ExtraHop

Reveal(x)

for Microsoft Azure

NETWORK TRAFFIC ANALYSIS FOR HYBRID ENTERPRISES

Illuminate Darkspace in the Cloud

Security teams face the constant challenge of needing to gather large amounts of data and act quickly based on what they see. To do that, they need total visibility into every transaction throughout their network. Getting answers, however, isn't always straightforward—especially in the cloud.

ExtraHop Reveal(x) brings new visibility and security to Microsoft Azure to fulfill shared responsibility requirements and eliminate the cloud "darkspace", allowing the SOC's scope of monitoring and incident response to encompass cloud infrastructure. By integrating with Azure, Reveal(x) presents a fundamentally new way of analyzing every digital interaction occurring on the network while providing unprecedented visibility, definitive insights, and immediate answers to secure the hybrid enterprise.

AUTOMATIC DATA ACQUISITION

Integrated deployment via Azure's Virtual Network Tap means instant, seamless access to full network traffic analysis.

DESIGNED FOR SPEED + EFFICIENCY

Collect and process all your data in real time at enterprise scale, without risk of diminished analysis: every transaction, everywhere, all the time.

TRANSACTION FLUENCY

In real time, we decode 50–plus protocols to expedite detection and response based on complete insights captured across the entire attack surface.

MACHINE LEARNING

We analyze 4,600 features extracted from wire data that we use to guide machine learning models.

FROM DATA CENTER TO THE CLOUD

Cloud is the future of digital business but complex architectures and the opportunity for misconfiguration leave you open to potentially catastrophic risk. ExtraHop Reveal(x) for Azure automatically discovers every cloud instance and begins identifying suspicious activity immediately, delivering real-time visibility at cloud scale. By integrating and contextualizing suspicious events into a unified analytics and investigation environment, Reveal(x) helps cloud-focused SOC teams respond with confidence and speed.

- Detect late-stage attack activities with machine learning trained on 4,600+ metrics
- Pivot from cloud-specific insights to forensic-level evidence in seconds

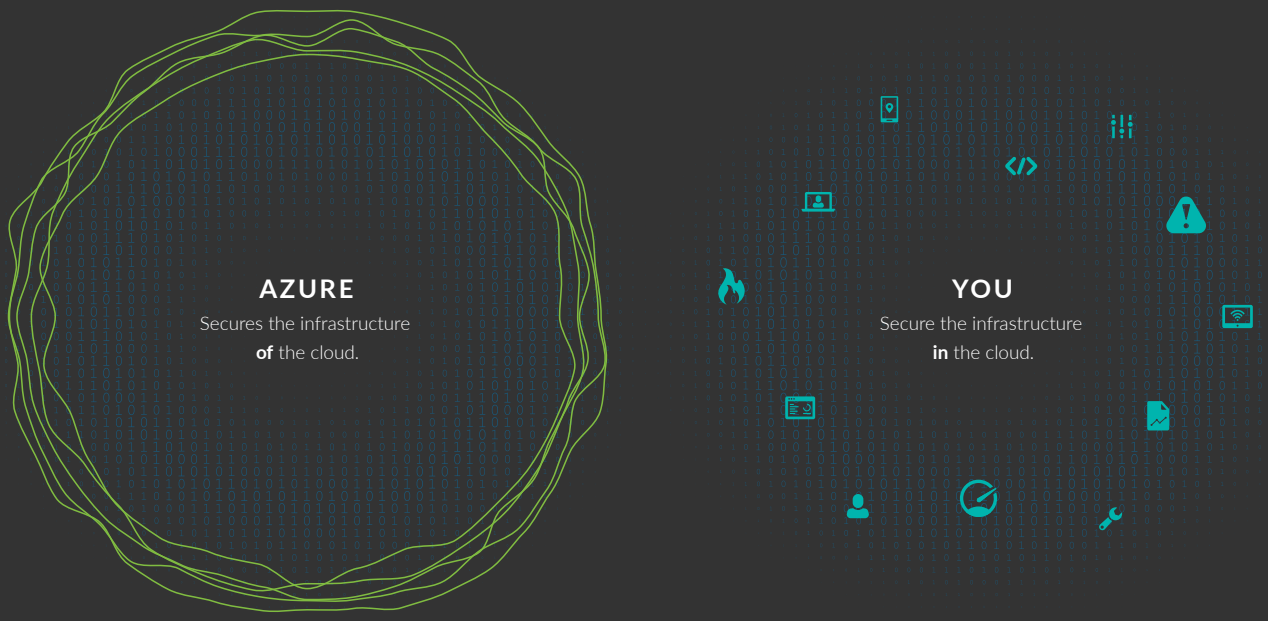
GO BEYOND FLOW LOGS

Reveal(x) uses Azure's industry-first virtual network tap to take you far beyond flow logs. Unlike any other solution on the market, Reveal(x) analyzes and decodes more than 50 protocols at 10 Gbps of data per virtual appliance—including full support for Azure SQL Databases and Azure Blob Storage protocols.

- Reveal(x) decrypts TLS 1.3 and other forms of encryption at line rate
- Integrate real-time wire data detections with Azure Security Center metrics and Structured Threat Information Expression (STIX) data

SHARE THE RESPONSIBILITY

ExtraHop Reveal(x) for Azure supports the customer's responsibilities under the shared responsibility model: data access, identity and access management, network security, and application security. By integrating and contextualizing cloud events with other infrastructure activities to create a unified analytics and investigation environment for SOC teams, Reveal(x) for Azure provides always-on, always-everywhere analysis of the application layer across the hybrid attack surface.



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, Reveal(x) 360, uses cloud-scale AI to help enterprises detect and respond to advanced threats—before they can compromise your business. With complete visibility from ExtraHop, enterprises can detect intrusions, hunt threats, and investigate incidents with confidence. 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