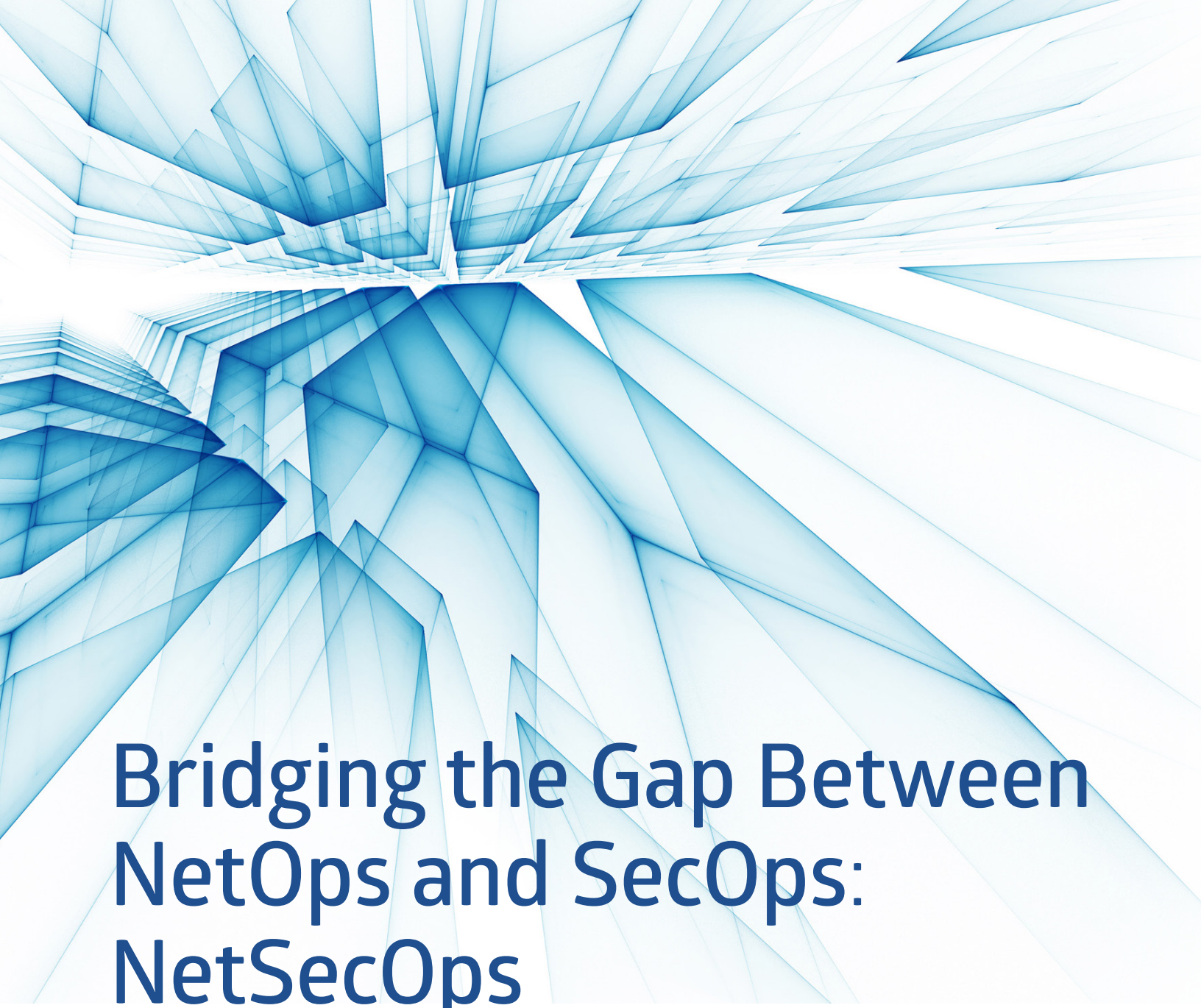


Bridging the Gap Between NetOps and SecOps: NetSecOps

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Prepared for ExtraHop
By Shamus McGillicuddy
July 2019

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

EXECUTIVE SUMMARY

Today's enterprises have recognized that network operations and security operations teams must be partners, not adversaries. IT organizations need a strategy for forging such partnerships. This Enterprise Management Associates white paper draws on multiple industry research studies to offer advice on how these two teams can successfully collaborate to provide a high-performing and highly secure network.

DIFFERENT MISSIONS, ONE GOAL: PROTECT THE BUSINESS

In today's IT organizations, network operations and security operations teams are forming strategic, but perhaps uneasy, alliances. These partnerships are uneasy because the two groups have traditionally been at odds with each other. While the security team is devoted to locking down applications and data, the network team strives to connect people to applications and data. Their missions might diverge, but both groups want to protect the business, whether from security risk or poor performance. Ideally, these two groups should work together to balance their core missions.

These partnerships are also critically strategic. Enterprise Management Associates (EMA) recently found that security incidents are the second most common root cause (24%) of IT service degradation, just slightly less common than network problems like congestion, device failure, or misconfigurations (25%).[1] In other words, security incidents often present themselves as performance problems, and IT teams that respond to security incidents as performance issues will miss opportunities to protect the business from attack. A network operations team might find itself responding to a performance issue that is actually a breach or ongoing attack, when the best thing to do would be to gather information and contact the security team. With the right tools, the network operations team should instead supplement the security group by helping with information gathering, sharing data and analysis, and supporting a remediation processes when appropriate.

In fact, 91% of today's network operations teams have formalized collaboration with their peers in the security group. Many (40%) have fully converged these two teams, particularly midmarket enterprises. Others have integrated their tools (35%) with the security team's tools, and a smaller number (16%) have shared their tools with the security group for collaboration.[2]

Incident detection (30%) and incident response (27%) aren't the only collaboration opportunities. Instead, the most popular target for collaboration is in infrastructure design and deployment (38%).[3] Network teams are looking for opportunities to build security into the network at the start of the design process. They can ask the security team to review segmentation strategies, and they suggest new network technologies that provide enhanced security, such as streaming telemetry for network traffic analysis.

Change management (26%) is also a common driver for this collaboration.[4] Collaboration on change management can prevent changes that introduce vulnerabilities or policy violations, and they can prevent changes to security infrastructure that affect performance.

1 EMA, "Network Performance Management for Today's Digital Enterprise," May 2019.
2 EMA, "Network Management Megatrends 2018: Exploring NetSecOps Convergence, Network Automation, and Cloud Networking," April 2018.
3 Ibid.
4 Ibid.

ESTABLISHING EFFECTIVE NETOPS/SECOPS COLLABORATION

The network operations and security operations teams are not natural allies or partners. Establishing common ground will require leadership and deliberate planning. EMA research identified some of the most critical steps to take when forming partnerships between these groups.

First, network and security teams must establish well-defined processes and best practices for effective cooperation and improved communication. Next, IT leaders must set the agenda, whether they are within the network or security group or sitting in the CIO's office. These leaders must set common goals for both groups to work toward. Finally, these groups must adopt a platform that offers shared data and analytics that are consistent, relevant, and current.

Step 1 – Best practices and processes

A lack of best practices and formal processes is the number-one challenge to effective network and security collaboration, according to EMA research.[5] Research also shows that security teams are more effective at instrumenting the network for packet data collection when they have formal processes for collaboration with the network team.[6]

Many enterprises may find a dearth of proven processes to follow for network and security partnerships. If that's the case, they should ask their network operations and security operations tool vendors for assistance. If a vendor has a customer success program in place, they may be able to help. Other parties within one's own enterprise may offer some assistance, too. For instances, IT service management teams often have responsibility for defining and maintaining IT processes, and they may be able to adapt such processes for these partnerships.

Finally, a key piece of defining best practices and processes is good communication. The two groups must share knowledge, ideas, and information. They should share data, document everything, and adopt collaboration tools.

Step 2 – Set the agenda

The number-two challenge to effective network and security collaboration is poor leadership.[7] Specifically, the two teams have different goals, and no one is getting them on the same page. Network and security directors should make it clear to staff that the adversarial relationships of the past must be consigned to history.

For instance, network teams frequently use NPM tools to monitor for security and to respond to security incidents. In fact, it's actually a top use case for NPM tools today. In the past, a network team might use its tools to prove its innocence during a security event. Today, this practice has become quite rare—only 16% of network operations teams say they are focused on diverting blame during a security event. Instead, 29% of network teams use NPM tools to assist or partner with the security team. Another 26% share their NPM tools directly with the security team, and 19% say they integrate their NPM tools with the security team's tools.[8]

Collaboration requires leadership further up the command structure, too. Network and security directors need support from above. IT executives should give these teams incentives to work together, and they should give them the room to make the partnership work.

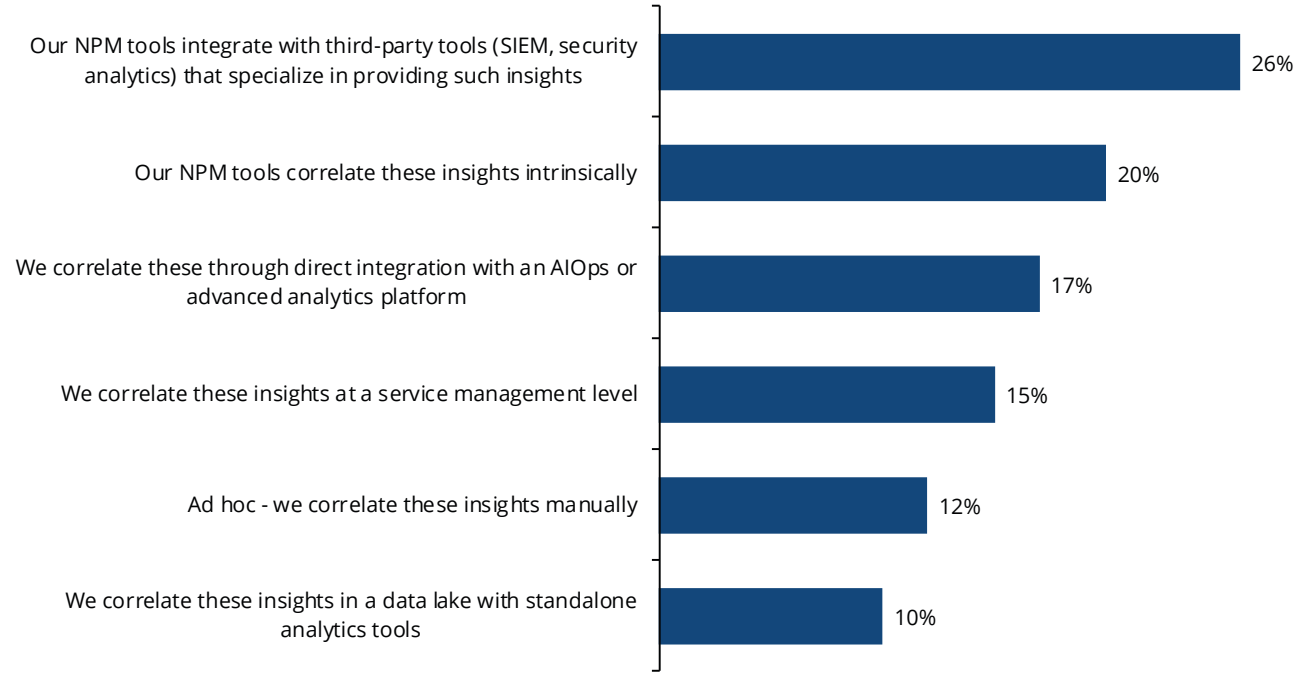
5 EMA, "Network Management Megatrends 2018: Exploring NetSecOps Convergence, Network Automation, and Cloud Networking," April 2018.
6 EMA, "Next-Generation Network Packet Brokers: Defining the Future of Network Visibility Fabrics," August 2018.
7 EMA, "Network Management Megatrends 2018: Exploring NetSecOps Convergence, Network Automation, and Cloud Networking," April 2018.
8 EMA, "Network Performance Management for Today's Digital Enterprise," May 2019.

Step 3 – Adopt a shared data platform

The number-three challenge to effective collaboration is a lack of shared data that is relevant, useful, and timely. Many network and security groups maintain their own datasets for their individual toolsets. They may pull data from the same sources, such as packets from the production network or logs from devices, but the data is captured, stored, and analyzed separately.

Without a common dataset, there is no shared reality between the two teams. EMA believes that NPM tools are a good starting point from the network team's perspective. Research found that NPM tools are the #1 most valuable tool in the network manager's toolset for collaboration with the security team.

When applying NPM tools to security, network teams take three main approaches. The most common method is to integrate an NPM tool with a security tool, like a security incident and event management (SIEM) or network detection and response (NDR) system. The second most common method is the use of an NPM tool that can provide security insights intrinsically. Finally, the third most popular strategy is the integration of an NPM tool with an AIOps or advanced analytics platform.[9]



Sample Size = 250

Figure 1. Primary approach to correlating NPM insights with network security monitoring

9 EMA, "Network Performance Management for Today's Digital Enterprise," May 2019.

EMA believes that NPM tools can either provide a common dataset on which network and security teams can collaborate, or such a tool may draw data from a common dataset, such as a network visibility fabric based on network packet brokers, a data lake, or another platform. In the former case, network operations can give the security team role-based access to the NPM tool for collaboration. In the latter, the security team can connect their own tools to the common dataset, confident that both groups are looking at the same data. Packet data is the best source of truth for such a dataset, but other sources like logs, flows, and device metrics can add additional context.

Adopting shared tools can provide other value beyond collaboration. For instance, if network and security groups consolidate onto shared tools, they not only facilitate collaboration but can also free up budget by covering both team's requirements with the same spend.

EMA research found that network teams that focus on fully-integrated, multifunction NPM platforms are more effective at applying those tools to security use cases. The research also found that NPM tools capable of correlating multiple classes of network data are also more effective at security.[10] By combining budget resources, both teams can afford greater coverage of their network than if they purchased separate network analytics tools. They will also find it easier to instrument the network with a combined toolset.

EMA PERSPECTIVE

EMA research found that network and security groups have a mandate to work together, not just for incident detection and response. They must also work together on network design, deployment, and change management.

This mandate is especially critical because security incidents often appear to IT operations as a performance problem. The longer it takes to connect the dots, the more likely is it that a breach could occur while the network team is focused on a performance rather than security.

EMA suggests enterprises do the following to foster this network and security team collaboration. They should establish well-defined processes and best practices for effective cooperation and communication. They should set the agenda, with team leaders and IT executives making sure the network and security groups can find common goals to work toward. Finally, they must adopt a platform for shared data and analytics that is consistent, relevant, and current.

ExtraHop is a good example of a vendor that offers a common data platform for both security and network operations. Many of ExtraHop's customers have combined network and security team budgets to purchase ExtraHop's Reveal(x) NDR product, which meets the unique needs of both teams and enables them in their respective missions. Enterprises that are working to improve network and security partnerships should evaluate ExtraHop to determine whether it meets their requirements for a data platform.

ABOUT EXTRAHOP

ExtraHop provides enterprise cyber analytics that deliver security and performance from the inside out. Our breakthrough approach analyzes all network interactions in real time and applies advanced machine learning to help you investigate threats, ensure the delivery of critical applications, and protect your investment in the cloud. With this approach, we help the world's leading enterprises including Credit Suisse, Hasbro, Caesars Entertainment, and Liberty Global rise above the noise of alerts, organizational silos, and runaway technology with complete visibility, real-time detection, and guided investigation. ExtraHop Reveal(x) has a fully interactive online demo available at www.extrahop.com/demo.

10 EMA, "Network Performance Management for Today's Digital Enterprise," May 2019.

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

3858.062519