ExtraHop

DATASHEET

Defend Your Containerized Environments with Reveal(x) 360

CONTAINER SECURITY WITH REVEAL(X) 360

Securing containers requires continuous monitoring, AI-powered analysis, and the ability to detect and respond to advanced threats as they occur in highly dynamic environments. With ExtraHop Reveal(x) 360, you can unify security across containers and services in a single management pane, securely accessible from anywhere. Defend your Amazon ECS, Amazon EKS, Google Kubernetes Engine, Azure AKS, Docker, OpenShift, and Nomad services, plus many more, with SaaS-based Reveal(x) 360.

VERSATILITY

Reveal(x) 360 provides cloud-scale visibility, threat detection, and response at the container and service levels in a single, SaaS-based security solution. Here's how it works:

- Reveal(x) 360 analyzes microservices using a virtual tap deployed in the container or as a sidecar.
- For analysis at the service level, Reveal(x) 360 leverages dynamic service-layer objects automatically updated via integration with your CI/CD pipeline to reduce management burden.

With versatile deployment options and security at the container and service levels, Reveal(x) 360 enhances your security coverage in containerized environments.

VISIBILITY

You can't defend what you don't see. With continuous auto-discovery, Reveal(x) 360:

- Discovers microservices and their pods and containers as soon as they start communicating across the network.
- Maps persistent and ephemeral dependencies based on those communications, including service calls.

This always-up-to-date inventory enables you to observe, understand, and secure containerized environments.

DETECTION & RESPONSE

The longer an attacker spends in your containerized environment, the more damage they can do. To find threats in real time, Reveal(x) 360:

- Combines rules with behavioral analysis to provide the full spectrum of detections.
- Analyzes microservices traffic across the network with cloud-scale machine learning to identify anomalous and malicious activities.
- Understands the past behavior in ephemeral environments via service-layer abstraction.
- Provides activity maps with timestamps to help you understand ephemeral environments at any point in time.

With continuous PCAP, a cloud-hosted record store, and intuitive workflows, you can go from detection to forensic evidence in clicks for faster response.

50% FASTER THREAT DETECTION

84% FASTER THREAT RESOLUTION

99% FASTER TROUBLE-SHOOTING

ABOUT EXTRAHOP NETWORKS

ExtraHop is on a mission to stop advanced threats with security that can't be undermined, outsmarted, or compromised. Our dynamic cyber defense platform, Reveal(x) 360, helps organizations detect and respond to advanced threats––before they compromise your business. We apply cloud-scale AI to petabytes of traffic per day, performing line-rate decryption and behavioral analysis across all infrastructure, workloads, and data-in-flight. With complete visibility from ExtraHop, organizations can detect malicious behavior, hunt advanced threats, and forensically investigate incidents with confidence. When you don't have to choose between protecting your business and moving it forward, that's security uncompromised.

Request a Free Trial **extrahop.com/request-free-trial**
Take the Demo **extrahop.com/demo/cloud**

ExtraHop

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