ExtraHop

Forensics Readiness Speeds Root Cause Analysis, Impact Scoping, & Recovery

ExtraHop Reveal(x) 360 gives incident responders visibility across hybrid environments that attackers can't evade. Your network is forensics-ready with 90 days of traffic record look-back, a unified PCAP repository, and a streamlined investigation workflow to eradicate intruders faster.

CHALLENGES

When it comes to incident response and network forensics, time is money. The weeks spent by your most skilled security analysts, the hours ticking by on expensive third party responder retainer contracts, and the downtime and cost attributed to recovery from data breaches and ransomware add up. Unfortunately, time isn't on your side: If you realize you are missing definitive network data mid-response, you may never know what movements intruders made toward your valuables until it's too late.

SOLUTION

Accurate, actionable data is the only accelerant to recovery and closing security gaps quickly. With Reveal(x) 360, incident responders can jump into action with context-enriched alert timelines, 90 days of unalterable, continuous traffic-record lookback, and PCAP-evidence repositories to eradicate intruders and recover faster. Reveal(x) 360, delivered as a cloud-scale SaaS solution, simplifies forensics readiness for your cloud and on-premises programs.

KEY BENEFITS

FIND ROOT CAUSE FASTER

Quickly look back across 90-days of continuous traffic records to identify the entry points, C2, and every lateral action taken from the origins of the attack.

SCOPE IMPACTED SYSTEMS & DATA CONFIDENTLY

Traffic headers tell responders which services, databases, and files systems are compromised, then payload inspection answers what they did and the severity of harm done.

MAXIMIZE SECURITY ANALYST CAPABILITIES

Reveal(x) makes incident response accessible to all analysts with rich transaction data available in intuitive and query-based starting points for their hunt.

MINIMIZE 3RD PARTY IR RETENTION CONTRACTS

With Reveal(x) 360, contract responders jump into context-enriched alerts, 90-days of traffic records, and PCAPs to close cases faster, without disrupting operations.

ATTACKERS CAN'T EVADE NETWORK EVIDENCE

Reveal(x) 360 includes 90-days of unalterable traffic records and a modularly scalable PCAP repository, up to 7.6 Petabytes, for use in regulatory and legal recourse.

HOW IT WORKS

Responders jump into action with contextualized alerts with attacker timeline

90-days of unalterable continuous traffic records to pinpoint root cause and threat hunting

Scope all impacted systems and compromised data

Long term packet evidence retention

Use Cases

ESTABLISH CYBERSECURITY RESILIENCE

Network forensics readiness builds resilience against the inevitable attack. Responders make quality decisions quicker to eradicate intruders faster using ground-truth traffic data.

STOP INTRUDERS BEFORE THEY DO REAL DAMAGE

Today's attackers will land on anything accessible, then pivot toward your valuables. The network is the most trusted data source to stop intruders as they move east-west through your infrastructure.

THREAT HUNTING

Reveal(x) 360 makes hunting accessible to analysts of all skill levels. Analysts can form and test hypotheses faster with automatically surfaced hunt starting points and efficient investigation workflows.

HYBRID CLOUD INCIDENT RESPONSE

Reveal(x) 360 provides responders cloud-native network forensic evidence at SaaS scale. Whether your digital transformation is on AWS, Google Cloud, or Azure, Reveal(x) 360 has a solution.

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 uses cloud-scale AI to help enterprises detect and respond to advanced threats—before they can compromise your business. When you don't have to choose betweenprotecting your business and moving it forward, that's security, uncompromised.

ExtraHop

info@extrahop.com
www.extrahop.com