ExtraHop

CUSTOMER STORY
CORA

Central Oregon Radiology Safeguards Sensitive Medical Images and Data with ExtraHop Reveal(x)

Improved protection against breaches in an increasingly targeted industry

Reduced security costs by eliminating overhead needed to support separate, niche solution providers

Recognized immediate value with shortened training time and improved IT collaboration

Executive Summary

Central Oregon Radiology Associates (CORA) is the region's largest, oldest, and most respected imaging group. For more than 70 years, CORA has provided advanced imaging services and minimally invasive procedures through multiple state-of-the-art outpatient imaging centers and hospitals in Central and Eastern Oregon communities.

THE BEGINNING

CORA supports more than 8,000 physicians, hospitals, and clinics for their medical imaging needs. That means creating, transmitting, and storing hundreds of thousands of sensitive CT scans, MRIs, ultrasounds, PET scans, and X-rays. Many of the medical imaging machines and IoT devices are located at hospitals and clinics but are managed by CORA, which creates a challenging array of small, widely distributed sites that need to be secured.

Security issues and breaches targeting healthcare organizations have been on the rise over the past few years, and in 2019, several attacks specifically targeted digital imaging and communications in medicine. CORA wanted to get ahead of the growing risk by upgrading their security posture to better defend against potential breaches.

> "We had instant confidence in the tool. The ability to essentially plug and play meant we started to see returns on our investment almost right away.

Richard Stepanek CIO,
Central Oregon Radiology Associates

CUSTOMER STORY

CORA

THE TRANSFORMATION

The small CORA team manages all aspects of IT so they turned to ExtraHop to provide critical visibility for both security and performance. Reveal(x) immediately proved effective in its proof-of-concept phase.

"Third-party assessments just come back with raw numbers for pen testing or vulnerability assessments," says Richard Stepanek, CIO. "Unless you have a pretty big team of dedicated security experts, it can be hard to know how to act on the information, but Reveal(x) directs us precisely where to find any potential issues so we can locate and mitigate it fast."

The POC clearly demonstrated how the CORA team could track and protect vast volumes of data—both stored and in flight—across a wide variety of outside organizations.

With such a broad set of users and connected devices, CORA also relies on Reveal(x) to ensure that sensitive medical data is shared and stored while following established protocol.

"The use of 'unauthorized' sharing services is big now because colleagues often just choose whatever they're familiar using, usually not with malicious intent," says Stepanek. Reveal(x) lets his team get ahead of those kinds of issues and be proactive about resolving them, so they aren't surprised if any breach occurs.

"It's helped close that loop with medical records folks. When we see anything outside of our normal channels, we can set authorizations and documentation up front, so no one gets crossways with HIPAA rules."

THE OUTCOME

Improved Protection Against Breaches

Healthcare as an industry is subject to much stronger regulatory requirements and protections related to sensitive medical data. Reveal(x) helped CORA reinforce its distributed security environment, potentially preventing security breaches that could amount to millions of dollars in fines and penalties, recovery costs, damage to the brand, and customer goodwill.

Reduced Security Costs

Using Reveal(x) means CORA can eliminate overhead previously devoted to other, niche solution providers. For instance, by reducing their IT infrastructure monitoring spend by nearly 75% and avoiding the need for a fully outsourced SIEM monitoring agreement, CORA has realized a 30% cost avoidance while still ensuring its spend on IDR capabilities.

Streamlined Security Management

Because Reveal(x) is easy to use and intuitive, the CORA team was trained in a short amount of time—and because the whole team can use the same tool, they can collaborate more efficiently. "The ability for my applications, network, and security people to all go into the same tool to see the different facets of any issue makes our job much easier," says Stepanek.

FIND MORE EXTRAHOP CUSTOMER STORIES AT **EXTRAHOP.COM/CUSTOMERS/STORIES**

ABOUT EXTRAHOP NETWORKS

ExtraHop provides cloud-native network detection and response for the hybrid enterprise. Whether you're investigating threats, ensuring the availability of critical applications, or securing your cloud investment, ExtraHop's breakthrough approach helps you rise above the noise so you can protect and accelerate your business. Learn more at www.extrahop.com.

ExtraHop

520 Pike Street, Suite 1600
Seattle, WA 98101