EXTRAHOP

CUSTOMER STORY

Seattle Children's and ExtraHop RevealX—Protecting More Than Data

- Complete visibility to detect lateral movement
- Faster threat and anomalous data detection
- Security that enables scientific innovation and specialized care

Executive Summary

At the vanguard of pediatric medical research, Seattle Children's Hospital's work in cancer therapies, genetics, neuroscience, immunology, and infectious diseases is recognized internationally. Its physicians include leading experts across nearly 60 subspecialties, from cancer to autism. As a premier health and research organization, Seattle Children's must maintain a strong security posture without stifling scientific innovation—which can be a tough balancing act as threat actors increasingly target health organizations.

The Beginning

Security to Protect Quality of Care

Seattle Children's sophisticated IT infrastructure includes cloud and on-premises workloads, a large electronic health record deployment, as well as numerous workstations, mobile devices, and connected medical IoT devices, including drug infusion pumps, monitoring, and imaging tools—all of which must remain secure to protect clinical operations, patient data, sensitive intellectual property, and ultimately the quality of care Seattle Children's provides.

The Transformation

A Fast-Changing Threat Landscape

Effectively securing a large-scale, complex, and highly regulated IT environment like Seattle Children's is compounded by an increasingly sophisticated cyberattack landscape.

"We see this every day," says Gooden. "Attackers aren't looking for a quick hit—they want to get in to learn where your data lives and how to get to it without drawing attention to themselves. So they go low and slow as they incrementally figure out how to get to our data. Ten years ago, the firewall was the thing that blocked everything. Today a firewall is nothing."

Preventing Lateral Movement

While Gooden and his team rely on zero-trust principles and architecture to protect Seattle Children's clinical and research operations, they know that alone is not enough. With the growing number of zero-day exploits like Log4Shell and supply chain attacks, they also need behavior-based detection to identify and investigate potentially malicious activity within their environment. That's where ExtraHop RevealX comes in.

"ExtraHop learns from the environment, correlating data points across our entire organization. It detects lateral movement and shows us where threat activity is happening anywhere in our infrastructure, regardless of the device, service, or user profile from which it originated," says Gooden. "ExtraHop gives us deep packet inspection, which is critical—especially when it comes to east-west packet movement and anomalous data detection."

Simpler Threat Hunting

Gooden and his team are also moving beyond just detection and response. "We're starting to implement things like active threat hunting," he says. "We're working more closely with our software suppliers to make sure that we understand the behavior associated with their systems and flagging anomalies so that we can collectively be proactive in closing the gaps that let attackers do what they do."

ExtraHop simplifies and streamlines threat hunting for Gooden's team with guided workflows and automated hunting techniques. And because the packet-based data source is nearly impossible for attackers to disable or modify, RevealX accelerates research and validation so Seattle Children's can detect threats proactively to avoid a breach.

Security at the Pace of Innovation

While Gooden and his team spend their days securing Seattle Children's IT estate, they view their role through the lens of the organization's mission.

"We operate in an environment where thousands of children and their families rely on us to provide critical care and to continue to drive towards treatments and cures that improve outcomes and lives. Security must protect that mission without slowing it down," says Gooden.

For Gooden, that means adopting practices and technologies that improve care and accelerate innovation and scientific discovery. This includes cloud-native technologies that can support both on-premises, remote, and cloud environments and provide visibility into highly varied and specialized devices and operating systems.

"When done right, security is the tip of the spear that drives innovation," says Gooden. "When our data is secure, our operations are secure, and our patients are safe, we can focus on the work we're all here to do: saving lives."

> "ExtraHop RevealX is a critical tool to help us protect data in transit and at rest. We have to see and understand how data is moving from point to point so we can quickly identify unusual or problematic patterns.
>
> ***Gary Gooden***
> CISO, Seattle Children's Hospital

ABOUT EXTRAHOP

EXTRAHOP®

ExtraHop is the cybersecurity partner enterprises trust to reveal cyber risk and build business resilience. The ExtraHop RevealX platform for network detection and response and network performance management uniquely delivers the unparalleled visibility and decryption capabilities that organizations need to investigate smarter, stop threats faster, and move at the speed of risk.