

# ULTA Beauty Securely Scales High-Growth e-Commerce Operation with ExtraHop

Unified visibility across work streams as well as security and network teams

Reduced false positive alerts for more efficient security operations

Accelerated migration of production workloads to Google Cloud

## Executive Summary

Ulta Beauty is the largest beauty retailer in the U.S. and the premier destination for cosmetics, fragrances, and skin and hair products. To deliver exceptional and secure guest experiences at scale, the company turned to ExtraHop for better visibility, detection, and investigation across their hybrid environment.



## The Beginning

With more than 1,200 stores, Ulta prides itself on delivering exceptional guest experiences in-store, online, and with its loyalty program that boasts 30 million members and growing.

To support this fast growth without compromising guest experiences, Ulta started migrating its e-commerce platform to Google Cloud. While this offered greater scale, it also increased complexity and introduced opacity.

"We are always working to wow our guests, and from our team's perspective, it's all about protecting that guest," said Brown. "As our network grew, we found we lacked the visibility we needed to detect and respond to breaches and attacks."

## The Transformation

For Ulta, visibility meant more than just tools that provided insight into one part of the retail environment. The team needed a way to detect, investigate, and respond to threats and performance degradations across the entire network, from on-premises data centers to store locations, and increasingly into Google Cloud workloads. For that, Ulta Beauty turned to ExtraHop RevealX.

"We partnered with ExtraHop to help us build a strong, first-line defense for our monitoring capabilities — at any user level," says Jeff Ybarra, Senior IT Manager of Network & Security for Ulta.

## The Outcomes

### Improving Cross-Functional Alignment and Efficiency

To scale resources and improve security posture, Ulta merged its security and network teams. “Networking and security are so interrelated,” said Brown. “It made sense for us to bring the two teams together into what we now call the ‘secure network operations center’ or the ‘SNOC.’”

With RevealX, the SNOC team allows both network engineers and security analysts to rely on the same source of insight and visibility across the environment.

But it’s not just alignment across teams. ExtraHop also provides high-fidelity, contextual alerts to keep teams focused on what matters. “The real value in ExtraHop RevealX is the time we see returned to our engineers,” said Brown. “That means they can focus on the things that matter, like projects, strategic initiatives, and — most importantly — innovation.”

### Unparalleled Cloud Visibility

For the team at Ulta Beauty, the visibility, detection, and response capabilities in RevealX provide unparalleled visibility into the security and performance of cloud workloads. Through native integration with Google Cloud Packet Mirroring and ExtraHop’s cloud-scale machine learning, RevealX gives the Ulta team the ability to rapidly identify and secure new workloads, spot misconfigurations, and detect threat activity as well as quickly investigate and resolve incidents.

“Before ExtraHop, we had limited visibility into what was going on in the cloud, but with RevealX, we can quickly identify vulnerabilities and exploits and understand how our applications are performing in the cloud,” said John Kreis, Senior IT Engineer.

“The technology is really helping us accelerate adoption of the cloud by ensuring our workloads are secure,” added Kreis.

“

The real value in ExtraHop RevealX is we see time returned back to our engineers so they can focus on the things that matter, like projects, strategic initiatives, and—most importantly—innovation.

**Diane Brown**

Chief Information Security Officer,  
Ulta Beauty

## ABOUT EXTRAHOP

ExtraHop is the cybersecurity partner enterprises trust to reveal cyber risk and build business resilience. The ExtraHop RevealX platform for network detection and response and network performance management uniquely delivers the unparalleled visibility and decryption capabilities that organizations need to investigate smarter, stop threats faster, and move at the speed of risk.

**EXTRAHOP®**