IDC

Observability Case Study: Interview with the Senior Network Manager of a Global Technology Supplier

ASSOCIATED WITH THE WHITE PAPER:

Network Intelligence and Insights: Driving Performance, Protection, and Productivity in Observability

AUTHORS:

Christopher Kissel

Mark Leary

Business Scenario

As a global developer and manufacturer of technology components operating across three major world regions, networking and security are critical focal points for the IT organization. Serving highly distributed engineering and production functions along with demanding customers such as major service providers, government agencies, systems integrators, and other technology providers, a resilient and responsive digital infrastructure is critical to success.

In this environment, network exchanges and access must be fully protected, while network services and systems must provide for consistent performance. As our interviewee stated, *"for most of our threats, it starts with the network."*

How Network and Security Operations (NOC/SOC) Are Managed

With networking and security being such a high priority for this company, there is a strong need to bring together the talent, tools, and processes in place within each of these IT domains. Forward movement is seen with organizational interactions, tool selection and use, and overall IT service integrity. **Read on...**

However, digging deeper into this organization's journey towards a more unified infrastructure management approach, there are strong indications that further strides are needed to deliver the best possible network foundation, security posture, and cloud connections.

Over just the last five years, three major IT reorganizations were intended to more effectively unify IT teams – especially IT ops and security. The first reorganization built out a strong security team but did not align infrastructure operations with security operations. According to the NetOps lead, interactions with the security team were accidental and adversarial. Often these interactions ended with the security staff saying, *"you're doing it wrong. Stop it."* A change in security leadership drove a second reorganization. Interactions between operations and security improved and increased. However, cross-team collaboration was still ad hoc. This latest and third reorganization, while still not aligning IT and security operations, is driving more conjoined efforts around design reviews, technology selection, and teamwork. With that said, work is to be done, especially in developing a truly bi-directional partnership between ITOps and security. Interestingly, there is no SecOps team in place in this organization. The security team focuses on analysis, policies, and audits – and avoids operational responsibilities. This greatly impacts teamwork with the operations groups such as NetOps. To ensure SecOps is covered, it is up to the various ITOps teams to ensure their solutions and practices are in line with the security team's standards and enforce security within their respective operating domains. As our NetOps lead states, *"lots of heavy lifting is needed to bring together network and security."*

For our NetOps lead, this still rather siloed approach drives her to actively seek security sign-offs on all architectural designs, change controls, tool selections, management practices, vulnerability assessments, and security policies. To ensure this sign-off happens in all circumstances, she uses a cross-trained (networking and security) expert as her NetOps liaison into security. This person's primary focus is to ensure security team alignment. This person also serves as the principal network security design and deployment specialist and trains NetOps staff in security considerations and techniques. It should be noted that the security team does not have any operations champions that serve a corresponding liaison role.

Where Observability Fits In

The highly distributed nature and strict security requirements of the network infrastructure drives a clear stance on three fronts. First, who and what is allowed on the network is firmly defined and highly restricted. Second, solutions and policies put in place to protect the network are controlled and coordinated. And third, tools used to monitor and manage the network must provide for detailed visibility into conditions and components – not only of networking systems and services, but also those exchanges, files, and data that use the network.

To date, much of the monitoring and management tools put in place reflect a rather piecemeal approach – incorporating discrete performance monitoring, device management, security controls, and cloud service utilities. Our NetOps lead expressed an urgent need to develop a more holistic set of tools and more collaborative set of practices that allow for both network and security solutions and associated management tools to operate more in concert.

To date, mostly what is in place is a collection of standalone and rather specialized tools and, unfortunately, talent. Fortunately, she sees some real gains being made as her NetOps security liaison and the security team have more of an impact on network changes, tool selection and use, and skill development of the NetOps team. Going forward she firmly believes, *"using some of the same tools in networking and security helps distribute the load on staff, but also brings people together—for new designs, for problem solving, for everyday practices, and for planned enhancements."*

Opportunities to Enhance Operations with a Greater Commitment to Observability

Our NetOps lead sees three areas of developing need for a more holistic monitoring and management approach for IT operations.

First, automation will be critical to further tighten up control over who uses the network and what is connected to the network. For example, in network access, the organization has commenced the implementation of a role-based access scheme, aimed at controlling almost 10,000 workers operating (and often collaborating) across the globe. In what is described as *"heavy access security"* for insiders and outsiders, automation is required for secure access to be provided efficiently and effectively.

Second, the company is moving from a hybrid cloud environment to one that is fully served by public cloud services. Detailed cloud services and infrastructure visibility and control will be vital for success. To date, there has been little movement along this front, owing to traditional management attention (tools, data, and staff) to on-premises computing, networking, and applications. Our NetOps lead expressed *"pointed expectations"* for the move to a cloud-based infrastructure but demands a deep understanding into how cloud service providers (SPs) will operate, secure, and evolve their network to align with her company's needs and how her staff will work with cloud SPs to assure services levels to her clients remain strong. As she states, *"today, our users get good service from IT because we know our infrastructure and our network. We want to provide this same level of support to users when we move more to the cloud."*

Third, and finally, our NetOps lead wants to see further streamlining and synchronizing of both the IT organization and the toolset and dataset that supports engineering and operations of the digital infrastructure—whether on-premises or cloud-based. Into the future, the disjointed tools and practices of the past will be less and less effective. She expresses the need to bring management resources together—both tools and talent. This should involve further consolidation of tools, heightened integration of tools and data, and increased shared use of common tools and data across all IT groups—cloud, networking, security, applications.

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. As a premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets, IDC's Custom Solutions group helps clients plan, market, sell and succeed in the global marketplace. We create actionable market intelligence and influential content marketing programs that yield measurable results.

IDC Research, Inc.
140 Kendrick Street, Building B, Needham, MA 02494, USA
T +1 508 872 8200