ExtraHop

Reveal(x)

NG-IDS USE CASES

Get More From Your IDS Budget with NG-IDS

Industry-wide, IDS programs continue to be the go-to technology for network security compliance check-off, despite disappointing operational results. However, with NGFWs absorbing many IDS perimeter functions, there is an opportunity to shift detection budgets deeper into the network with NG-IDS. Building on IDS, ExtraHop Reveal(x), an NG-IDS technology, also spots east-west threats, stops post-compromise intruders, and closes compliance gaps due to cloud initiatives and encryption blind spots.

Pushing IDS deeper in the network will just add more unmanageable alerts and keep you oblivious to intrusions crossing perimeter defenses. Be the hunter, not the hunted, and optimize your IDS budget with Reveal(x), a cloud-scale, machine-learning-powered NG-IDS that will streamline investigation and response workflows.

Detection Across the Kill Chain

IDS dependence on exact signature matching forces defenders to catch attacks right at the instant of intrusion. Errors are inevitable from brittle bimodal signatures that lack context. Adversaries are determined, making perfect defense challenging to achieve.

Reveal(x) applies in-depth principles of behavioral analysis and pattern matching across the whole kill chain. Like IDS, Reveal(x) includes high-risk vulnerability exploit detection, but then adds layers of post-compromise detectors that give you the opportunity to catch attackers at every stage of the intrusion cycle. Reveal(x) turns the tables, forcing attackers to walk a tightrope, giving you the edge to stop the threats before real damage occurs.

Reveal(x), a cloud-native next-gen IDS technology, provides the scale, speed, and visibility required by IT security teams to rise above the noise

BREACH DETECTION & RESPONSE

Detect threats and augment or automate response actions

POST-COMPROMISE KILL CHAIN DETECTION

Stop advanced intruders who've crossed perimeter defenses

CLOUD-SCALE MACHINE LEARNING

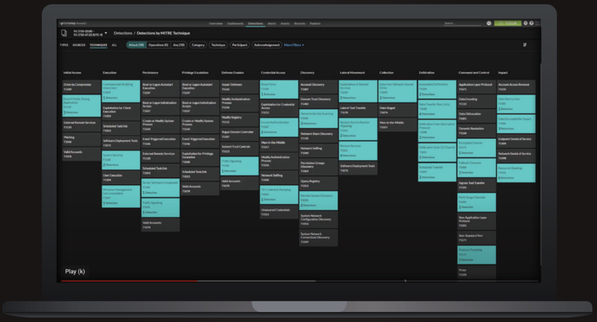
Detects, prioritizes, and contextualizes threats against your critical assets

HYBRID SECURITY

Unified cloud-native and on-premises threat detection and response

PERFECT FORWARD SECRECY DECRYPTION

Decrypts SSL/TLS 1.3 with PFS passively and in real time



Close Compliance Gaps

Regulatory compliance is the primary motivator for many organizations maintaining and expanding IDS programs. Yet, gaps from digital transformation, cloud initiatives, and hidden attacks across encrypted channels increase risk exposure not easily plugged with IDS.

HYBRID CLOUD

Reveal(x) delivers unified security across on-premises and cloud environments, 360-degree visibility, and situational intelligence frictionless to the DevOps innovation pipeline.

aws

Google Cloud

Azure

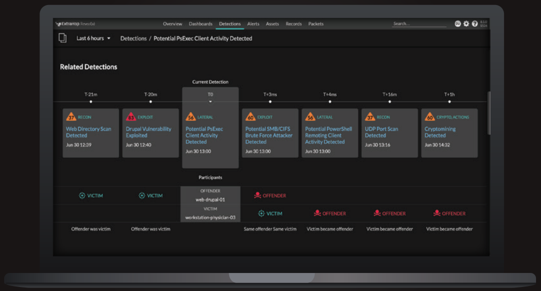
vmware

ENCRYPTION VISIBILITY

Reveal(x) performs all SSL/TLS decryption 'on box,' providing you with deep, meaningful network traffic analysis without any risk to sensitive data or data regulated by various industry standards such as HIPAA, PCI, GDPR, and others.

Save Money with One Tool to Detect, Investigate, and Respond

Many IT admins refer to IDS as an alert canon. Unfortunately, IDS also stops at alerts, leaving your time-strapped analysts to investigate root-cause with other investigation tools and, in some cases, access yet another PCAP repository tool for forensic evidence.



Detections / Potential PsExec Client Activity Detected

Related Detections

Current Detection

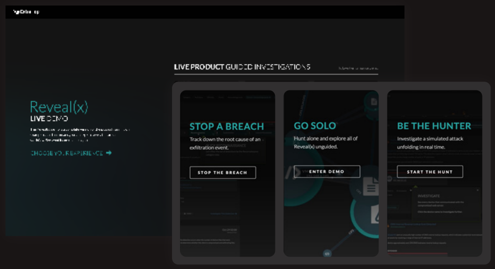
T-21m	T-20m	T0	T+3ms	T+4ms	T+16m	T+1h
37 RECON Web Directory Scan Detected Jun 30 12:39	83 EXPLOIT Drupal Vulnerability Exploited Jun 30 12:40	56 LATERAL Potential PsExec Client Activity Detected Jun 30 13:00	60 EXPLOIT Potential SMB/CIFS Brute Force Attacker Detected Jun 30 13:00	56 LATERAL Potential PowerShell Remoting Client Activity Detected Jun 30 13:00	37 RECON UDP Port Scan Detected Jun 30 13:16	60 CRYPTO, ACTIONS Cryptomining Detected Jun 30 14:32
VICTIM	VICTIM	Participants OFFENDER web-drupal-01	OFFENDER			
		VICTIM workstation-physician-03	VICTIM	OFFENDER	OFFENDER	OFFENDER
Offender was victim	Offender was victim		Same offender Same victim	Victim became offender	Victim became offender	Victim became offender

Reveal(x) transforms packets into structured wire data at line-rate, up to 100Gbps. The metadata, classified and indexed, is analyzed along many dimensions, yielding high-fidelity insights about threat activities and unusual, potentially malicious behavior. Reveal(x) enriches the metadata and insights with asset intelligence, threat intelligence, and risk context.

Analysts can navigate rapidly through detection, investigation, and response using optimized workflows and on-demand, typically 90 days of metadata, or even raw packet storage from a single tool.

Explore the Interactive Demo

READY TO TRY REVEAL(X) FOR YOURSELF?



Track down the root cause of an exfiltration event.

Hunt alone and explore all of Reveal(x) unguided.

Investigate a simulated attack unfolding in real time.

ABOUT EXTRAHOP NETWORKS

ExtraHop provides cloud-native network detection and response for the hybrid enterprise. Whether you're investigating threats, ensuring the availability of critical applications, or securing your cloud investment, ExtraHop's breakthrough approach helps you rise above the noise so you can protect and accelerate your business. Learn more at www.extrahop.com.

info@extrahop.com
www.extrahop.com