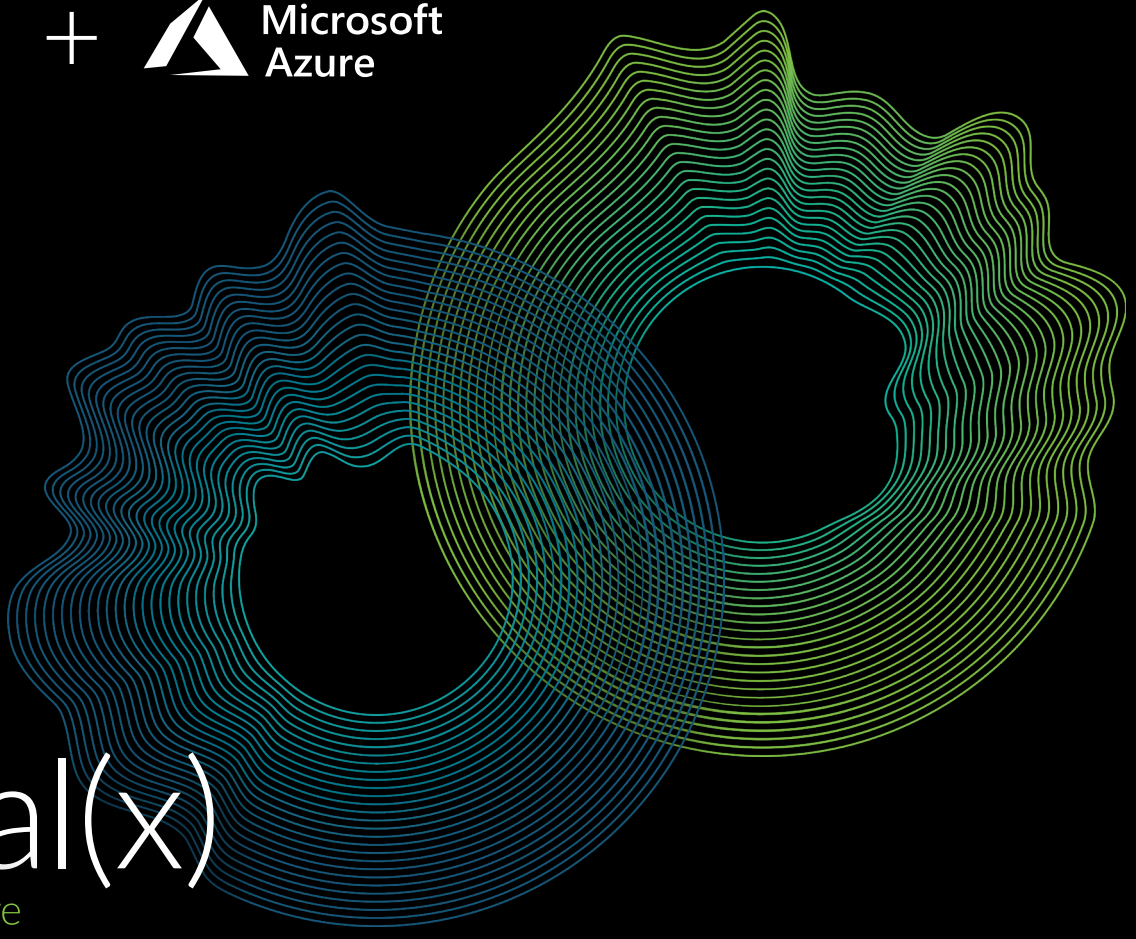
ExtraHop + Microsoft Azure



Reveal(x)

for Microsoft Azure

Protect applications and data in your Microsoft Azure environment with cloud-native network detection & response (NDR).

SECURE YOUR INVESTMENT IN AZURE CLOUD

As enterprises migrate more business-critical applications to the cloud in order to take advantage of greater scale and efficiency, the pressure is on for SOC teams to move security with them.

ExtraHop Reveal(x) for Azure provides the inside-the-perimeter visibility, threat detection, investigation, and response you need to secure applications and data across your hybrid environment.

Cloud Threat Detection

ExtraHop Reveal(x) for Azure targets the top three threat categories in cloud environments: misconfiguration, unauthorized access, and insecure APIs. Reveal(x) combines deep content insights and transaction fluency with event data from Azure Security Center to identify events of interest including rogue instances, disabled log systems, and suspicious file execution. ExtraHop Reveal(x) for Azure discovers and classifies everything traversing your environment.

Rich Transactional Data

ExtraHop is the only vendor who converts all wire data to a fully indexed record of every element of every transaction. It's an exponential gain in empirical data that has never before been available. We deliver the largest and richest set of factual and contextualized data to answer the most important questions coming from your Security and Operational teams. No other source comes close to delivering the depth, breadth, and value derived from our data.

Shared Responsibility

No other platform delivers the visibility required to effectively meet shared responsibility models and prioritize the use of security resources (SOC analysts, security infrastructure) based on critical assets and risk. Cloud service providers use a shared responsibility approach that leaves most of the security responsibility up to the enterprise. Reveal(x) for Azure provides visibility to tackle the burdens that SecOps has to carry.

HOW IT WORKS

Reveal(x) leverages the Microsoft Azure Virtual Network Tap (vTAP) to combine real-time analysis of network traffic with security events from Azure Security Center, providing analysts with everything they need to respond with confidence.

KEY FEATURES

By combining network traffic analytics with security events from Azure Security Center, Reveal(x) provides everything an analyst needs for confident response.

- **Out-of-Band Decryption**
  Decrypt and analyze all SSL/TLS 1.3 traffic at line rate.
- **Transaction Fluency**
  Decode 70+ protocols to expedite threat detection, investigation and response.
- **Cloud-Scale Machine Learning**
  Leverage 5,000+ features extracted from wire data for behavioral detection.

COMPLETE VISIBILITY

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

SEAMLESS DEPLOYMENT

By automatically deploying to new cloud environments via the Azure vTAP, Reveal(x) begins automatically identifying threats in cloud darkspace immediately – as quickly as one second.

ABOUT EXTRAHOP NETWORKS

ExtraHop is the leading provider of cloud-native network detection and response (NDR) for the hybrid enterprise. With complete visibility, real-time threat detection, and automated investigation powered by cloud-scale machine learning, ExtraHop enables security teams at leading enterprises including Credit Suisse, The Home Depot, Caesars Entertainment, and Liberty Global to rise above the noise of alerts, organizational silos, and runaway technology in order to accelerate investigations, unify policies across hybrid environments, and build their security the way they're building their business: cloud-first. To experience the power of ExtraHop, explore our interactive online demo at www.extrahop.com/demo.

ExtraHop

520 Pike Street, Suite 1600
Seattle, WA 98101
877-333-9872 (voice)
206-274-6393 (fax)
info@extrahop.com
www.extrahop.com