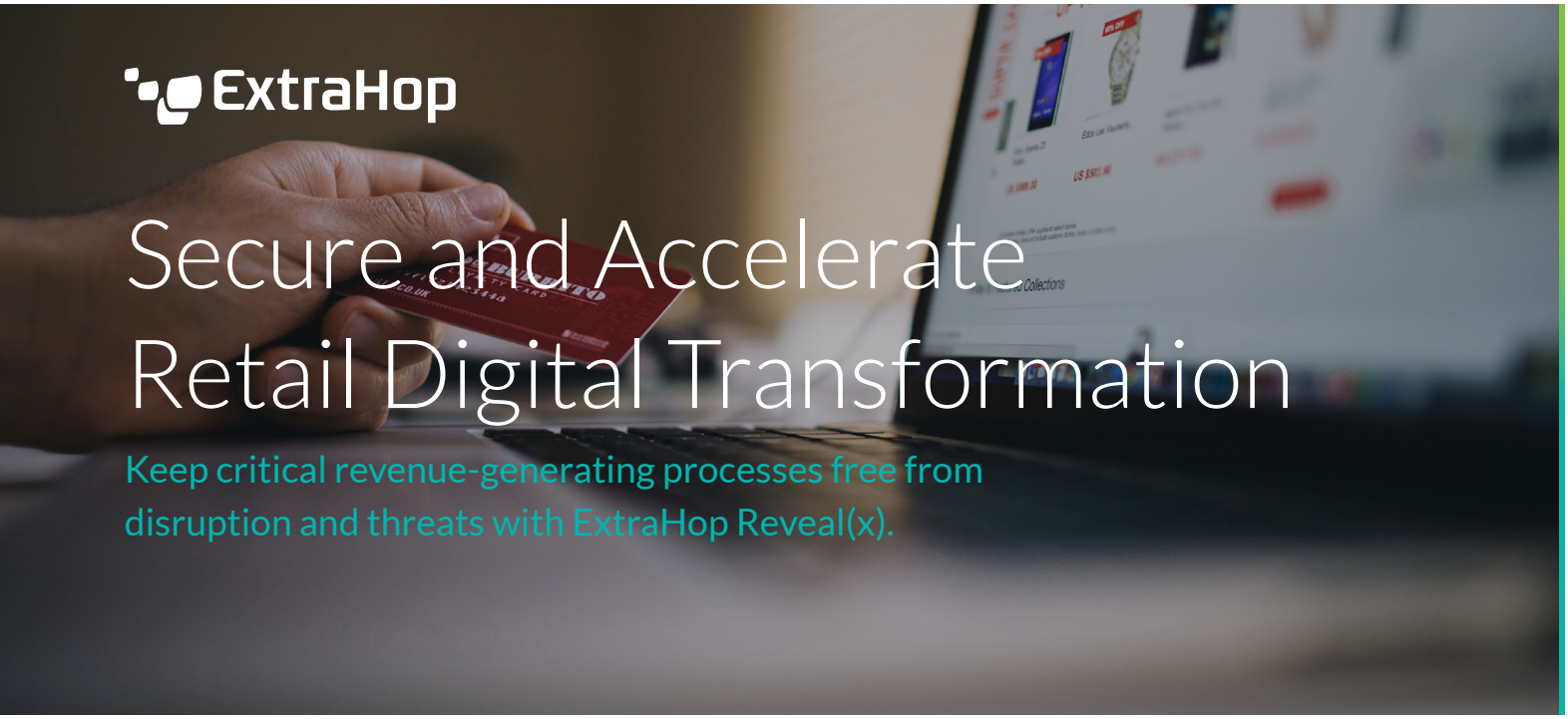

Secure and Accelerate Retail Digital Transformation

Keep critical revenue-generating processes free from disruption and threats with ExtraHop Reveal(x).

From brick and mortar to e-commerce, retail businesses are no stranger to risk. Operating on tight margins, facing constant competition, and shifting consumer preferences keep the threat of disruption top of mind. The impact of the global COVID-19 pandemic has only heightened the challenges.

Retailers are embracing Digital Transformation (DX) to gain a competitive edge. Improving customer experiences and achieving operational efficiencies are paramount to survival in an increasingly digital world.

The Challenge

Accelerating omnichannel expansion, spinning up new interactive and personalized purchasing experiences, and migrating to public clouds are just a few ways retail is realizing digital transformation. As new initiatives roll out, an expanded attack surface increases the risk of compromise and impacted service levels.

Digitizing shopping workflows, supporting contactless payment systems, or deploying self-service kiosks risk exposing sensitive personally identifiable information (PII) and payment details.

Reengineering revenue-generating applications to leverage public cloud infrastructure introduces operational visibility challenges across hybrid environments.

Adopting Internet of Things (IoT) devices like handheld scanners or beacons in retail locations, warehouses, and throughout fulfillment networks create new entry points and attack vectors for malicious actors.

Automating processes in distribution and data centers promise increased operational efficiency while also adding new potential points of failure.

Maintaining compliance with PCI Data Security Standard (DSS) requirements and other data protection regulations is complicated and time-consuming for stretched IT resources.

TAKE AWAY

As retail DX initiatives build upon complex hybrid infrastructures—with a mix of modern and legacy applications, cloud services, and connected devices—operational visibility is needed to stave off disruption.

The Opportunity: Complete Visibility, Closer Collaboration, and Faster Response

Supporting rapid adoption and resiliency to meet the challenges retailers face, IT organizations need complete visibility to ensure operational efficiency and stop threats before they breach the network. Only with a comprehensive view of the entire retail environment and closer incident response collaboration can IT operations teams keep one step ahead of unplanned outages, breaches, or ways to achieve greater efficiencies.

UNIFY VISIBILITY TO KEEP REVENUE-GENERATING APPLICATIONS SECURE AND AVAILABLE

Visibility is a cornerstone of every security and service management framework. Complete, real-time visibility is vital to ensure retail revenue-generating uptime and safeguard from cyber threats.

Retail IT functions—network, security, and cloud ops teams—that closely collaborate to identify gaps, blind spots, troubleshoot degraded shopper experiences, and uncover threats increase the speed and scale of a retailer's revenue-generating workflows by:

- Detecting suspicious behaviors and prioritizing forensic investigations and remediation to address the highest risk cyber threats
- Monitoring continuously and automating audits to stay compliant with regulatory requirements
- Identifying shopper experience issues and reduce troubleshooting time through real-time operational awareness

CONFIDENTLY FLEX AND SCALE TO THE CLOUD

Public clouds offer cost-effective means to scale to meet demand bursts—such as Black Friday or Cyber Monday shopping surges. However, the complex web of hybrid infrastructure that results creates exploitable blindspots that increase risk.

Retail IT teams that embrace a cloud-native approach to managing operations across on-premises and multiple cloud environments minimize risk and management burden by:

- Automating the discovery and classification of assets across hybrid infrastructures to maintain a real-time view
- Embracing advanced encryption—like TLS 1.3—without losing visibility into network traffic activities
- Correlating dynamic asset information, real-time network metadata, and activities to respond to the alerts that matter

ACHIEVE REAL-TIME DEVICE AND IOT AWARENESS

Retailers continue to adopt a wide range of IoT and smart devices to improve all aspects of the shopping experience. More than 60% of retailers are currently deploying IoT capabilities[1], and that number is expected to skyrocket as 5G is increasingly available. Managing and monitoring IoT can be difficult, if not impossible, making it challenging to identify failing or compromised devices.

Retailer IT teams that employ continuous, real-time discovery and classification of all devices, including unmanaged or un-instrumentable devices, minimize risk without impacting business by:

- Ensuring no connected device or asset goes undiscovered on the network
- Mapping device relationships, peer groups, and behaviors in real-time to identify suspicious actions
- Detecting device activities to spot threats and anomalous behavior like malicious attempts to gain access or move laterally

The Solution: Cloud-native Network Detection and Response

ExtraHop Reveal(x) is the only Cloud-Native Network Detection and Response solution that provides the scale, speed, and visibility required by retailers to rise above the noise of increasingly complex, hybrid infrastructure powering Digital Transformation in retail.

Unlike perimeter-focused tools that rely on fixed agents or gateway devices, Reveal(x) passively monitors your network and analyzes all network interactions to deliver complete visibility, real-time detection, and intelligent response.

Quickly find and solve problems ranging from slow shopper experiences to addressing security gaps and investigating threats in both the east-west and north-south corridors.

Complete Visibility

Achieve 360-degree visibility—without agents—of hybrid networks.

Automate the discovery of every asset on the network.

Identify and profile every managed, unmanaged, or rogue device—including enterprise IoT.

Real-Time Detection

Streamline operations with one integrated workflow for security, network operations, and cloud teams.

Detect suspicious activity using cloud-scale machine learning and advanced behavioral analysis to identify threats and performance anomalies with high fidelity.

Monitor and safeguard network traffic in real-time—including SSL/TLS encrypted traffic—up to 100 Gbps.

Intelligent Response

Accelerate investigation workflows with associated packets for any incident just a click away.

Save analyst time and automatically uplevel operational staff to take on more significant investigative responsibilities.

Automate and orchestrate responses through integrations with SIEM, EDR, SOAR, and NGFW, and more.

With complete visibility, retail digital transformation initiatives can be safeguarded from threats. Retailer IT teams can identify vectors of attack ahead of disruption, understand the full implication security events have on application performance and speed resolution for greater peace of mind.

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 can 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
877-333-9872 (voice)
206-274-6393 (fax)
info@extrahop.com
www.extrahop.com

Sources: [1] BDO 2020 Retail Digital Transformation Survey