Accelerate Zero Trust Adoption with Reveal(x)

Network detection and response enables a Zero Trust architecture more rapidly and at lower risk

Plan, Implement, and Secure

Zero Trust initiatives are on the rise. Distributed workforces and widespread cloud adoption have rendered traditional network-boundary security less effective. Once past perimeter defenses, adversaries gain unfettered lateral movement across the network.

Trust and trusted access can no longer be based on a user's or device's location. As a result, growing numbers of public sector organizations at federal, state, and local levels have started to embrace a Zero Trust security model.

The need to adopt Zero Trust is evident. However, the path to success is not as clear.

Network Data Speeds Zero Trust Success

ExtraHop Reveal(x) network detection and response (NDR) delivers the complete visibility and increased collaboration across IT operations needed to achieve your Zero Trust mandate more rapidly and with lower risk.

Reveal(x) unlocks actionable insights into network assets, cloud workloads, applications, and users by passively monitoring all traffic traversing your hybrid environment. Advanced behavioral analysis transforms dynamic and opaque network communications into real-time situational awareness. The complete coverage and real-time visibility help IT teams know everything on the network, continuously verify Zero Trust policies are working, and detect malicious behavior before it's too late.

As everything touches your network, network data becomes a natural single-source of ground truth to eliminate friction between IT operations silos. By breaking down silos between NetOps, SecOps, CloudOps, and IT Ops, Reveal(x) makes the news levels of collaboration possible.

Support all phases of your Zero Trust rollout

Gain complete coverage and real-time visibility

Scale from core to cloud to a remote workforce

Eliminate friction between NetOps, SecOps, CloudOps, and IT Ops

COMPLETE VISIBILITY OF YOUR ZERO TRUST ARCHITECTURE

Achieve 360-degree visibility—without agents—of hybrid networks, cloud transactions, and device types.

Automate the discovery of every asset on the network.

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

REAL-TIME DETECTION OF THREATS TO ZERO TRUST SAFEGUARDS

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

Detect suspicious activity using advanced machine learning and 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 to validate segmentation outcomes.

INTELLIGENT RESPONSE ACROSS YOUR ZERO TRUST ENVIRONMENT

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

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

Integrate with solutions like CrowdStrike, Phantom, Demisto, and Palo Alto Networks and automate remediation.

ExtraHop Reveal(x) is the only cloud-ready network detection and response product that provides the scale, speed, and visibility required by public sector organizations.

Reveal(x) eliminates blind spots other tools miss and gives public sector IT teams the confidence to meet their Zero Trust goals without compromising their ability to support the institution's mission.

Learn More

Reach out to your ExtraHop representative for more information. Ready to try Reveal(x) for yourself?

START DEMO

ABOUT EXTRAHOP NETWORKS

ExtraHop

ExtraHop provides cloud-ready 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**.

info@extrahop.com
www.extrahop.com