

ExtraHop Reveal(x)

for Midsize Enterprises

Reveal(x) now brings threat detection and response and complete visibility, including application analytics, to midsize enterprises in a single platform that's simple to deploy and manage, and provides instant value out of the box, with optional on-demand security expert services to further accelerate response and increase security maturity.



COMPLETE VISIBILITY

Reveal(x) provides visibility across the entire enterprise, covering critical security needs and operational use cases in a single, simple platform across on-premises, cloud, and hybrid environments, so cross-functional teams can consolidate tools and maximize efficiency.

REAL-TIME DETECTION

Reveal(x) detects the most common, catastrophic threats in real-time, stopping ransomware in its tracks, and catching insider threats and low-and-slow attackers before damage is done, with rich context on every detection so any analyst can respond with confidence.

GUIDED INVESTIGATION

Reveal(x) lets every analyst be an army with guided investigation and rich context around every detection, accelerating response and resolution, and helping analysts learn quickly and add value rapidly in the most relevant context: your actual environment.

RISE ABOVE RANSOMWARE & MORE.

Reveal(x) detects the most common and increasingly catastrophic threats, such as ransomware, right out of the box using a combination of machine learning and rules-based detections to provide confident detections, no false positives, and rapid investigation and response options across the entire environment that any analyst can understand.

Potential Ransomware Activity Detected

This client read from and wrote data to an unusually large number of files over the SMB/CIFS protocol. Investigate to determine if this client is compromised and potentially encrypting data as part of a ransomware attack.

This device read approximately 300 files and wrote 400 files from the following CIFS server:

- 192.168.0.25

IN PROGRESS

REC-1483
wibur

OFFENDER
Device: 192.168.0.33
192.168.0.33

VICTIM
Device: 192.168.0.25
192.168.0.25

Related Detections

Timeline: T-14d TO TO

- Suspicious SMB/CIFS Client File Share Access (Jan 27 04:00, 56 Detections)
- Suspicious SMB/CIFS Client File Share Access (Today 04:00)
- Potential Ransomware Activity Detected (Today 04:00)

Participants

OFFENDER: Device: 192.168.0.33
VICTIM: Device: 192.168.0.25

Same offender Same victim | Victim became offender

RISK FACTORS

Likelihood [Progress bar]

Complexity [Progress bar]

Business Impact [Progress bar]

Ransomware attacks are increasingly common because they provide attackers with a high return on their investment. Different strains of ransomware malware are easily acquired or created in multiple programming languages. The impact of ransomware on a business can be devastating, especially if sensitive or business critical data is unavailable for an extended period of time, or if a high ransom is paid.

ATTACK BACKGROUND

Ransomware is a type of malware that often encrypts files on a victim machine and makes those files inaccessible until the victim pays a ransom for the decryption key. Ransomware attacks can originate from phishing emails, outdated network services, or large scale attack campaigns. After the ransomware encryption begins, the encryption process can quickly spread throughout the network and across file shares on critical assets.

MITIGATION OPTIONS

- Maintain off-site and up-to-date backup files that can restore critical systems
- Periodically test backups to make sure they are working
- Disable external services that are exposed to the Internet, especially services that run over file sharing or remote access protocols
- Reduce the spread of ransomware by implementing microsegmentation, which partitions network traffic into secure zones, based on the zero trust security model
- Update operating system software to the latest version to reduce the number of vulnerabilities that can be exploited
- Enforce a strong password policy to reduce the possibility of attacks that are linked to ransomware

REFERENCE

- MITRE ATT&CK: T1486: Data Encrypted for Impact
- MITRE ATT&CK: T1485: Data Destruction

Was this detection helpful? YES NO

Investigate Instantly
Get to root-cause in just a click or two.

See The Whole Story
Related detections show the progress of an attack from beginning to end.

Understand what the detection means, and how to mitigate future instances.

Cross-reference popular security frameworks.

DETECT THREATS

Breach Detection & Response
Detect all stages of the attack lifecycle and expedite forensics

Insider Threat Detection
Detect, contain, and document risky and malicious behavior

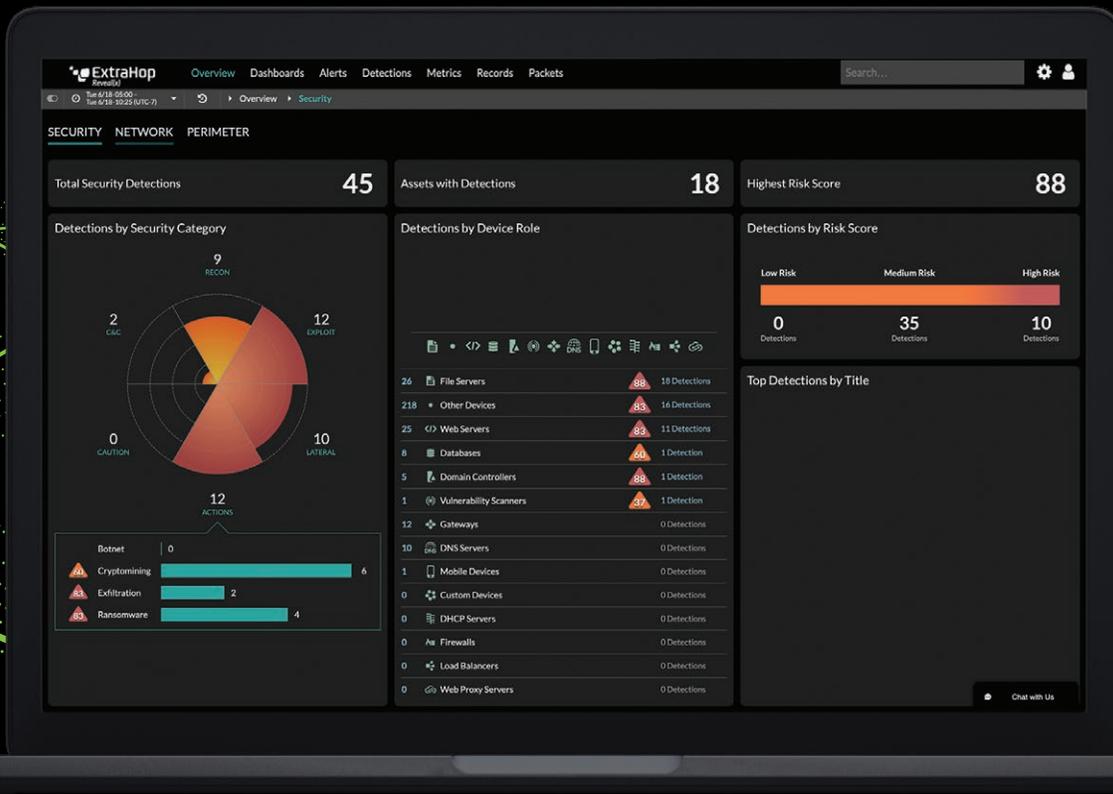
Ransomware Defense
Contain and minimize active attacks, recover data

IMPROVE POSTURE

SOC Productivity
Prioritized detection, reduced false positives

Red Team /Audit Findings
Find or validate concerns and vulnerabilities

Reduce Attack Surface
Improve hygiene, audit encryption, and decommission risky assets



EXTRAHOP REVEAL(X) BENEFITS FOR MIDSIZE ENTERPRISES

Get Value Instantly

Reveal(x) is fast and simple to deploy, and starts detecting threats right out of the box using advanced machine learning, threat intelligence, and precise, built-in rules.

Understand Threats Fast

Reveal(x) includes guided investigations, mitigation steps, remediation suggestions, and MITRE, CIS, and NIST links for rich context and rapid response to every detection.

Detect What Matters

Reveal(x) detects ransomware, cryptomining, and other costly, fast-acting threats immediately, as well as low-and-slow advanced threats that lurk for months.

Get On-Demand Expertise

ExtraHop Spotlight Services provide targeted on-demand expert security guidance for investigating and responding to specific detections in your environment.

Unify Security and Application Visibility

Reveal(x) deeply analyzes application traffic so you can detect threats and troubleshoot application performance in one place.

Upskill Your Analysts

With Reveal(x), every analyst is an army. Rich context, powerful workflows, and trusted detections mean even Tier 1 analysts can validate detections and respond with confidence.



ExtraHop Spotlight Services

ExtraHop Spotlight Services give our customers on-demand access to ExtraHop security experts to provide targeted guidance, education, and recommendations for how analysts can respond to specific detections in their own environment. This optional service can help security analysts respond more quickly, and level up their own knowledge and skills rapidly to provide more value, faster.



ExtraHop Professional Services

ExtraHop Professional Services provide expert guidance for our customers to deploy Reveal(x) and get the exact outcomes they're seeking as quickly and effectively as possible, focusing on the pillars of Operationalization, Risk Optimization, SOC Optimization, NPMD Optimization, and ultimately Business Transformation.

OUR CUSTOMERS RISE ABOVE THE NOISE.

95%

IMPROVEMENT
IN TIME
TO DETECT

77%

IMPROVEMENT
IN TIME TO
RESOLVE

59%

REDUCTION
IN STAFF TO
RESOLVE

25%

MORE SECURITY
THREATS
SUCCESSFULLY
IDENTIFIED



Fast, amazingly thorough... Reveal(x) is a product with which many security operations center (SOC) teams could hit the ground running.

DAVE SHACKLEFORD, SANS INSTITUTE INSTRUCTOR



ABOUT EXTRAHOP NETWORKS

ExtraHop provides cloud-native network detection and response for the hybrid enterprise. Our breakthrough approach uses cloud-scale machine learning to provide complete visibility, real-time detection, and intelligent response. We help the world's leading enterprises rise above the noise of alerts, organizational silos, and runaway technology by detecting threats up to 95 percent faster and accelerating response by up to 60 percent. With ExtraHop, you have the perspective you need to protect and scale your business.



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