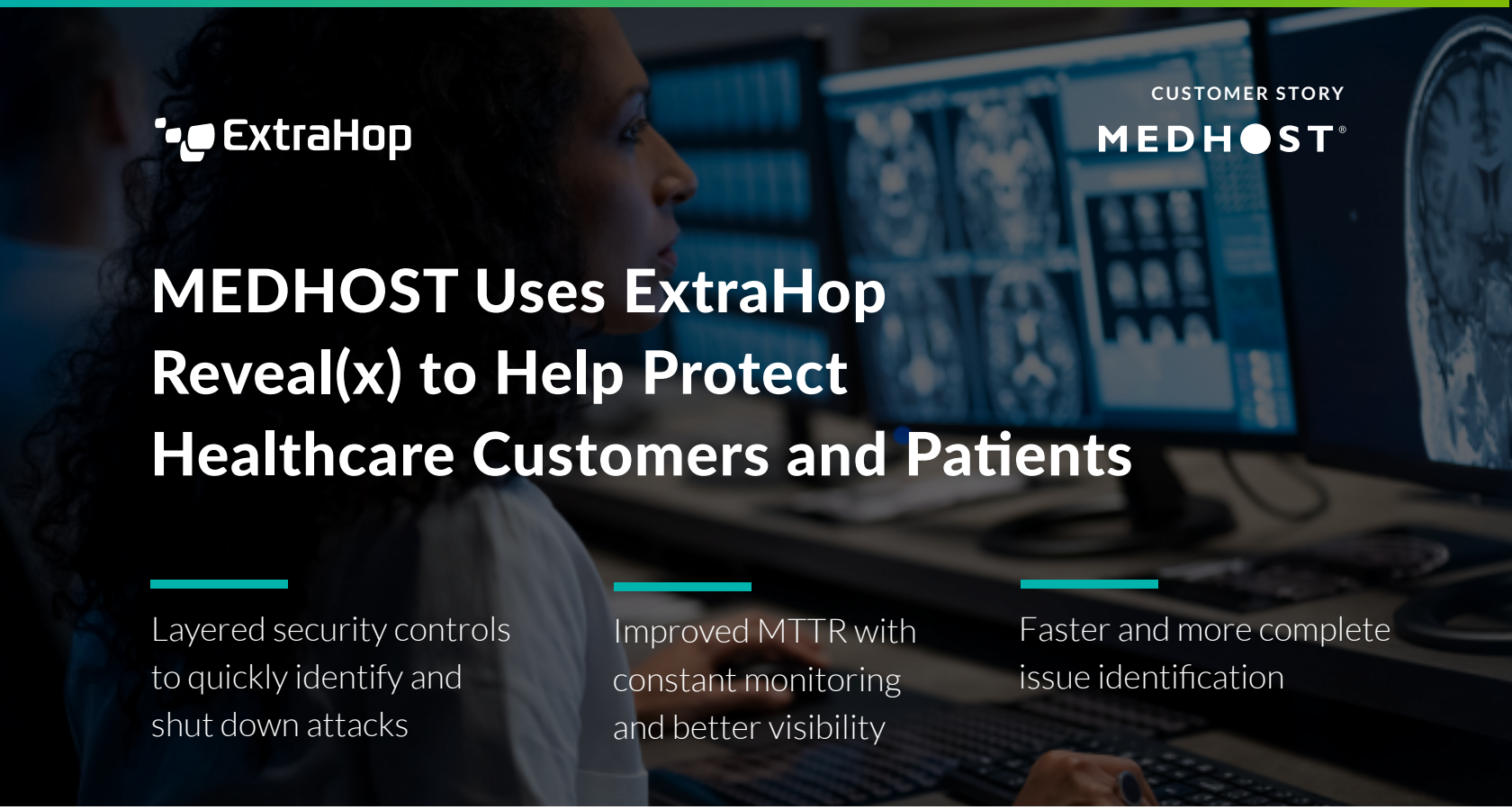

ExtraHop

CUSTOMER STORY

MEDHOST

MEDHOST Uses ExtraHop Reveal(x) to Help Protect Healthcare Customers and Patients

Layered security controls to quickly identify and shut down attacks

Improved MTTR with constant monitoring and better visibility

Faster and more complete issue identification

EXECUTIVE SUMMARY

MEDHOST delivers market-leading healthcare engagement solutions nationwide to healthcare facilities of all types and sizes. The company's integrated product portfolio includes cloud-based clinical, financial, and operational solutions. As a conduit of critical medical and personal data, MEDHOST is particularly sensitive about maintaining data and network security—especially as healthcare data becomes increasingly lucrative and attractive targets for malicious actors.

THE BEGINNING

FAST-GROWING COMPANY UPDATES CYBERSECURITY

MEDHOST manages its own security, but also hosts hospital systems in its cloud. While MEDHOST does not own its customers' networks and security controls, it can be impacted by customers' vulnerabilities. In early 2022, the threat landscape shifted for MEDHOST as Russian attacks on Ukraine put critical industries like healthcare in the crosshairs.

"We've been on high alert over the past few weeks," says Todd Williams, Director of Information Security at MEDHOST. "From the contractors we use to our offshore vendors to our supply chain—bad actors would love to get their hands on patient health information and healthcare source code."

Since the news broke, MEDHOST has been peeling back the covers to ensure effective execution of the fundamentals––for itself and its customers. From geographically distributed systems to connected medical devices, MEDHOST has worked tirelessly to eliminate vulnerabilities throughout their connected ecosystem.

MEDHOST's top security priorities are to prevent ransomware, data exfiltration and manipulation, and software supply chain attacks on its CI/CD development pipeline.

> "Healthcare is a prime target for bad actors. With ExtraHop Reveal(x), we have forensic knowledge at our fingertips that helps us stop attacks cold—before they can impact our systems or our customers' systems.
>
> **TODD WILLIAMS**
> **DIRECTOR OF INFORMATION SECURITY, MEDHOST**

CUSTOMER STORY

MEDHOST®

THE TRANSFORMATION

BETTER VISIBILITY CREATES STRONGER SECURITY FOR SENSITIVE DATA

MEDHOST has used ExtraHop for several years, first to improve network and application performance, and more recently to provide real-time threat detection across its hybrid environment.

"Visibility used to be a real issue," says Williams. "ExtraHop really opened our eyes and allowed us to put our arms around all the data—especially with the addition of Reveal(x), which gives us behavior monitoring. It's always watching. Combined with our log aggregation, Reveal(x) gives us a complete picture of activity that's happening on the network." With Reveal(x), MEDHOST can see adversaries testing the fences to see where any weak points might be.

"ExtraHop can decrypt and inspect things like Active Directory and TLS 1.3 protocols in-line across my entire network, including east-west traffic. I don't have to go through 15 change management cycles and three months' worth of work with development teams and server teams just to go see our own traffic. It's game-changing."

THE OUTCOME

MORE EFFICIENT SECURITY AND NETWORK COORDINATION

Baked-in security

Reveal(x) helps MEDHOST create a substantially more secure product, which is critical when hosting hospital data. "During any incident response, our clients need to know that we've got it handled, and that their data is protected," says Williams. ExtraHop allows MEDHOST to build security frameworks and layered security controls right down to the OSI layer.

In one incident, Reveal(x) alerted MEDHOST to an attack through its on-prem Active Directory federated services. "It was password spraying and locking out users," says Williams. "With Reveal(x), we could look into the payload and see it was coming from North Korea before we shut it down."

Detection of threats other tools miss

MEDHOST quickly discovered that Reveal(x) is a more powerful tool for network security than its closest competitors. In its initial penetration test, Reveal(x) returned alerts that other tools simply missed. "Right out of the box, we plugged Reveal(x) into the network and turned it on at 8:00, and it was scanning our network by 8:01," says Williams.

"As the day went on, we continued to get alerts—but none of our other security tools indicated that we had an issue. After a simulation of the domain takeover at 8:00 that night, we finally got an alert from another tool indicating that an incident had taken place—far too late to act on the information."

The team also quickly learned how to use Reveal(x) to get more information behind each alert. "Reveal(x) surfaces a tremendous amount of key information in the alerts—including data that lets us blunt attacks much more quickly," says Williams. That kind of information means the MEDHOST team can perform root cause investigations to identify activity that occurred during specific incidents.

ABOUT EXTRAHOP NETWORKS

ExtraHop is on a mission to stop advanced threats with security that can't be undermined, outsmarted, or compromised. Our dynamic cyber defense platform uses cloud-scale AI to help enterprises detect and respond to advanced threats—before they compromise your business. When you don't have to choose between protecting your business and moving it forward, that's security uncompromised.

ExtraHop

520 Pike Street, Suite 1600
Seattle, WA 98101