ExtraHop

EBOOK

USE CASES FOR A SECURE HYBRID ENTERPRISE

Reveal(x) 360

Cloud-Native Network Detection and Response Delivered as a SaaS

TABLE OF CONTENTS

50% FASTER THREAT DETECTION

84% FASTER THREAT RESOLUTION

99% FASTER TROUBLE-SHOOTING

INTRODUCTION

Modern Attack Surfaces and Security Gaps

The attack surface stretches from the on-prem data center to the cloud to remote deployments and the device edge. But tools that only secure the perimeter, rely on logs, or require agents only show part of the picture and can be difficult to scale.

As a result, 62% of IT and cybersecurity professionals say they have gaps in their coverage.[1]

Security teams need the ability to see every device, every workload, every user, everywhere—and detect and confidently respond to advanced threats anywhere—in real time. What they're missing is unified coverage, available in a single interface and powered by the richest data source in hybrid security: network traffic packets.

ExtraHop Reveal(x) 360 brings the power of network traffic packets to hybrid security, helping organizations manage the attack surface, decrease risk, and stop breaches up to 84% faster.[2]

With SaaS-based Reveal(x) 360, SecOps teams can detect, investigate, and respond to threats from the data center to the cloud to the user and device edge in a single management pane.

This unified approach eliminates the complexity of deploying and operating separate tools in each environment. It also removes the friction caused by data silos between security and IT teams who need to collaborate closely in order to provide a safe, reliable digital experience.

For cloud deployments, Reveal(x) 360 leverages native integrations with packet mirroring features from Amazon Web Services and Google Cloud, as well as the announced Microsoft Azure vTAP, to unlock network detection and response (NDR) for cloud security without the need for cumbersome agents.

1 ExtraHop 2021 Cloud & Hybrid Security Tooling Report https://www.extrahop.com/resources/whitepapers/cloud-and-hybrid-security-tooling-report

2 Forrester Study: Total Economic Impact of ExtraHop Reveal(x) https://www.extrahop.com/resources/analyst-reports/forrester-tei-study/

OVERVIEW

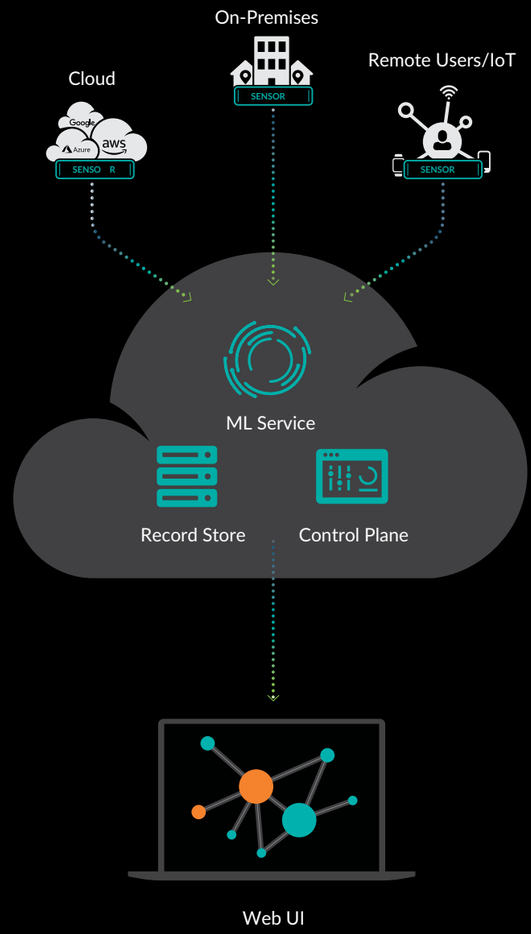
Reveal(x) 360 at a Glance

Unified Security Across Deployments

As the first and only SaaS-based NDR solution on the market, Reveal(x) 360 extends cloud-native security across hybrid and multicloud environments by providing full visibility, real-time threat detection, and intelligent response at enterprise scale. Integrated workflows accelerate threat hunting and amplify organizational resources.

ExtraHop sensors deployed in data centers, clouds, and remote sites decrypt and process network data, extracting records and de-identified metadata which are sent securely to Reveal(x) 360 for behavioral analysis, real-time threat detection, and investigation. ExtraHop offers two models for sensor purchases: reserved priced and a consumption-based model for on-demand sensors billed by the hour and available through the Reveal(x) 360 cloud console.

A cloud-based record store with 90-day lookback provides fully hosted and managed search for streamlined incident investigation. A cloud-hosted control plane—accessible from anywhere via the secure web-based Reveal(x) 360 user interface—gives you a unified view of the environments where sensors are deployed.



ExtraHop

Reveal(x) 360
USER BENEFITS

Stronger Security with Agentless Network Detection and Response

ELIMINATE BLIND SPOTS
with Complete Coverage

DETECT THREATS
up to 50% Faster

STOP BREACHES
up to 84% Faster

Fill Security Monitoring Gaps
With Reveal(x) 360, SecOps teams can detect, investigate, and respond to threats from the data center to the cloud to the user and device edge in a single management pane. Continuous monitoring and L2–L7 analysis ensure end users are always up to date and in the know.

Secure Hybrid Environments Without Friction
By integrating with Amazon VPC Traffic Mirroring, Google Cloud Packet Mirroring, and the announced Azure Virtual TAP, Reveal(x) 360 eliminates friction caused by deploying agents, making it highly elastic and easier to scale. Reveal(x) 360 also integrates with third-party packet brokers on-premises and in the cloud.

Gain Complete Visibility and Rich Insight
Reveal(x) 360 provides east-west and north-south visibility as well as packet-level insight and out-of-band decryption of SSL/TLS 1.3 encrypted traffic at line rate.

Detect Threats in Real Time
By combining machine learning-powered behavioral analysis with rules-based detection, peer group analysis, and deep learning, Reveal(x) 360 identifies known and unknown threats and provides holistic coverage of attacker tactics, techniques, and procedures.

Respond Quickly and Confidently
Reveal(x) 360 automates the first steps of investigations to streamline workflows, enabling you to go from alert to response in clicks, not days. For deeper context, you can dig into a cloud-based record store with 90-day lookback.

Reduce Time to Deploy and Management Burden
As a SaaS-based solution that doesn't require agents, instrumentation, or configuration, Reveal(x) 360 deploys quickly in hybrid environments. For AWS deployments, you can deploy Reveal(x) 360 on-demand sensors directly from the cloud console.

See Value Immediately
As soon as it's deployed, Reveal(x) 360 begins passively monitoring network traffic and starts learning complex relationships through continuous asset discovery, classification, and mapping.

ExtraHop

Reveal(x) 360

HYBRID SECURITY USE CASES

Gain Complete Coverage. Detect Threats Faster. Act Quickly.

Organizations with hybrid deployments need security that evolves with their digital transformation. With agentless visibility delivered as a SaaS, Reveal(x) 360 provides the elastic, highly scalable threat detection and response capabilities that meet organizations wherever they are in their hybrid cloud journey.

ExtraHop

COMPREHENSIVE INVENTORY OF ALL DEVICES

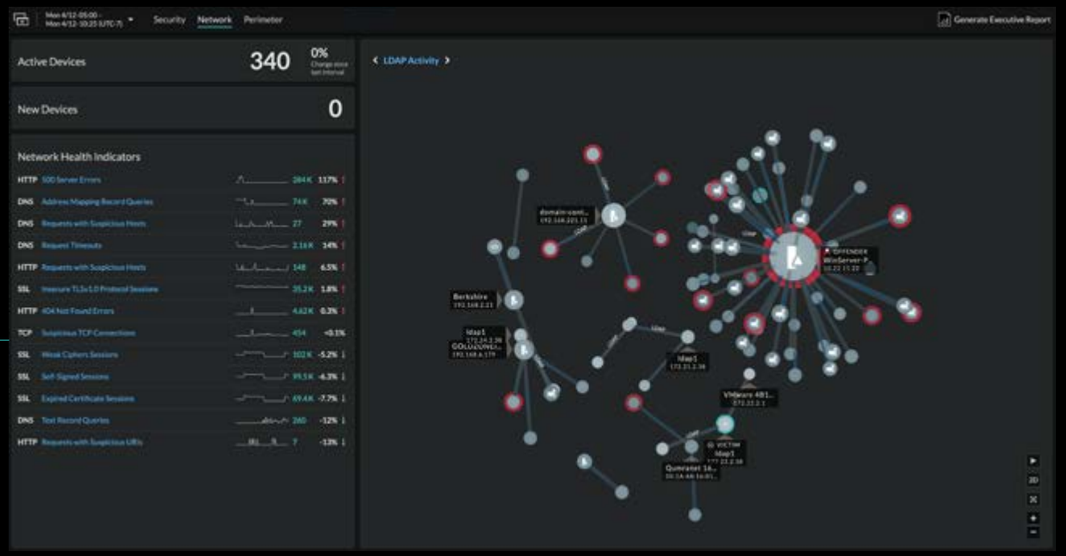
Unmanaged, uninstrumentable, and rogue devices create significant security risk. Reveal(x) 360 passively monitors all network-connected assets, including IoT and employee-owned devices. Behavior-driven device discovery helps you understand what each device is and how it's interacting with every other device.

- Gain a complete inventory of your hybrid environment with automatic discovery as soon as a device connects.
- Understand device relationships, peer groups, and behaviors in real time.
- Access deeper device details, including hardware, operating systems, users, protocols, behavior history, and much more.

How many of your devices are not covered by your current security tooling?

How do you identify unmanaged, uninstrumented, and rogue devices?

What's your process for ensuring new devices are instrumented by your security tooling?



Asset dependency mapping available through the Reveal(x) 360 user interface.

ExtraHop

MONITOR SENSITIVE DATA

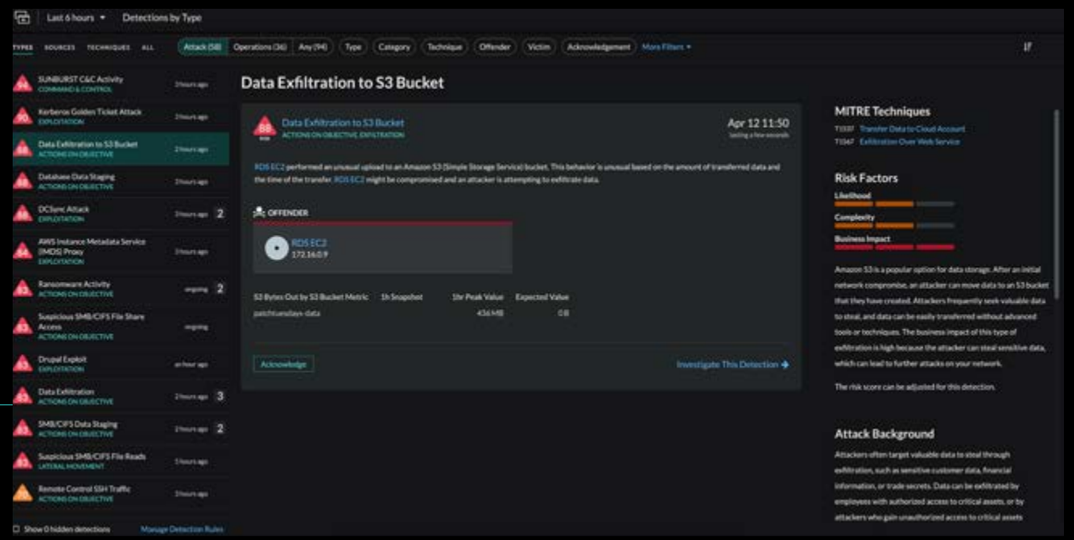
Attackers can't steal data without moving it across the network. But data protection products, zero trust architecture, and logging with manual post-hoc analysis create large blind spots, slow down investigation and response, and create significant implementation and administration burdens. Reveal(x) 360 provides rich context into the "who," "what," "when," and "where" of every data transfer—even with perfect forward secrecy enabled—for faster investigation, deeper understanding, and more rapid response.

How do you currently monitor access to sensitive data?

How do you detect unauthorized movement of large quantities of sensitive data?

How do you get context to know if a data transfer is malicious?

- See all data movement from a network perspective to automatically identify data sensitivity.
- Trace internal data transfers as well as movement to external endpoints, APIs, and cloud services.
- Gain instant access to packet-level forensics for data leakage as well as access to decryption keys.



Monitor data exfiltration in hybrid environments through the Reveal(x) 360 user interface.

ExtraHop

DETECT POST-COMPROMISE RECON AND LATERAL MOVEMENT

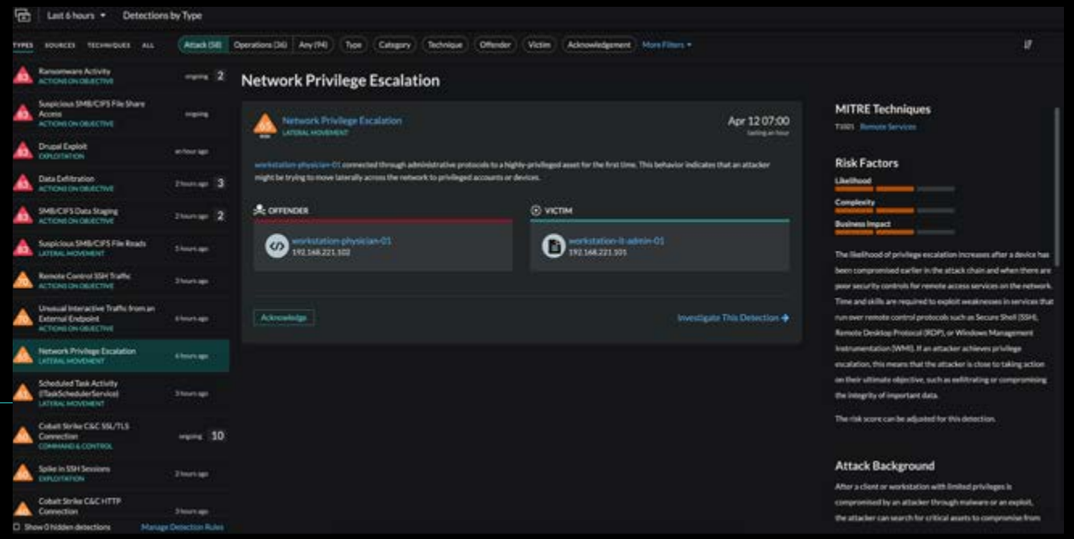
Once attackers compromise a workstation and steal credentials, it's extremely difficult to detect them. The limitations of perimeter-focused tools, logging, and endpoint tools create significant blind spots in the east-west traffic corridor where attackers pivot to critical assets and expand their foothold. Reveal(x) 360 helps you protect your "crown jewels" from late-stage attacks and probing activities in hybrid environments.

- Gain a comprehensive view of activity across hybrid environments.
- Detect behaviors such as unusual login time and suspicious interactive traffic.
- Speed up time to detect and respond.

What percentage of your hybrid environment is covered by log and endpoint data?

What network controls do you have in place to discover and limit device activity?

How do you track normal and abnormal account activity?



Gain up-to-the-moment insight into unusual activities that indicate post-compromise behaviors.

STREAMLINE THREAT HUNTING

Threat hunting helps reduce organizational risk and provides valuable intelligence to augment detection capabilities and strengthen security posture. But existing threat hunting tools that rely on host-reported data can be evaded or tampered with by attackers, creating blind spots and causing security teams to miss more sophisticated threats. Reveal(x) 360 provides guided workflows for threat hunting, a complete dataset to develop and test hypotheses, and mechanisms to automate hunting techniques, made simple and accessible for analysts of any experience level.

What is your organization's current approach to threat hunting?

What are the barriers to expanding your threat hunting capabilities?

How do you use network data in your threat hunting activities?

- Zero in on transactions of interest to threat hunters.
- Quickly test granular and wide-ranging threat hunting hypotheses.
- Rapidly research and validate a wide variety of indicators of compromise (IOCs).

Reveal(x) 360 provides dashboard and query-based starting points for threat hunting.

ExtraHop

Reveal(x) 360

CLOUD SECURITY USE CASES

Eliminate Blind Spots. Detect Threats Other Tools Miss. Respond Faster.

Purpose-built for cloud, multicloud, and hybrid environments, Reveal(x) 360 helps you strengthen your security posture and harden your complex attack surface. Agentless deployment enables Reveal(x) 360 to provide complete visibility in ephemeral environments and removes security friction from DevOps processes.

ExtraHop

ELIMINATE CLOUD BLIND SPOTS

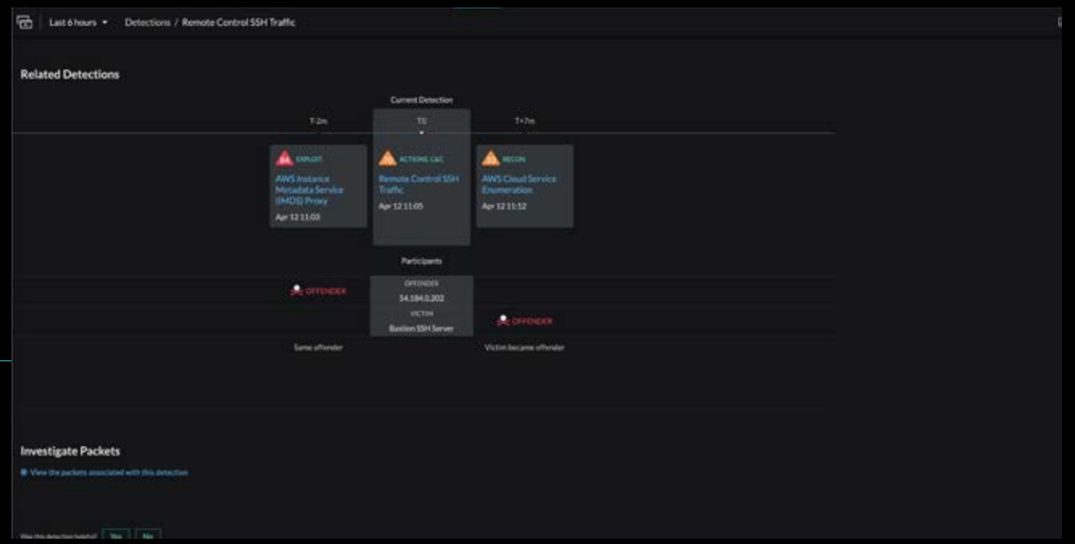
Understanding which cloud services are sending and receiving data is critical to securing sensitive data. With complete coverage across hybrid and multicloud deployments, Reveal(x) 360 enables security teams to monitor sensitive workloads no matter where they live.

- View cloud workload activity and identify anomalous behavior automatically.
- Trace data transfers inside the VPC and to external endpoints, APIs, and cloud services.
- Automatically provides the context of data flows: which users are sending and receiving, where data is going, and what the data contains.

How do you monitor access to sensitive data in the cloud?

How do you detect unauthorized movement of large quantities of sensitive data in the cloud?

Do you have visibility into encrypted traffic and up to Layer 7?



Reveal(x) 360 provides continuous visibility into sensitive cloud workloads and data through passive monitoring, even in encrypted traffic.

DISCOVER SUPPLY CHAIN ATTACKS

To truly secure supply chains, you need the ability to monitor cloud workloads for unexpected changes or communications with untrusted or unknown entities. Reveal(x) 360 decreases risk and helps you manage the attack surface to reduce potential damage from supply chain attacks.

- Continuous monitoring to quickly surface unexpected changes to cloud workloads.
- Machine learning infers which assets house critical data and makes forensics instantly available for data leakage.
- Detect whether production workloads are pulling updates when they shouldn't in real time.
- Quickly identify and examine unknown or unexpected communications.

How do you monitor and secure your workloads and container deployments in the cloud?

What processes do you have in place to assure that new dependencies introduced in production are secure?

Monitor AWS services through a dedicated pane in the Reveal(x) 360 user interface.

DETECT LATERAL MOVEMENT

Lateral movement is a necessary stage in every breach, and on average, there are 10 lateral movements in every attack. The ability to detect post-compromise recon and lateral movements is essential for securing critical data and cloud workloads. Although attackers can hide evidence of their tactics from logging tools, lateral movement between cloud workloads always generates network artifacts.

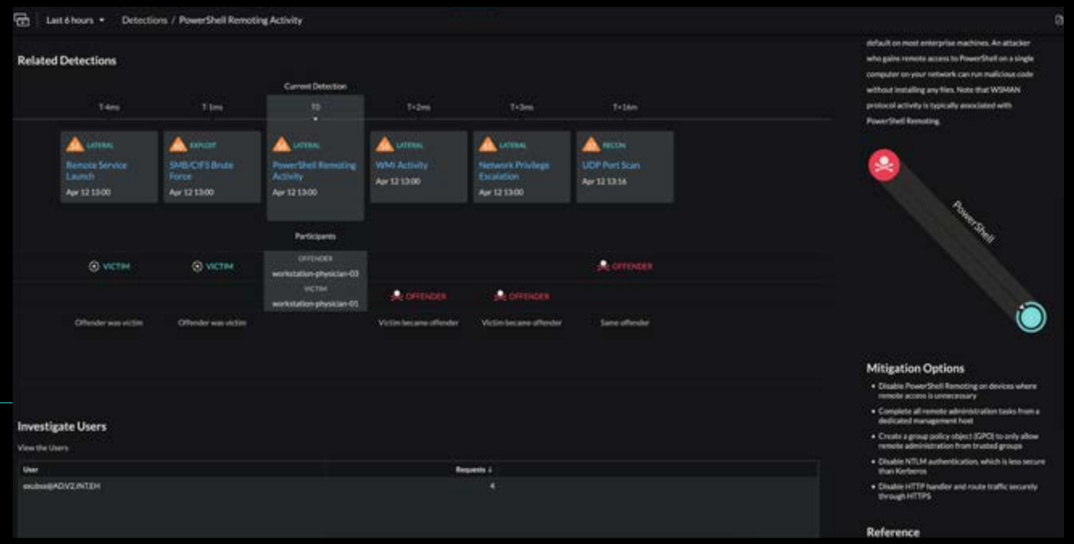
- Track privileged account activity and monitor anomalous communication across segments.
- Detect payload attacks using machine learning to identify behaviors such as “low and slow” data staging and exfiltration.
- Intuitive user interface adds necessary context that streamlines investigations, speeding response.

Do your existing security controls provide real-time detection of threats?

Can your network controls detect suspicious activity over encrypted channels?

How do you track normal and abnormal service account activity?

Detect and investigate communications between cloud workloads and outside entitles.



ExtraHop

RESPOND FASTER TO THREATS

Privacy regulations have strict disclosure rules that require IR teams to conduct investigations quickly and accurately. And yet, attacks can go undetected for weeks or months. With Reveal(x) 360, security teams can improve time to respond by up to **84%**.

- Accurately determine the scope of incidents for implementing appropriate response, internal assessment, and regulatory reporting.
- Instantly access automatically curated cloud asset information, network metadata, and forensic evidence in one solution.
- Intuitive investigation workflows to go from detection to context and forensics in clicks.

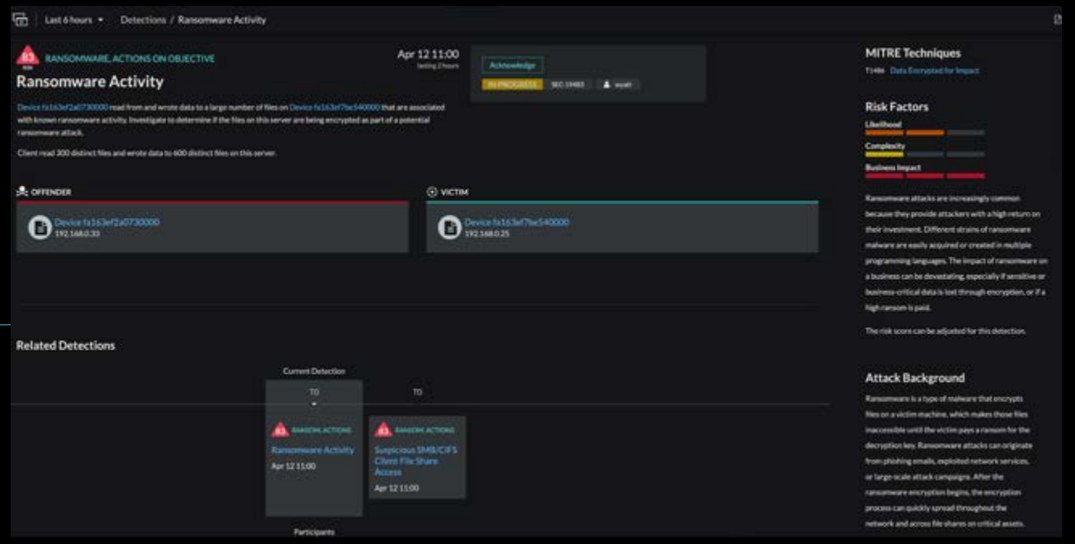
Are your tools causing alert fatigue and increasing your MTTR?

Do your current tools provide context and associate disparate cloud security events?

What information do you need during an investigation?

How many tools do you use to gather data?

Reveal(x) 360 enables faster triage of cloud security alerts with accurate, high-context detections.



ExtraHop

Reveal(x) 360

IT OPS USE CASES

Stop the Blame Game. Support Distributed Workforces. Be Cloud Ready.

Data silos, war rooms, and finger pointing. When broken user experiences and unexpected outages occur, they affect more than the bottom line. With Reveal(x) 360, you gain complete, real-time visibility to address application and network performance issues from a unified platform that works across cloud, on-premises, and hybrid environments.

QUICKLY RESOLVE PERFORMANCE ISSUES

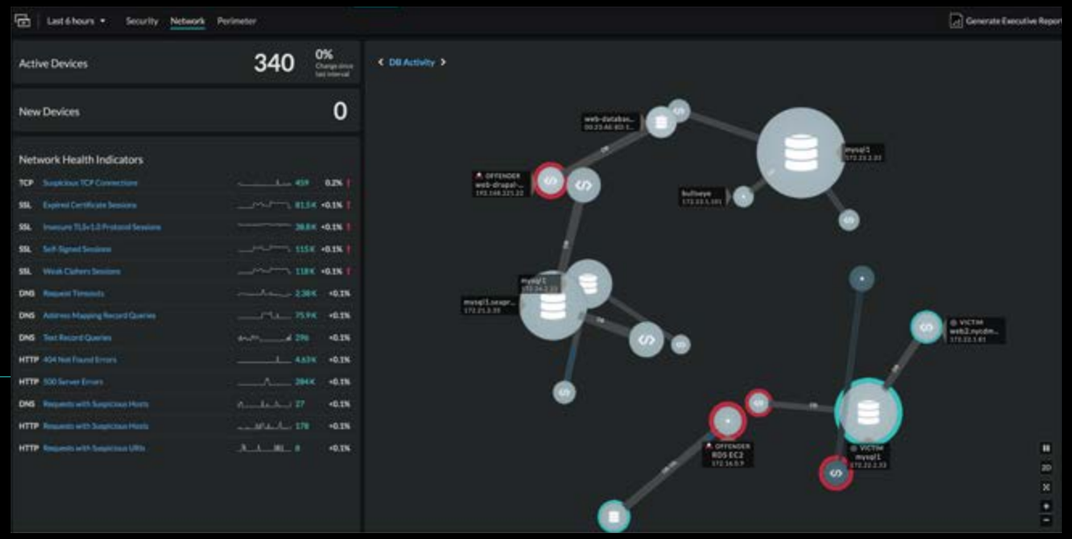
The ability to quickly resolve performance issues and reduce unplanned downtime is essential for delivering world-class user experience. Reveal(x) 360 enables you to quickly triage and troubleshoot with network-based monitoring that eliminates visibility gaps and speed up time to detect and respond.

- Automated device and application discovery, classification, and mapping to understand inventory and relationships.
- Correlate activity along the application delivery chain to understand in context exactly what's happening.
- Intuitive workflow speeds troubleshooting from issue to root cause in 3 clicks.

How do you mitigate data silos created by log and NetFlow-based tooling?

How comprehensive is your view of the application delivery chain?

Are you forced to conduct manual post-hoc analysis of UX issues?



Map device and application relationships and behaviors in real time.

ExtraHop

DETECT REMOTE ACCESS ISSUES AND OPTIMIZE TRAFFIC

As remote workers increase, so do the challenges associated with remote access infrastructure complexity and visibility. Encryption also limits visibility for many organizations. Reveal(x) 360 ensures better availability for remote workers by helping you solve network issues up to 92% faster. By providing the visibility and context organizations need to measure and understand utilization, Reveal(x) 360 helps eliminate bottlenecks without requiring infrastructure upgrades.

- Real-time view of the entire environment, including SSL/TLS 1.3-encrypted traffic, to understand utilization and dependencies.
- Detect issues across the distributed infrastructure and quickly troubleshoot network slowdowns.
- Create custom dashboards for continuous monitoring and tuning.

Where does visibility end and black box begin in your application delivery chain?

How do you gain visibility into SSL/TLS 1.3-encrypted traffic?

How do you currently ensure availability for remote workers?

Understand real-time utilization and dependencies.

ExtraHop

RELIABLY FLEX AND SCALE TO THE CLOUD

Infrastructure is increasingly hybrid with a mix of sanctioned and unsanctioned cloud services and SaaS applications that create governance and compliance issues while increasing support costs. Migration to the cloud increases the chances of broken user experiences. Reveal(x) 360 enables organizations to reliably flex and scale to the cloud.

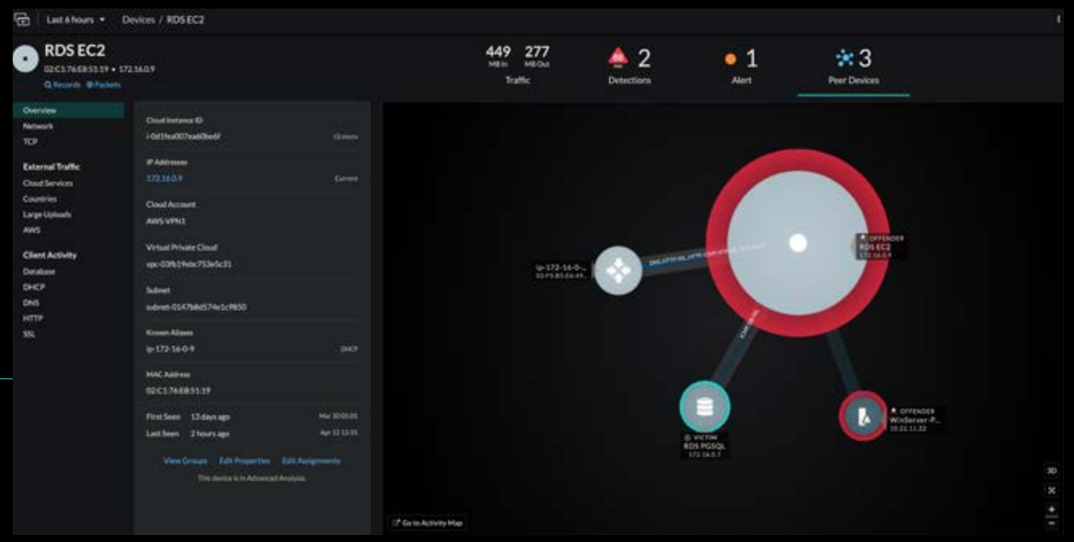
- Discover all application traffic and map and understand dependencies.
- Measure performance before, during, and after migration.
- Agentless operational visibility across on-premises, cloud, and hybrid environments from a unified platform.

How do you ensure an unbroken user experience when migrating to the cloud?

Which tools do you use for east-west and north-south visibility?

How do you discover shadow IT and map application dependencies?

Map and undestand dependencies for complete visiblity into every asset across cloud migrations.



ExtraHop

ON-DEMAND AND LIST PRICING

Cloud Sensors

Empower your security and IT teams to protect and monitor data and workloads from the device and remote edge to on-premises data centers and branch offices to the cloud.

You can deploy Reveal(x) 360 sensors across on-prem, cloud, and edge environments. AWS customers can deploy sensors, including on-demand sensors which can be easily selected through the Reveal(x) 360 cloud console. You can also purchase sensors for AWS environments via the Reveal(x) 360 listing on AWS Marketplace.

If you're interested in reserved or on-demand pricing, or if you need to deploy sensors in your data center, branch office, Azure, or Google Cloud environments, please contact an ExtraHop sales representative or your preferred Value Added Reseller (VAR) for assistance.

Reveal(x) 360 On-Demand Cloud Senors and List Pricing

EXTRA SMALL	1 Gbps throughput 20 GB daily record capacity	**$5.04/hr**
ULTRA EXTRA SMALL	1 Gbps throughput 20 GB daily record capacity Continuous PCAP	**$8.00/hr**

Cloud Record Store

A key component of Reveal(x) 360 is the cloud record store (CRS), which enables immediate access to in-depth network and threat information for the past 90 days. These records are stored securely in the cloud and provide analysts the ability to quickly determine root cause and remediate vulnerabilities.

ExtraHop records are structured information about transactions, messages, and network flows that are generated and sent from a Reveal(x) 360 sensor to the cloud record store for storage and retrieval. After your records are stored, you can easily query them from the Reveal(x) 360 console for investigation, threat hunting, and forensics with 90-days of lookback.

If you want to purchase additional bands of record capacity for AWS environments, you can transact via the Reveal(x) 360 listing on AWS Marketplace. To learn more about Reveal(x) 360 record capacity pricing, including reserved pricing, contact an ExtraHop sales representative or your preferred Value Added Reseller (VAR) for assistance.

Additional Record Capacity per Day - List Price (90-day lookback period)

50GB	$1.69 per GB / day
100GB	$1.41 per GB / day
200GB	$1.27 per GB / day
500GB	$1.01 per GB / day
1TB	$0.84 per GB / day

On-Demand Record Capacity

$1.69 per GB

Full Product Demo

START DEMO

Try Reveal(x) 360 for Free

FREE TRIAL

ExtraHop

Reveal(x) 360

Cloud-Native Network Detection and Response Delivered as a SaaS

50% FASTER THREAT DETECTION

84% FASTER THREAT RESOLUTION

99% FASTER TROUBLE-SHOOTING

aws partner network | competency

Google Cloud

Azure

North America | EMEA | APAC

ExtraHop