ExtraHop Introduces New Layer of Cloud Threat Defense to Identify and Isolate Advanced Cyberattacks

Submitted by: Positive Marketing
Wednesday, 23 March 2022

Reveal(x) 360 for AWS Now Applies Advanced AI to All Network Telemetry Sources, Providing Continuous Visibility of Malicious Activity Without Requiring Dev Resources

SEATTLE – March 23, 2022 – ExtraHop (https://www.extrahop.com/), the leader in cloud-native network detection and response, today announced that it has extended the power of Reveal(x) 360 to provide frictionless threat visibility for Amazon Web Services (AWS). ExtraHop Reveal(x) 360 now applies advanced AI to layers of network telemetry to create a “threat heatmap” purpose-built to detect and stop advanced attacks like double-extortion ransomware and software supply chain attacks. Armed with this advanced threat visibility, security teams can zero in on, investigate, and remediate hotspots of malicious activity without requiring developer time or resources—or slowing down business innovation.

Cloud security teams are outnumbered and the traditional approach of prevent-and-protect can’t keep pace with modern advanced attack techniques. According to the IBM-Ponemon Institute 2021 Cost of a Data Breach report (https://www.ibm.com/account/reg/us-en/signup?formid=urx-50915), the cost of public cloud breaches far exceeds that of breaches in hybrid environments, costing, on average, $1.19 million more per incident. Organizations with high levels of cloud migration in general experienced costlier breaches, with the average cost of a breach for cloud-mature organizations hovering at just over $5 million, compared to $3.46 million for organizations with low levels of cloud adoption. As developers deploy assets at a breakneck pace and adversaries continue to evolve their attacks on mission-critical applications and workloads, enterprises need a low friction, high fidelity approach to defend against advanced post-compromise activities.

“We live in an era of large attack surfaces and frequent business compromise. Organizations need to assume that attackers are actively operating inside their cloud environment, moving laterally and evading traditional security controls,” said Jesse Rothstein, co-founder and CTO, ExtraHop. “ExtraHop Reveal(x) 360 was purpose-built to covertly and reliably detect malicious behavior. With the introduction of a new subscription tier for AWS, we’re expanding our high-fidelity detection, threat hunting, and investigation capabilities in cloud environments without adding friction for dev teams or the organizations that need to innovate with speed and agility.”

ExtraHop has been at the forefront of stopping modern cloud attacks through the use of network telemetry. By natively integrating with Amazon VPC Traffic Mirroring, the company pioneered a SaaS offering that delivered cloud threat detection without agents. This new offering expands this power to include VPC Flow Logs and additional protocol analysis, providing both depth and breadth of visibility for threats in AWS.

VPC Flow Logs are popular for cloud security because of the broad coverage they provide, including in areas of the cloud where capturing packets can be difficult. While flow logs are an excellent data source for monitoring and analyzing network traffic, most organizations do not leverage them for real-time analysis, limiting their efficacy. Moreover, gaining access to multiple data sources has historically required using multiple products and user interfaces, which creates friction due to complexity and tool

sprawl. ExtraHop Reveal(x) 360 now eliminates these challenges, combining real-time analysis of flow logs, packets, and protocols in a unified interface providing long-overdue threat defense for cloud environments.

- Breadth and depth of detection: Real-time visualization of threat hotspots across workloads allows security teams to quickly investigate any incident down to root cause. This approach reduces false positives and keeps security teams focused on the highest-priority threats, maximizing and scaling scarce analyst resources. Reveal(x) 360 also unifies visibility and threat detection across IaaS, PaaS, container, and serverless environments.

- Zero friction for SecOps and DevOps: As an agentless solution, Reveal(x) 360 for AWS deploys without friction and provides broader coverage than agent-based endpoint tools and application logs. Reveal(x) 360 collects and analyzes flow log and packet metrics to create a real-time view of all cloud workloads, while AI behavioral detection surfaces the highest priority threats for investigation and remediation in a single management pane.

- Lower TCO: The new Reveal(x) 360 sensor deploys without agents and a single instance provides broad, correlated coverage of attack patterns and activity across multiple workloads in a single user interface while reducing total cost of ownership.

“Cloud application developers have zero tolerance for security measures that impinge application performance or slow code development velocity. Pair this with the complexity of microservices-based applications that are easily accessed via APIs and you start to understand the challenges of securing the cloud,” said Frank Dickson, program vice president, security and trust, IDC. “ExtraHop’s ability to ingest both VPC Flow Logs and packets in a single UI for cloud security coverage is a no-brainer. Security teams can illuminate and investigate malicious activity in near real time without requiring developers to make adjustments to code development.”

Contact your ExtraHop sales representative or channel partner for more information, or visit www.extrahop.com/solutions/cloud/aws-security (http://www.extrahop.com/solutions/cloud/aws-security).

Additional Resources:
Landing page with additional information (https://www.extrahop.com/solutions/cloud/aws-security/)
Reveal(x) 360 ebook (https://www.extrahop.com/resources/papers/revealx-360-ebook/)
Solution brief (https://www.extrahop.com/resources/papers/aws-cloud-threat-defense-solution-brief-form/)

About ExtraHop
Cyberattackers have the advantage. ExtraHop is on a mission to help you take it back 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, enterprises can detect malicious behavior, hunt advanced threats, and forensically investigate any incident with confidence. ExtraHop has been recognized as a market leader in network detection and response by IDC, Gartner, Forbes, SC Media, and numerous others. Learn more at www.extrahop.com.

(http://www.extrahop.com/)

Press Contacts

Jake Galland
Positive
jgalland@positivemarketing.com
020 3637 0640

Ashley Stewart
ExtraHop
pr@extrahop.com