IDC

Observability Case Study:
Interview with the CIO of a Leading National Healthcare Provider

ASSOCIATED WITH THE WHITE PAPER:

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

AUTHORS:

Christopher Kissel

Mark Leary

Business Scenario

Even before the pandemic, the healthcare industry was in a period of significant transformation. COVID-19 then heightened and accelerated healthcare digital initiatives far beyond even the most aggressive provider plans. Evolution turned to a revolution overnight as telemedicine, care networks, patient needs, operating and supply costs, and staff challenges exploded. For this national healthcare provider, its digital infrastructure and IT organization were suddenly called upon to excel in both operations and innovation. All the while, the provider was prioritizing systems and services that delivered the best possible patient care.

Fighting on multiple fronts, this CIO needed to transform technologies, practices, and the talent behind both. He needed to modernize his infrastructure and the ways and means his staff went about managing and securing all included systems and services. He believed that a unified approach was a best practice, and that such an approach was built on a "team ethos" driven by common tools, shared data, and cross-functional skills. **Read on...**

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

Owing to his CIO role, all the necessary pieces needed to implement this unified IT management approach were under his control. Unfortunately, the existing culture, practices, and people were not. The CIO needed to transform his people and practices as fast and as fully as the healthcare technology and business were transforming. He looked to put in place a senior management group that showed three key traits – cross-skilled across IT domains, highly motivated to change the status quo, and had the energy for both a fast start and prolonged push forward.

With executive commitment and strong management catalysts in place, this CIO was firmly convinced change required a technology boost. While IDC sees many organizations apply management tools and techniques based on their existing organizational structure and capabilities, this CIO believed that unified tools and practices could drive the needed changes to his IT operating model. The more efficient and effective these tools and practices were, the faster and farther his organization could advance. For him, *"the tools and the teams in the IT space must come together."* His belief was that tools and talent must be readily shared across IT functions, problems, and projects. His word of warning on management included, *"when you have separate teams and toolsets, you not only have a siloing of people and capability, you also have a siloing of product and the IT landscape."*

Where Observability Fits In

Within this CIO's domain, he viewed observability as a core tenet of his unified IT management approach.

While he looked for commonality and collaboration across all IT domains and infrastructure components, there is a particular emphasis on the following:

- **Dashboard focus.** The ability to offer a single source of detailed information and present role-based views, alerts, and insights to staff and teams allow for more efficient and effective management efforts. In the past, IT operations and engineering had been driven by specialized tools with limited information.
- **Security posture.** A very visible breach a few years ago was one of the primary catalysts for a more unified IT management approach. Bringing teams and tools together have served to strengthen the security posture – and all the associated practices and policies now in place to ward off future threats. NetOps and SecOps sharing tools and data – along with cross-skilled staff – has served to bolster the organizations security posture.

- **Cloud empowerment.** As cloud services build within this healthcare provider's infrastructure, the CIO expresses concern over the *"disempowerment and disenfranchisement"* of the digital infrastructure. The more cloud services in play, the less his organization feels they can control its own digital destiny. In his view, increased visibility into and control over cloud services are vital to fully incorporating cloud management in any unified IT management thrust and returning the power of operating and innovating the digital infrastructure to the subscriber.
- **Integrated solutions.** This CIO is pushing to *"use fewer tools to do more things."* His expectation is that more intelligence and insights come from fewer sources. And those fewer sources are able to provide support for a broader set of operators, engineers, and analysts; detailed data collection and sharing; and ready tailoring for best use by the organization.
- **Supplier partnership.** While much of this CIO's attention is focused on managing his own IT talent, intelligence, toolset, and practices, he firmly believes that his suppliers must be as committed to his goals and organization as he is to their solutions – both private systems and public services. His belief in the need to *"understand a supplier's capability to respond in moments of need"* could not be overstated – especially with cloud services and security solutions. His advice is to *"really nail down"* KPIs for both the solution and the solution's supplier – whether system vendor or services provider.

Opportunities to Enhance Operations with a Greater Commitment to Observability

For his organization, this CIO cited three main focal points for his planned observability thrust. First, building out cloud intelligence, insights, and in-house expertise. Cloud services use is expanding within his digital infrastructure. That means more costs, criticality, and complexity. He faces more decisions to cloud or not to cloud. And these decisions are easier if he is not going to lose visibility or control. Second, performance monitoring and management – end-to-end across his entire infrastructure – is of increasing concern. Healthcare solutions are producing more highly sensitive data and requiring more real-time exchanges among high-value workers and partners. Service levels must be consistent, even in the face of rapid innovation. Third, he warned that organizations must be ever-vigilant in cybersecurity. As he stated, *"you must never be comfortable with what you've done"* no matter how many systems, policies, practices, and staff are in place.

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