

Leading Manufacturer Brings Network Security to the Shop Floor with ExtraHop Reveal(x)

Improved protection against breaches in a highly distributed manufacturing environment

Faster response and issue mitigation based on improved visibility

Better, data-driven security decisions ensure an improved security posture in a fast-changing environment

Executive Summary

This leading manufacturing company currently employs more than 2,000 people at facilities throughout the United States. Their expansion and fast growth continue with the steady addition of new production lines and machinery.

THE BEGINNING

Sophisticated OT Networks Require Modern Security

Manufacturing is quickly becoming one of the most hacked industries in the world. Newly modernized shop floors and sophisticated operational technology (OT) networks make manufacturing a more attractive target for IP theft, phishing attacks, and ransomware.

This manufacturer was determined to get ahead of the curve by implementing robust security processes before becoming a target. The company relies on an IT team of about 50 with diverse skills and responsibilities to manage both mainframe and .NET apps. Automation requires communications across systems. And the team has to stay up to date on a host of fast-evolving security and compliance requirements.



We use ExtraHop every day. When we see a potential problem, it's the first place we go to check it out. With Reveal(x), we're constantly aware of patterns so we can quickly identify actual issues that need mitigation.

CIO & VP-IT, Leading Manufacturer

THE TRANSFORMATION

Constant Connectivity and Zero Downtime

The company recently overhauled their entire environment, moving from physical servers to hyper-converged systems—all while continuing to operate as usual. Equipment on the shop floor requires constant connectivity, so they needed a security solution that guaranteed zero downtime.

And because the team manages all aspects of IT across a highly distributed estate, they also needed visibility into all their critical systems. Reveal(x) immediately proved effective in its proof-of-concept phase, according to the company's CIO & VP of IT.

"At the first demo, we could tell that we'd be able to operationalize Reveal(x) almost immediately," he says. "We don't have a big enough team to focus solely on security. ExtraHop fulfilled all of our requirements for security and visibility."

Ultimately, the company built out a SNOC (security and network operations center) at headquarters. "We created a command center and put ExtraHop dashboards right in the center of it," says the CIO.

ExtraHop worked closely with the security team on exactly what dashboards would be the most important for them. "We put a dashboard that shows the MITRE framework right in the middle," says the CIO. "That means we're constantly aware of patterns so we can quickly identify actual issues that need mitigation."

THE OUTCOME

Faster Mitigation and Data-driven Decisions—at Scale

FIND MORE EXTRAHOP
CUSTOMER STORIES AT
[EXTRAHOP.COM/
CUSTOMERS/STORIES](https://EXTRAHOP.COM/CUSTOMERS/STORIES)

Security that grows with the business

Beyond being targets of cybercrime themselves, manufacturing companies must always be alert to the fact that their systems can be used as a backdoor into other systems. As this company continues to grow, they'll add new facilities and expand their OT network—all of which will have to be protected to be sure they're never targeted or used as a point of entry for an attack on another company.

Visibility leads to faster response

For this company, visibility into network behavior is the first, most crucial piece in the security puzzle. Using Reveal(x), the team can quickly identify potential issues and investigate them—ensuring they can reinforce security throughout their distributed environment.

Data-driven security decisions

The company relies on micro-segmentation and host-based firewalls to protect their network. Using ExtraHop, the team can watch the traffic and behavior to uncover patterns or gaps that may not be ordinarily evident. They use that information to further refine their segmentation rules.

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.

© 2021 ExtraHop Networks, Inc. All rights reserved. ExtraHop is a registered trademark of ExtraHop Networks, Inc. in the United States and/or other countries. All other products are the trademarks of their respective owners.



520 Pike Street, Suite 1600
Seattle, WA 98101