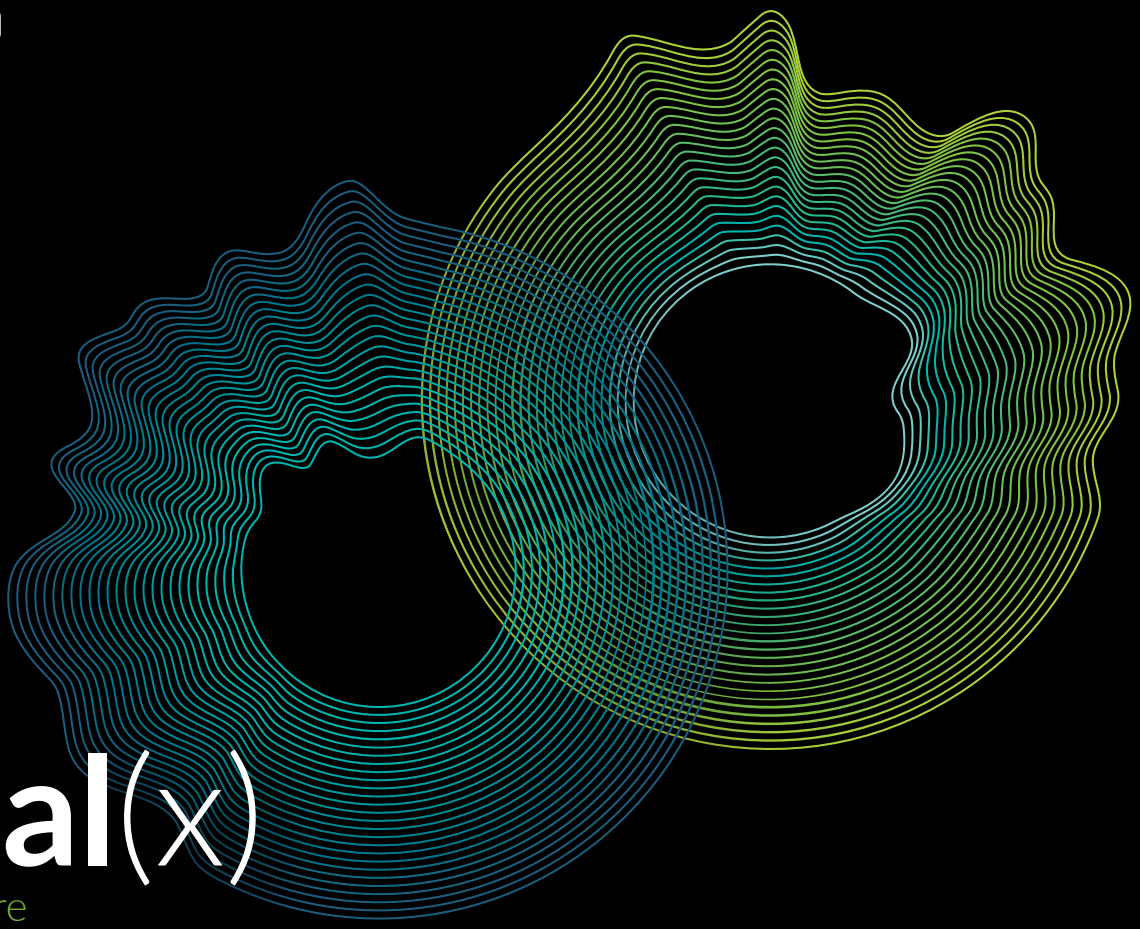
ExtraHop



Reveal(x)

for Microsoft Azure

Seamless Security for Hybrid Enterprises

YOUR ENTERPRISE IS EVERYWHERE. IS YOUR SECURITY?

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

ExtraHop Reveal(x) for Azure provides the East-West visibility and deep contextual insights you need to preserve the security of your applications and data no matter where they live: on-premises, in the branch office, or with your cloud provider.

Cloud Threat Detection

ExtraHop Reveal(x) for Azure targets the top three threat categories in cloud environments: misconfiguration, malicious data access, and application security. 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 that 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 the Security and Operational teams. No other data source comes close to the amount of data and the value derived from the data.

Shared Responsibility

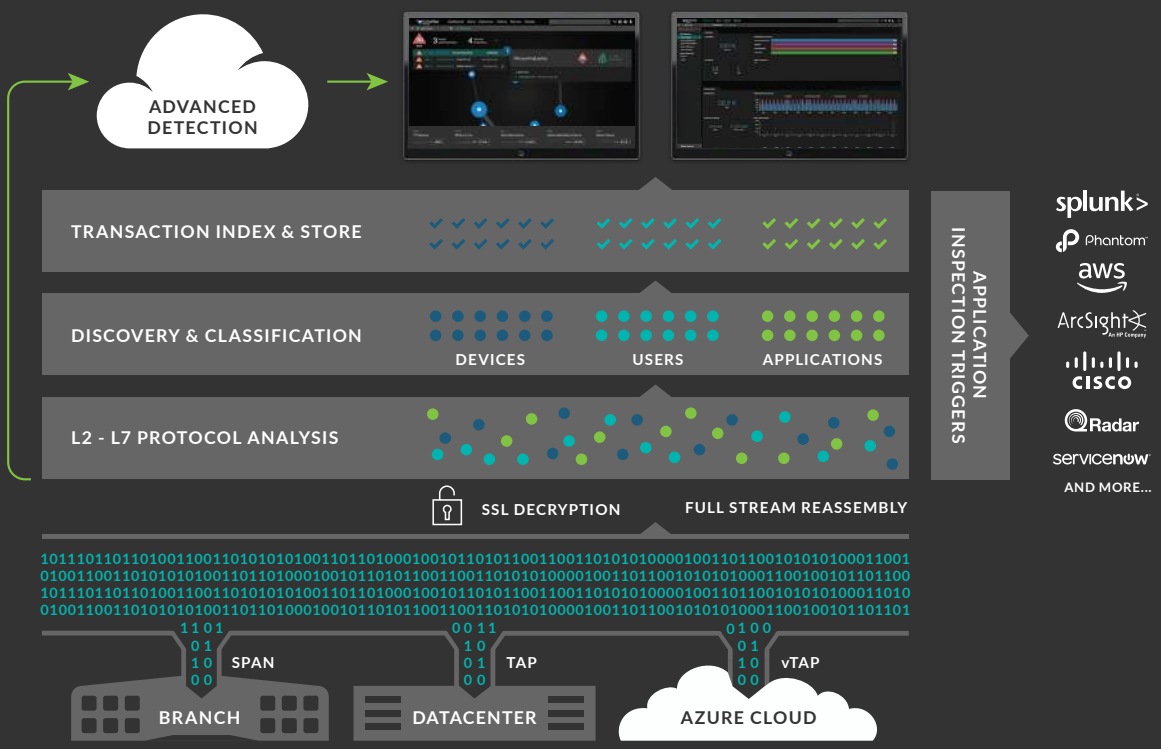
No other platform delivers the visibility required to effectively meet shared responsibility models and prioritize use of security resources (SOC analysts, security infrastructure) based on critical assets and risk. Cloud vendors use a shared responsibility approach that leaves most of the security responsibility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

Seamless Deployment + Immediate Insight

By automatically deploying to new cloud environments via the Azure Virtual Network Tap, Reveal(x) for Azure begins automatically identifying threats in the cloud darkspace immediately – as quickly as one second. By combining network traffic analytics with security events from Azure Security Center, Reveal(x) provides everything an analyst needs to know to respond.

HOW IT WORKS

Powered by wire data, the richest data source available, ExtraHop Reveal(x) focuses behavioral detection on critical assets providing fast, high-fidelity insights into what matters in your environment.



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.

ABOUT EXTRAHOP NETWORKS

ExtraHop is the first place IT turns for insights that transform and secure the digital enterprise. By applying real-time analytics and machine learning to all digital interactions on the network, ExtraHop delivers instant and accurate insights that help IT improve security, performance, and the digital experience. Just ask the hundreds of global ExtraHop customers, including Sony, Lockheed Martin, Microsoft, Adobe, and Google. To experience the power of ExtraHop, explore our interactive online demo. Connect with us on Twitter, LinkedIn, and Facebook.

ExtraHop

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