ExtraHop

CUSTOMER STORY

U.S. XPRESS

U.S. Xpress Rebuilds Security with Reveal(x) to Support Rapid Growth

Integrations improve security team efficiency and effectiveness

Visibility eliminates shadow IT risk

Faster and more complete performance issue identification and inventory tracking

EXECUTIVE SUMMARY

U.S. Xpress Enterprises, Inc. has offered transportation services and tools since 1985 and has evolved into a vital link in the supply chain. They provide a broad portfolio of capacity solutions, including dedicated fleet servicing for some of the nation's largest shippers. The company's brokerage offering, Xpress Technologies, maximizes capacity for shippers and carriers so they can better manage and grow their business. Powered by more than 10,000 professionals, these businesses are driving innovation across the industry and helping to shape the future of logistics.

THE BEGINNING

FAST-GROWING COMPANY UPDATES CYBERSECURITY

A fast-growing company, U.S. Xpress went public in 2018. The company had used Symantec Endpoint Protection, but steady changes to the business meant the company needed to upgrade its security posture.

The company first replaced their simple antivirus solution with a more functional EDR from CrowdStrike before adding AlienVault's Open Source SIEM. The final piece was a strong NDR solution, so they investigated offerings from Darktrace, Gigamon, and ExtraHop.

"We picked ExtraHop Reveal(x) over the others because of its speed," says Cybersecurity Manager Kevin Wright. "The advanced machine learning and integrations are also key to achieving our business goals—and ExtraHop's customer service is second to none."

> "Reveal(x) is a critical component protecting our device data privacy, cybersecurity, and compliance. It allows us to quickly pinpoint those applications that don't have good security standards, so it's key to keeping us safe.

KEVIN WRIGHT
CYBERSECURITY MANAGER,
U.S. XPRESS ENTERPRISES

THE TRANSFORMATION

REVEAL(X) SIMPLIFIES SECURITY MANAGEMENT

Wright's team has only three people who manage the company's cybersecurity, and they appreciated the opportunity to build out a program using the best tools they could find to maximize their effectiveness.

"Autodiscovery, peer group analysis, and the ease of creating investigations to view multiple detections make Reveal(x) simple to manage and use for our small team," he says. "And we especially like its real-time DVR capability—which lets us rewind time to look into specific issues instead of having to dig into a bunch of alerts with limited data to figure out what happened."

The security team has extended the use of Reveal(x) to the company's network engineers and developers who build in-house apps. These teams use the platform to assess performance analyses for servers and apps. The network team is also able to use it to troubleshoot networking issues.

"After a couple weeks to be sure that Reveal(x) had identified legitimate traffic, we added integration to CrowdStrike and customized dashboards. ExtraHop customer service was key in making our install so efficient and clean," says Wright.

THE OUTCOME

CREATING AN EFFECTIVE SECURITY ECOSYSTEM

Integrations fuel new efficiencies

"ExtraHop integrations were paramount in the success of this project," says Wright, "especially for a team like ours."

Reveal(x) works in sync with U.S. Xpress' SIEM, which saves the security team time while also making them more effective. Wright credits an ExtraHop engineer for helping the team set up a log collector that forwards logs, alerts, and investigations directly into the SIEM.

"We work with our SIEM on a daily basis, so this was a huge efficiency gain for us," says Wright.

Reveal(x) ensures app quality and inventory tracking

U.S. Xpress has an internal team of developers who develop and build in-house applications that are hosted both on-premises and externally. The development team uses ExtraHop Reveal(x) to ensure quality of service for all applications and web servers. "They've used it to troubleshoot some notoriously badly written applications, too," says Wright.

Visibility reduces shadow IT risk

U.S. Xpress needed Reveal(x) to integrate smoothly with their EDR and SIEM so they could get full visibility of everything in their environment. For instance, Reveal(x) integration lets the team easily run alerts, investigations, and responses through SOAR workflows. "You can trigger off of 'if this appliance does not have CrowdStrike as an agent then do XYZ,'" Wright explains.

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