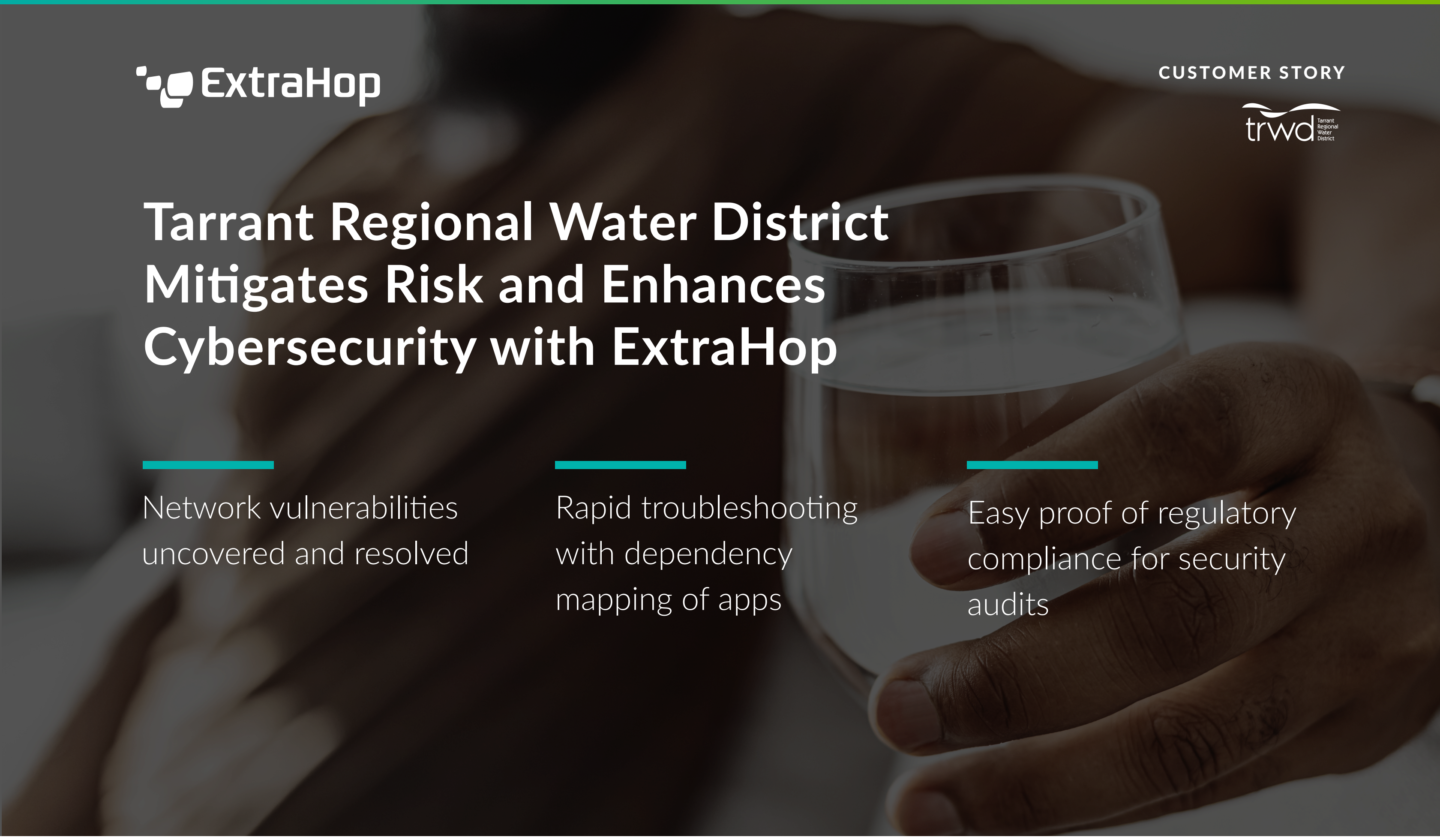

CUSTOMER STORY

Tarrant Regional Water District Mitigates Risk and Enhances Cybersecurity with ExtraHop

Network vulnerabilities uncovered and resolved

Rapid troubleshooting with dependency mapping of apps

Easy proof of regulatory compliance for security audits

Executive Summary

Serving eleven counties in North Texas, Tarrant Regional Water District (TRWD) provides water to over 2.1 million people. The district is responsible for flood-control measures across the region and maintains an extensive network of levees and trails.

THE BEGINNING

When Adam Boldin joined TRWD, they lacked the resources for robust network visibility and had no dedicated in-house security team. His arrival also coincided with an executive mandate to boost the security of the district's IT infrastructure. He said, "There really wasn't much information beyond being able to see the physical network locations. We had a lot of work to do."

To establish an accurate baseline across the organization's complex infrastructure—including TRWD's homegrown applications for monitoring water services—Boldin focused on identifying a network detection and response (NDR) solution that could deliver what he needed.

> "
>
> Reveal(x) competitors just don't have feature parity, and ExtraHop gets things done quicker, too.
>
> ADAM BOLDIN,
> NETWORK ARCHITECT,
> TARRANT REGIONAL WATER DISTRICT

THE TRANSFORMATION

Boldin had already extensively compared NDR vendors in a previous role. He said, "ExtraHop was doing things that nobody else could do, and it was perfect for TRWD."

Before fully adopting Reveal(x), TRWD worked with ExtraHop Professional Services to start establishing a network traffic baseline. ExtraHop also helped TRWD consolidate key metrics from multiple data streams into a single dashboard.

When it came time to fully adopt Reveal(x), the migration proved to be easy, with minimal workflow disruptions. Boldin said, "A remote support engineer took over. When I next logged in, all of our data and dashboards had been perfectly migrated."

The district's critical applications and data centers are configured to have continuous packet monitoring, with retention policies based on business and operational priorities. On average, TRWD feeds 10 gigabits of data per second into Reveal(x). Reveal(x) retains this information for up to 60 days to facilitate full PCAP analysis whenever needed. ExtraHop's dependency mapping capabilities enabled the servers running custom water monitoring applications to be enrolled into a dedicated device group.

THE OUTCOMES

In addition to being a designated component of the U.S.'s critical infrastructure, TRWD also falls under Environmental Protection Agency regulations. Boldin said, "We've been able to implement all the necessary controls, and I leverage Reveal(x) to prove compliance with cybersecurity mandates. It makes things straightforward and efficient for me."

ExtraHop also simplifies troubleshooting, Boldin said, "The dependency mappings help us understand when developers have modified the way an application interacts with the network. Being powerful and easy to use, Reveal(x) is my go-to troubleshooting tool, and I can share with our developer's dashboards showing the impact of code changes."

The ability of Reveal(x) to expose and contextualize network vulnerabilities brings unique value to TWRD. "Reveal(x) competitors just don't have feature parity, and ExtraHop gets things done quicker too," said Boldin.

While TRWD was operating with a lean in-house security team, Boldin, with the help of ExtraHop support, was better equipped to tackle major security concerns. This was especially evident after the SUNBURST story broke. "ExtraHop sent me a step-by-step guide—almost an 'Exfiltration for Dummies' on how its detectors work and how to use Reveal(x) to look back through my DNS archives to see if I'd already been affected. Since ExtraHop retains all of those records, I was able to do the search very easily."

He concluded, "Reveal(x) really saves our hide when it comes to identifying potential incidents or a vulnerability—it just helps me sleep better!"

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