ExtraHop Announces Reveal(x) Cloud: Threat Detection, Investigation, and Response for the Hybrid Enterprise

New SaaS-based security solution powered by Amazon VPC traffic mirroring empowers enterprise SecOps teams to build a cloud-first approach to securing the hybrid attack surface.

SEATTLE & BOSTON – AWS RE:INFORCE – JUNE 25, 2019 – ExtraHop today announced ExtraHop® Reveal(x) Cloud™, a Software-as-a-Service (SaaS)-based network detection and response (NDR) solution for the cloud-first hybrid enterprise. Reveal(x) Cloud provides deep and continuous visibility, enabling Security Operations (SecOps) teams to analyse every transaction, detect threats, and respond to attacks to gain control over their hybrid attack surface and protect their investment in the cloud. While the cloud has proven to be a force multiplier for DevOps and IT Ops, for SecOps teams already struggling under the burden of a sprawling attack surface and a shortage of skilled analysts, adopting cloud platforms can be a vulnerability. With SecOps taking the blame for stalled migration efforts, enterprises are recognising the need to take a cloud-first approach to securing elastic workloads rather than trying to retrofit old practices to new technology design patterns. Without native network visibility in the cloud, enterprises have been limited to log- or agent-centric tools, making it difficult to detect and investigate complex threats in a timely manner due to lack of continuous visibility across all environments. Reveal(x) Cloud is a SaaS-based solution that provides security teams with a zero-infrastructure service for AWS that deploys quickly, delivers immediate asset discovery, and offers threat detection, investigation, and response. The solution takes advantage of new enterprise features introduced by AWS during AWS re:Inforce 2019, including Amazon Virtual Private Cloud (Amazon VPC) traffic mirroring that supports passive observation of network traffic from cloud workloads, and private network peering that allows for the secure transmission of data between AWS accounts. It also connects natively with AWS data sources, such as Amazon CloudWatch, AWS CloudTrail, and Amazon VPC flow logs. Check out the video to learn about how Amazon VPC traffic mirroring changes the game for monitoring AWS workloads: https://extrahop-1.wistia.com/medias/t1c688n7ea “Today, security operations teams often rely on tools and data sources like logs that don’t provide a complete picture,” said Dave Brown, Vice President, EC2 Compute and Networking Services, Amazon Web Services, Inc. “With the introduction of Amazon VPC traffic mirroring, we’re allowing customers to extract traffic of interest from any workload in an Amazon VPC and send it to the right tools to detect and respond faster to attacks often missed by traditional log- and agent-centric tools. With Reveal(x) Cloud, ExtraHop is delivering a purpose-built solution designed to enable AWS customers to take full advantage of network traffic for better cloud visibility, detection, and response.” Reveal(x) Cloud offers a host of features designed to help SecOps teams support the shared responsibility model, protect cloud workloads by ensuring compliance, and deliver security across the hybrid attack surface. Automatic Discovery and Classification: Up-to-the-minute visibility and classification across all cloud workloads allows SecOps teams to track rogue instances, prioritise investigations by risk score, and correlate malicious activity and asset criticality to focus on the highest-risk threats. Application Layer Decoding: Full support for AWS services, such as Amazon Elastic Compute Cloud (Amazon EC2), Amazon Simple Storage Service (Amazon S3), and AWS Elastic Load Balancing means visibility into behaviour, not just activity, while machine learning at the application layer provides immediate detection of exfiltration activity. Encrypted Payload Visibility: Reveal(x) Cloud decrypts SSL/TLS-encrypted traffic at line rate, including cipher suites supporting perfect forward secrecy, providing complete visibility into all communications, including encrypted malicious traffic. Rich Integrations: AWS CloudTrail events enrich network-based threat detection with on-box activity (disabled logging, suspicious processes, suspect file execution), while connection with Amazon CloudWatch allows granular tracking of privilege manipulation. Customers can also leverage integrations with orchestration platforms, such as Phantom, ServiceNow, and Palo Alto Networks, to automate response workflows. “The modern hybrid enterprise has created an expansive and complex attack surface that cannot be managed by traditional security tools or architectures," said Jesse Rothstein, CTO and co-founder, ExtraHop. "It's time to stop retrofitting old models onto the new reality and start building cloud-first security operations. With Reveal(x) Cloud and Amazon VPC traffic mirroring, SecOps teams finally have inside-the-perimeter visibility and control over their hybrid attack surface.” ExtraHop Reveal(x) Cloud is now available in preview. Please contact your ExtraHop sales representative for more information. What the industry is saying: “With Amazon VPC traffic mirroring in Reveal(x) Cloud, ExtraHop is further reducing the barriers to cloud adoption, by giving enterprises the same level of insight they’ve always had into their on-premises traffic,” said Mike Sheward, Senior Director, Information Security, Accolade. “Visibility has always been key in security, combine Reveal(x) with the native security features you find in AWS, and you’re going to have more actionable visibility than ever.” “Cloud providers continue to work with security vendors and with enterprise customers to provide functionality and integrations that make it easier, more efficient, and more secure to build presence in the cloud,” said Fernando Montenegro, Principal Analyst, 451 Research. “Amazon VPC traffic mirroring is just the latest example. ExtraHop’s Reveal(x) Cloud fits within this trend, as it allows customers to use traffic monitoring to achieve better network visibility, detection and response, and to do that as a service. This is likely to assist SecOps teams making the transition to support cloud deployments.” At ePlus, we believe that Cloud platforms, combined with the right technologies, can transform IT from a cost center to a business enabler,” said Justin Mescher, Vice President of Cloud and Data Center Solutions at ePlus. “We’re building Reveal(x) Cloud into our CyberSecurity and Cloud practices to help our customers increase their visibility and act quickly and accurately. This will bring improved cloud readiness and security

posture, leading to more rapid adoption of transformational Cloud services." "Pervasive enterprise digital transformation efforts are dramatically expanding the attack surface, but many organisations are failing to transform their cybersecurity approaches to keep pace, continuing to use the same cybersecurity methods they have always used while attempting to support continuously evolving business models," said Joe Vadakkan, Global Cloud Security Leader, Optiv. "Combining industry-leading technologies such as ExtraHop's Reveal(x) with Optiv's end-to-end services, enables us to provide clients with an approach to cybersecurity that is aligned to new business models and centered on client-focused outcomes. We believe that ExtraHop Reveal(x) Cloud will deliver great value to cloud workloads by providing the necessary visibility to more efficiently detect and respond to incidents." To learn more about how Reveal(x) Cloud delivers cloud-first network security, read the blog from ExtraHop co-founder and Chief Customer Officer, Raja Mukerji: http://www.extrahop.com/company/blog/2019/announcing-revealx-cloud-ndr-for-the-cloud-first-enterprise. To learn more about ExtraHop's vision for the cloud-first enterprise. check out the post from CEO, Arif Kareem: http://www.extrahop.com/company/blog/2019/security-leaders-embrace-cloud-first-future To learn more about the company's industry-leading cyber analytics platform, visit: https://www.extrahop.com/solutions/security and explore the Reveal(x) live interactive online demo: https://www.extrahop.com/demo About ExtraHop ExtraHop provides enterprise cyber analytics that delivers security and performance from the inside out. Our breakthrough approach analyses all network interactions in real time and applies advanced machine learning to help you investigate threats, ensure the delivery of critical applications, and protect your investment in the cloud. With this approach, we help the world's leading enterprises including Credit Suisse, Hasbro, Caesars Entertainment, and Liberty Global rise above the noise of alerts, organisational silos, and runaway technology with complete visibility, real-time detection, and guided investigation. To experience the power of ExtraHop, explore our interactive online demo: https://www.extrahop.com/demo or connect with us on LinkedIn: https://www.linkedin.com/company/extrahop-networks: and Twitter: https://twitter.com/ExtraHop ENDS

Contacts

David Bass
+61 2 9922 6820
mailto: david@basspr.com.au