ExtraHop Reveal(x) 360
Frictionless cloud security for healthcare

Why Reveal(x) 360?

• Helps security teams decrease risk and reduce potential damage from ransomware attacks.
• Deploys without agents for greater scalability and elasticity while removing friction and complexity.
• Unifies visibility, detection, and response in a single management pane.
• Improves visibility in AWS environments, even if traffic is encrypted.
• Provides real-time advanced threat detection, dynamically updated as infrastructures and threats evolve.
• Enhances existing AWS-native tools and offers integrations with third-party vendors like CrowdStrike.

Product overview

Healthcare cybersecurity requires defending a complex web of applications and sensitive data spread across cloud, hybrid, and device deployments. With Reveal(x) 360 network detection and response (NDR), you gain unified visibility, detection, and response capabilities to stop threats faster and manage your attack surface with confidence.

Product features

Advanced threat detection
Reclaim the upper hand against cyber attackers:
• Cloud-scale machine learning (ML) analyzes network data to identify suspicious and malicious behaviors in real time.
• Identifies known and unknown threats while providing coverage of attacker tactics, techniques, and procedures.

Streamlined investigation and threat hunting
Intuitive workflows speed investigation and significantly reduce time to resolution:
• Cloud-hosted record store provides 90-day lookback for deep investigation.
• Enables fast, thorough investigation of post-compromise activities like recon and lateral movement in real time.

Intelligent response capabilities
Stop ransomware and supply chain attacks:
• Creates high-fidelity alerts with context as well as a related detections timeline and more.
• Empowers analysts to quickly and accurately determine the scope of incidents and workloads involved to implement appropriate responses.
How it works

Every asset—including applications, IoT, and medical devices—uses the network to communicate, making NDR essential for securing patient data and clinical and billings systems.

To start securing your cloud and hybrid environments with Reveal(x) 360, simply deploy ExtraHop sensors in any environment you want to defend. Reveal(x) 360 sensors integrate with Amazon VPC Traffic Mirroring to ingest copies of network traffic packets, which are decrypted to extract records and de-identified metadata. That information is securely sent to Reveal(x) 360 for ML-powered behavioral analysis, real-time threat detection, and intelligent response. This process includes investigation or taking automated action on compromised workloads, domains, and IP addresses.

Through the Reveal(x) 360 record store with 90-day lookback, you can conduct index record search, query, and drill-down investigation across your hybrid environment for situational intelligence. A cloud-hosted control plane—accessible via the secure web-based Reveal(x) 360 user interface—provides a unified view of the environments where the sensors are deployed.

ExtraHop has obtained HIPAA compliance certification for all online services. The HIPAA certification covers administrative, technical, and physical safeguards as well as organizational, documentation, and breach notification requirements.
Differentiators

- A cloud-based record store with 90-day lookback provides fully hosted and managed search for streamlined incident investigation
- Continuous packet capture (PCAP) is available for forensic investigation
- Cloud-hosted services securely accessible from anywhere via a single management pane unify visibility, ML-powered threat detection, and response across AWS, hybrid, and distributed environments

Additional Resources

- Reveal(x) 360 eBook
- Solution Brief
- Online Demo

Data Points

45% Increase in healthcare ransomware attacks

50% Faster Threat Detection

84% Faster Threat Resolution

99% Faster Troubleshooting

Solution available in AWS Marketplace