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

Closing Coverage Gaps Across the Hybrid Attack Surface

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 exclusively on logs, or require agents only show part of the picture and can be difficult to scale. Legacy tools also struggle to provide visibility and monitoring for containerized environments.

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

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

With SaaS-based Reveal(x) 360, you can detect, investigate, and respond to advanced threats like ransomware and software supply chain attacks in a single management pane. This unified approach eliminates the complexity of deploying 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 security, Reveal(x) 360 integrates with packet mirroring features from Amazon Web Services (AWS) and Google Cloud, as well as the announced Microsoft Azure vTAP to eliminate the need for agents.

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, forensic investigation, 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 passively monitors network traffic and starts learning complex relationships through continuous asset discovery, classification, and mapping. It also provides east-west and north-south visibility and out-of-band decryption of SSL/TLS 1.3 encrypted traffic at line rate.

Detect Threats in Real Time

By combining advanced AI analysis with rules-based detection, peer group analysis, and deep learning, Reveal(x) 360 quickly 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

Reveal(x) 360 deploys without agents in public cloud and on-premises environments. For AWS environments, you can deploy on-demand sensors directly from the Reveal(x) 360 management pane.

Managed Services

Reveal(x) Advisor offers threat-free network assurance for the hybrid enterprise. ExtraHop experts will augment lean security teams by identifying vulnerabilities, detecting incidents, and stopping adversaries.

ExtraHop

Reveal(x) 360

CLOUD THREAT DEFENSE

Multi-Layered Security Against Advanced Threats for AWS

Reveal(x) 360 cloud threat defense for AWS enables security teams to stop threats from the inside with complete visibility, post-compromise detections, proactive threat hunting, and deep forensic investigation.

Reveal(x) 360 deploys without adding friction to DevOps processes, freeing security teams to defend critical workloads and applications without slowing down innovation, digital transformation, or business. With Reveal(x) 360, you can visualize your entire attack surface in real time from a single management pane.

By combining the breadth of VPC Flow Logs with the depth of network packets, Reveal(x) 360 provides a multi-layered approach to defending against advanced threats like ransomware, software supply chain attacks, and more. Security teams can use flow logs for broad visibility and packets to conduct deep forensic investigations.

ExtraHop analyzes all layers of network telemetry with advanced AI to create accurate detections, high-fidelity alerts with context, and a threat heatmap. Armed with this advanced threat visibility, security teams can zero in on, investigate, and remediate hotspots of malicious activity in real time.

aws PARTNER Security Software Competency

Reveal(x) 360 offers several subscriptions for multi-layered cloud threat defense in AWS. Every Reveal(x) 360 subscription leverages ExtraHop's cloud-hosted AI service and record store.

To view Reveal(x) 360 pricing, visit our **AWS Marketplace listing**.

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

RANSOMWARE MITIGATION

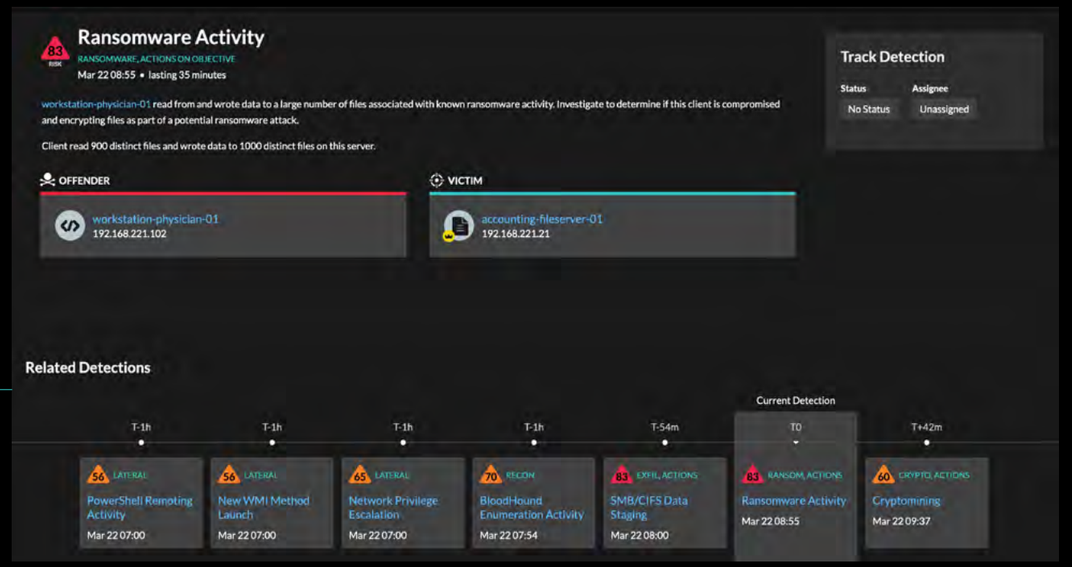
Ransomware is becoming more sophisticated, and traditional prevention tactics can't keep up with the latest advances. Ransomware gangs now take advantage of east-west visibility gaps and encrypted traffic to stay hidden just long enough to reach the endgame of their attacks and expand their blast radius. Reveal(x) 360 provides the visibility and investigation capabilities needed to detect and mitigate ransomware with speed and confidence.

- Gain complete east-west visibility to light up the darkspace where ransomware hides after it slips past perimeter defenses.
- Detect the subtle post-compromise activities used in the midgame of every successful attack with AI-powered behavioral analysis.
- Quickly investigate high-fidelity detections to take a targeted approach to response that only quarantines compromised devices or workloads.

How do you prevent ransomware from compromising perimeter defenses?

What are your current ransomware mitigation strategies?

How do you detect post-compromise activities in the ransomware kill chain?



Reveal(x) 360 detects ransomware in every stage of the attack killchain and creates high-fidelity alerts.

ExtraHop

MONITOR SENSITIVE DATA

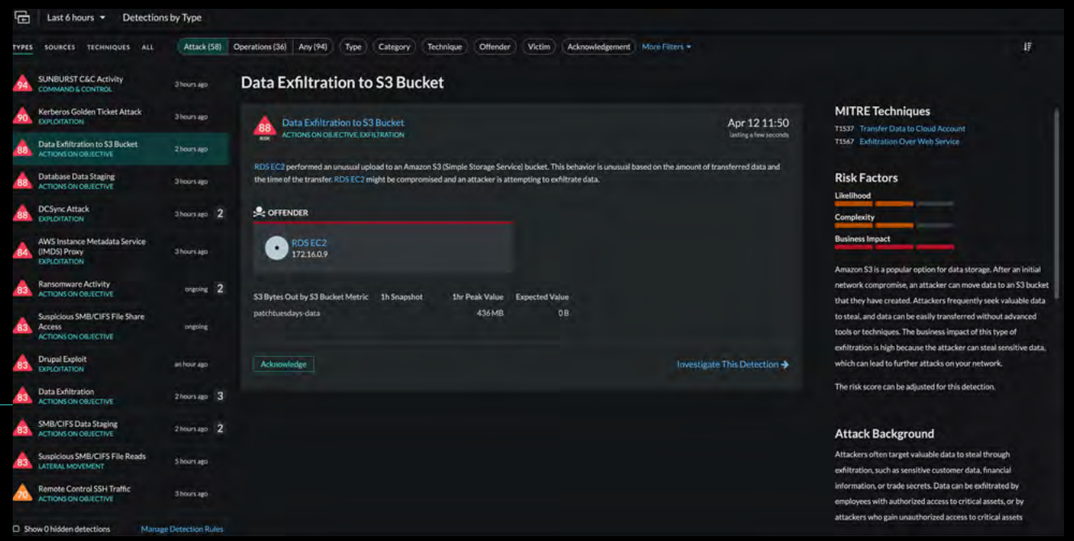
Attackers can't steal data without moving it across the network. But data protection products, zero trust architecture, and logging with manual post-hoc analysis create large blind spots, slow down investigation and response, and create significant implementation and administration burdens. Reveal(x) 360 data monitoring 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

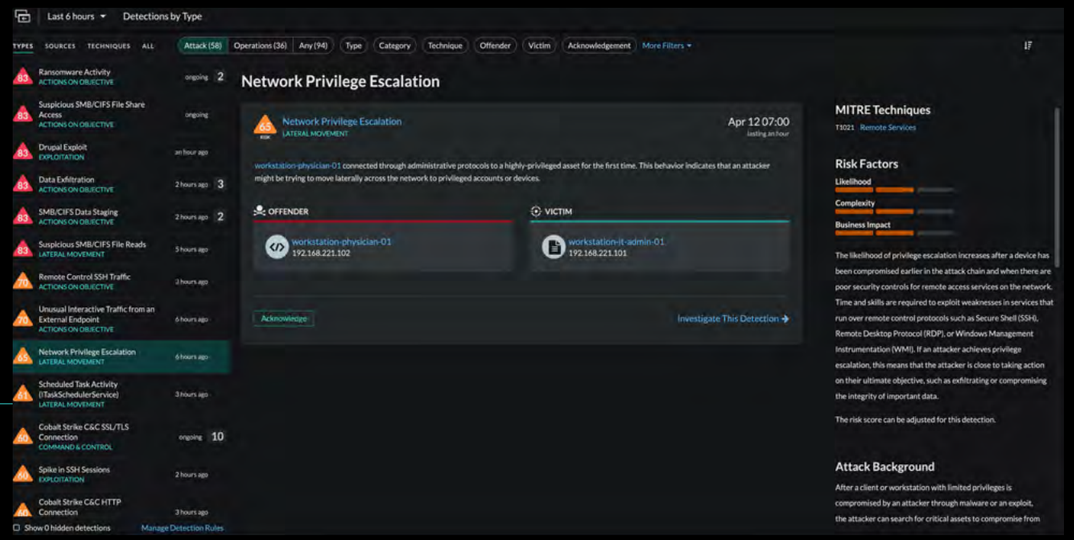
Once attackers compromise a workstation and steal credentials, it's extremely difficult to detect them. The limitations of perimeter-focused tools, logging, and endpoint tools create significant blind spots in the east-west traffic corridor where attackers pivot to critical assets and expand their foothold. Reveal(x) 360 detects post-compromise activities to help 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

COMPREHENSIVE INVENTORY OF ALL DEVICES

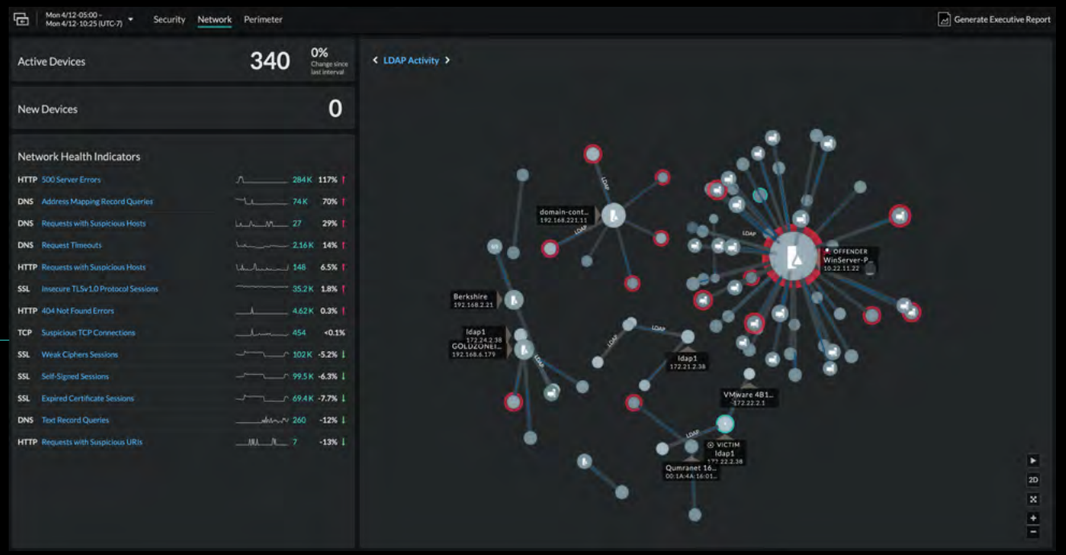
Unmanaged, uninstrumentable, and rogue devices create significant security risk. Reveal(x) 360 monitors all network-connected assets, including IoT and employee-owned devices, to enhance your security hygiene. Behavior-driven device discovery helps you understand what each device is and how it's interacting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

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

MONITOR CRITICAL CLOUD WORKLOADS

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 critical workloads no matter where they live.

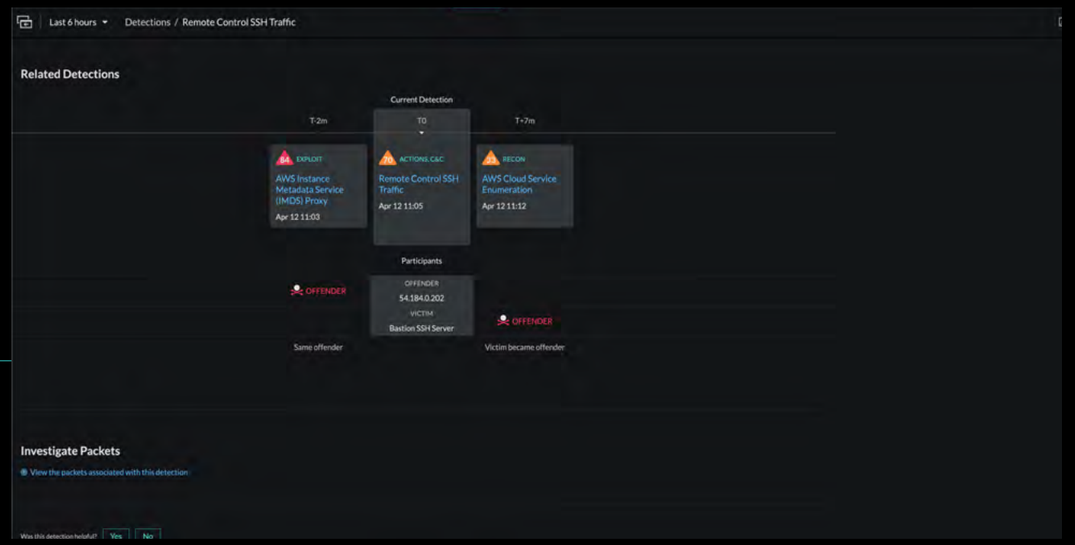
- View cloud workload activity and identify anomalous behavior automatically.
- Trace data transfers inside the VPC and to external endpoints, APIs, and cloud services.
- Automatically provides the context of data flows: which users are sending and receiving, where data is going, and what the data contains.

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.



ExtraHop

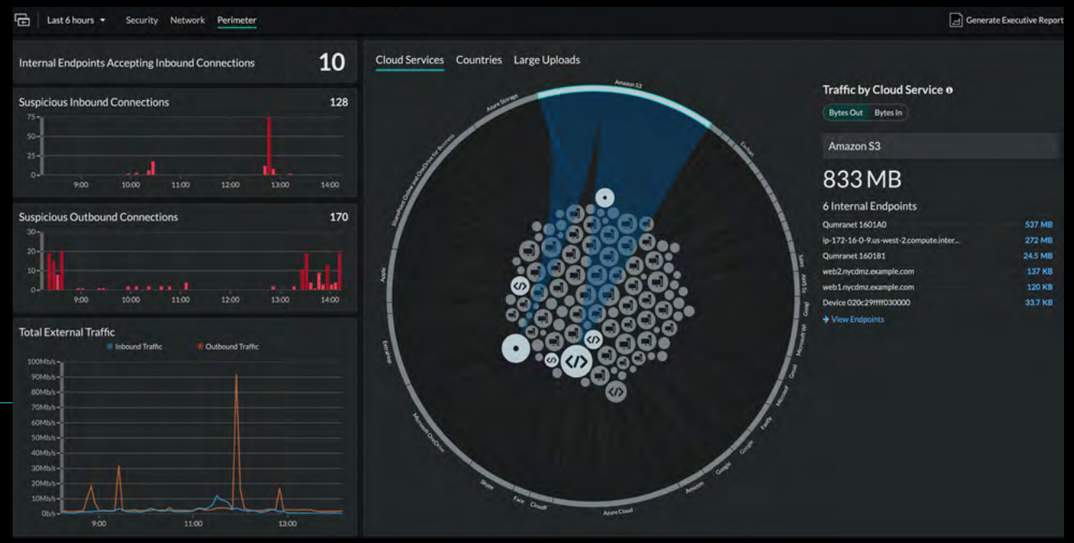
DETECT SOFTWARE SUPPLY CHAIN ATTACKS

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, helps you manage the attack surface, and defend against software 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.

ExtraHop

CONTAINER SECURITY

Securing containers requires the ability to detect and respond to advanced threats as they occur. But maintaining visibility and understanding what constitutes malicious behavior can be difficult in ephemeral environments. Reveal(x) 360 provides cloud-scale visibility, advanced threat detection, and deep investigation across containers and services. With versatile deployment options, you get the most coverage with the smallest tooling footprint.

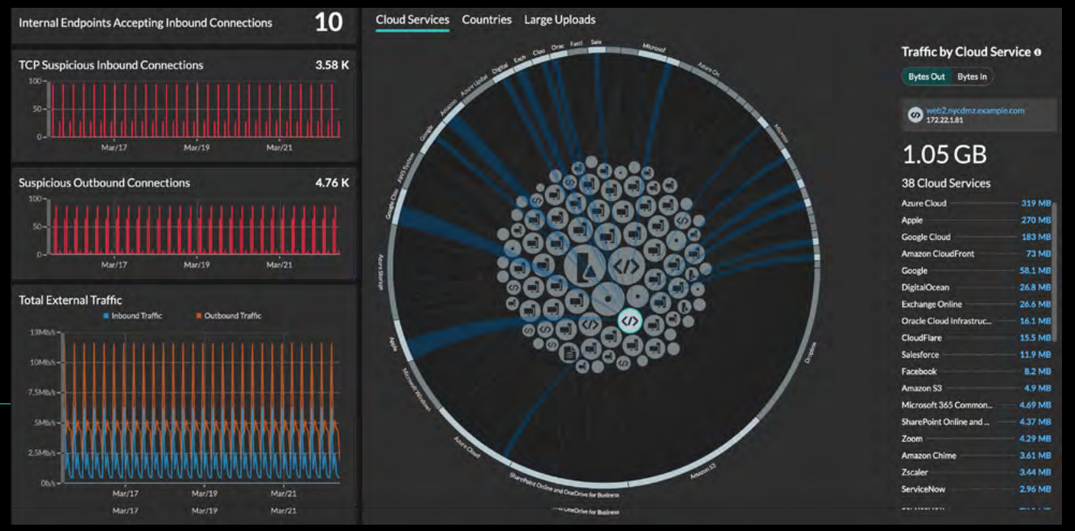
- Discover microservices, pods, and containers as soon as they communicate and map dependencies, including service calls.
- Analyze network traffic with advanced AI to detect anomalous or malicious behavior, plus create activity maps with timestamps.
- Go from detection to forensic evidence in clicks, leveraging continuous PCAP, a cloud-hosted record store, and intuitive workflows.

How do you maintain visibility in ephemeral container environments?

How do you know if containers have been compromised by an attack?

How quickly can you detect, investigate, and respond to threats to containers?

Discover new containers, map dependencies, and monitor and analyze traffic.



ExtraHop

FORENSIC INVESTIGATION

The ability to drill down to forensic evidence quickly is a key component of meeting disclosure rules and slashing mean time to respond. Reveal(x) 360 speeds forensic investigation by automatically curating cloud asset information, metadata, and forensic evidence in a single tool.

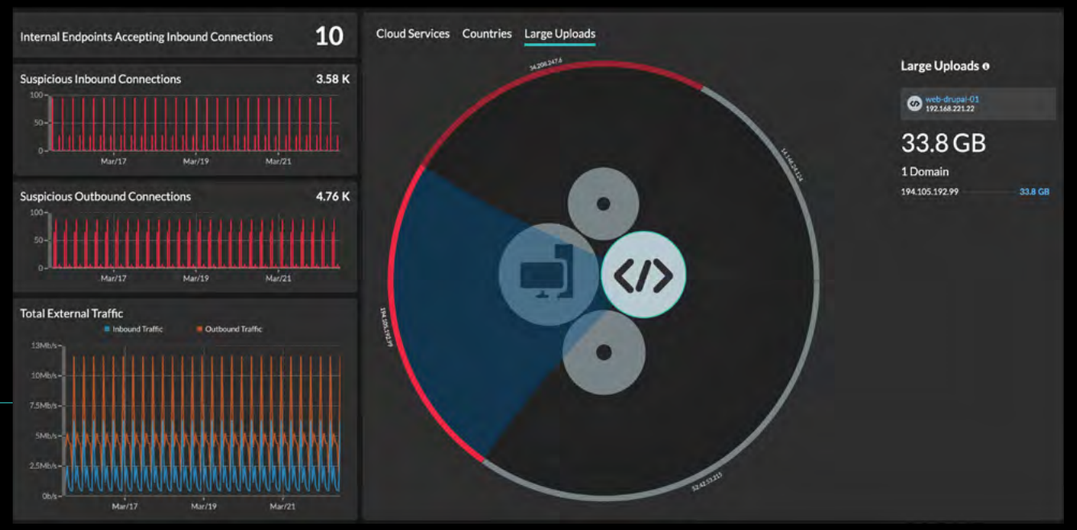
- Accurately determine the scope of incidents for implementing appropriate response, internal assessment, and regulatory reporting.
- Correlate cloud asset information, historical metadata, and forensic details for the context needed to surface real threats in the cloud.
- Intuitive investigation workflows to go from detection to context and forensic evidence in clicks.

Are cloud-native tools causing alert fatigue and increasing MTTR?

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

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 speeds up time to detect and respond.

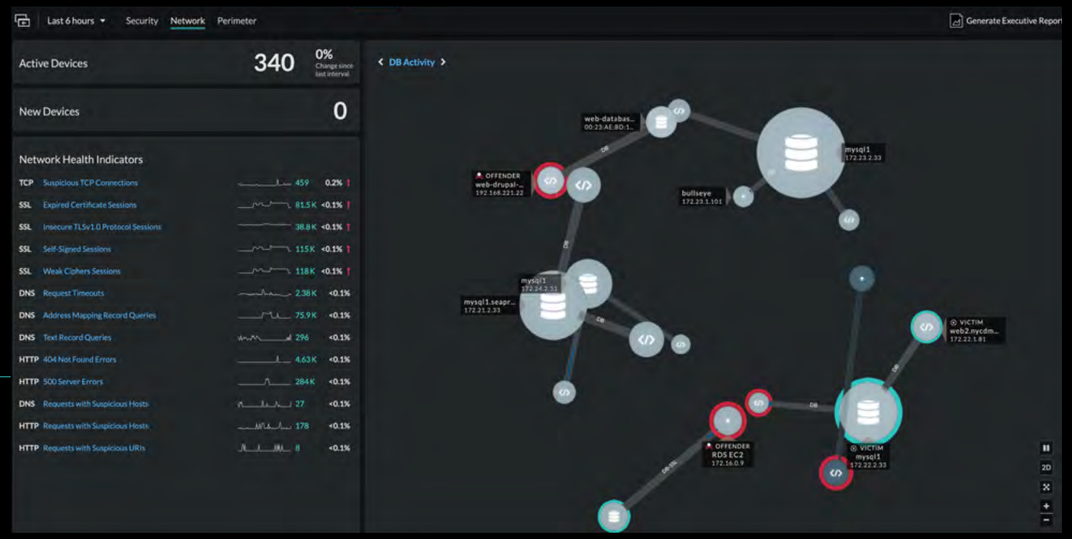
- Automated device and application discovery, classification, and mapping to understand inventory and relationships.
- Correlate activity along the application delivery chain to understand in context exactly what's happening.
- Intuitive workflow speeds troubleshooting from issue to root cause in 3 clicks.

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

SUPPORT HYBRID WORKFORCES

Remote workforces need reliable remote access, and VPN and connection issues or sluggish application performance can prevent them from doing their jobs. Reveal(x) 360 provides a real-time view of your entire hybrid environment to detect availability issues before they can impact productivity. With thousands of TCP metrics and customizable dashboards, you can tune remote access traffic patterns, troubleshoot network slowdowns, and support hybrid workforces.

- 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.

How do you measure and monitor remote access traffic?

How do you optimize traffic for remote workers?

How do you detect remote login issues before they become a problem?

Understand real-time utilization and dependencies.

ExtraHop

CLOUD MIGRATION

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 quickly, confidently, and securely migrate to the cloud.

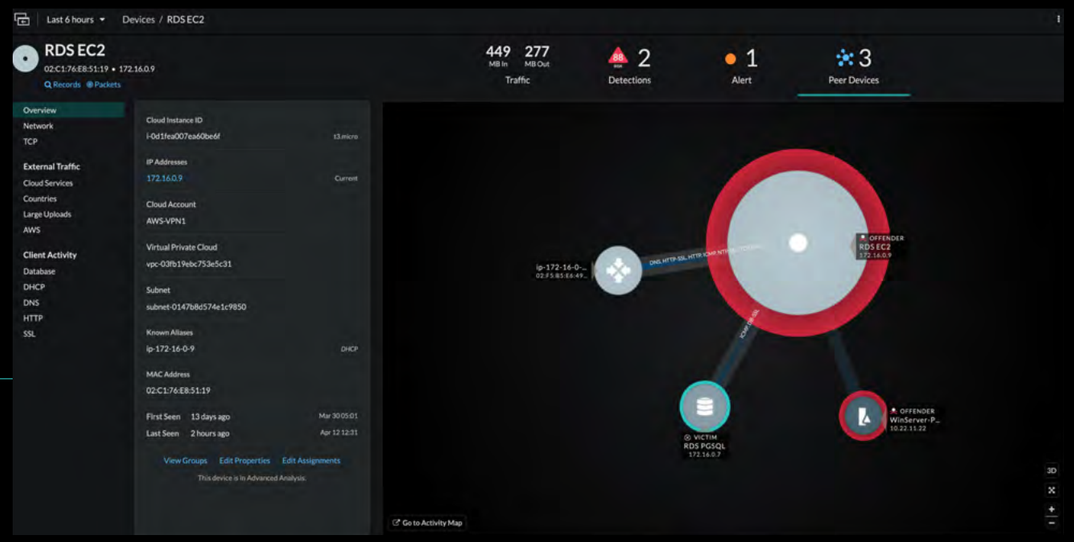
- Discover all application traffic and map and understand dependencies.
- Measure performance before, during, and after migration.
- Agentless operational visibility across on-premises, cloud, and hybrid environments from a unified platform.

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

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