced by a bad change to the network.

The third-most important tool for security collaboration is network flow monitoring, such as NetFlow, sFlow, and IPFIX. Flow monitoring can show high-level views of network traffic patterns and activity. Sophisticated analysis of flows can reveal patterns of suspicious behavior, even signature behavior of known threats.

Security Capabilities From Network Management Tools Facilitating NetSecOps Collaboration

EMA's research found that the majority of network teams (97%) are interested in using security capabilities provided by their network management vendors to support collaboration. In fact, 30% say this is critical to their efforts to collaborate with the security group. Such capabilities include security insights, features, or dedicated products.

Security-related capabilities from network management tools are potentially key to NetSecOps collaboration. However, enterprises should make sure that these security capabilities offer some integration with the data and workflows in their network management tools, even if they adopt separate security products from that network management vendor.

EMA asked individuals who want security-related capabilities from their network management solutions where they would like to apply these capabilities. The data center took the top spot at 47%, followed by cloud workloads at 43% and IoT devices at 39%. Secondary priorities include SaaS applications (31%) and remote sites/branch offices and end-user devices/BYOD tying at 28%, respectively.

Benefits and Challenges of Converged Network and Security Management

Enterprises have plenty to gain when their network management and security management teams converge and collaborate, but achieving successful collaboration won't be easy. EMA research identified the four top challenges to this collaboration. Above all else, networking and security groups have different goals, according to 31% of network managers. That's because networking and security teams aren't necessarily natural partners and are often pulled in two different directions. The network team focuses on connectivity by providing employees, partners, and customers access to applications, data, and services. The security team works to lock down data and limit connectivity to applications. Thus, it's important to acknowledge the challenges that IT organizations experience when these teams try to come together.

Leading challenges to successful network and security team collaboration

1. Conflicting goals
2. Cross-team skills gaps
3. Conflicts over sharing and ownership of data
4. Data quality and relevance

Successful collaboration will require strong leadership. If that leadership can't be found within the two groups, they must turn to the executive IT suite for support and direction.

Cross-team skills gaps (29%) are also a significant issue. It's common for individuals to lack the skills and experience required to use the technology, tools, and processes that their peers in the other team rely upon. This challenge is more apparent within specific IT teams. Successful network operations teams are less likely to struggle with these skills gaps (21%). Another equally problematic roadblock is that tools lack sufficient support for collaboration, according to 29% of respondents. To address this challenge, network management tools will need workflows and features that facilitate collaboration and provide security-related insights.

Twenty-seven percent are struggling significantly with conflicts about sharing and ownership of data. 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. EMA suggests that this is an issue that IT leadership needs to address by setting an agenda of cooperation. Another 27% report major problems with the quality of the data they share between networking and security. To remedy the out-of-date or inconsistent data dilemma, network and security teams should find ways to unify their data collection and the tools they use for analysis wherever possible.

The Benefits of Network/Security Collaboration

When network and security management teams share tools, combine data, and collaborate, the enterprise benefits on multiple fronts. EMA research identified the top five drivers for this collaboration. First, 39% of IT organizations believe network and security convergence will result in improved network performance. In fact, enterprises that have unified their network and security teams are more likely to pursue improved network performance (48%).

The second leading driver of this collaboration is risk reduction (34%). With the right processes and tool integrations, IT organizations will gain better visibility into the network and improve overall network integrity. Network managers that are collaborating with security managers will be less likely to commit network design, configuration, and change errors that open up vulnerabilities. Furthermore, the security team will be less likely to impose security controls that degrade network health and performance.

Third, 32% of IT organizations expect accelerated security incident detection and response. Convergence can accelerate their ability to identify and remediate incidents. These streamlined workflows also cut the amount of time that high-value engineers devote to incident response. Instead, they can devote more time to strategic projects. Thus, many IT organizations are targeting operational cost efficiency (27%).

Top Drivers of Network Management and Security Management Collaboration

1. Better network performance
2. Security risk reduction
3. Faster security incident detection and response
4. Operational cost efficiency

EMA Perspective

Collaboration with the security team won't always be easy for network managers. There are technical and cultural barriers to overcome, but the potential benefits are hard to ignore. EMA research has strong evidence that enterprises have not only recognized the importance of this collaboration, but network operations teams are working more closely with information security teams right now than in years past. The partnerships are starting with simple conversations and are gradually expanding into technical reviews of the processes and technologies each group uses to fulfill their responsibilities to the business. Each team has to make concessions and perhaps relinquish control to the other group.

Tools will be a major factor. The network and security teams must identify opportunities to share and integrate their management and monitoring systems, their datasets, and their workflows. Tools that natively support such requirements will be immensely valuable. Security-related capabilities from network management tools are a potential best practice approach to NetSecOps collaboration.

About Riverbed

Riverbed enables organizations to maximize performance and visibility for networks and applications, so they can overcome complexity and fully capitalize on their digital and cloud investments. The Riverbed Network and Application Performance Platform enables organizations to visualize, secure, optimize, remediate and accelerate the performance of any network for any application. The platform addresses performance and visibility holistically with best-in-class WAN optimization, network performance management (NPM), application acceleration (including Office 365, SaaS, client and cloud acceleration), and enterprise-grade SD-WAN. Riverbed's 30,000+ customers include 99% of the Fortune 100. Learn more at riverbed.com.

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**

4080.042021