



ExtraHop Partners With CrowdStrike to Deliver Cloud-Native Threat Detection from the Network to the Endpoint

New Integration Helps Security Teams Detect and Respond to Sophisticated Attacks While Addressing New Vulnerabilities Arising Due to the Remote Workforce Shift and Increased Hybrid Cloud Adoption

SEATTLE — June 3, 2020 — ExtraHop, the leader in cloud-native network detection and response, today announced a partnership with CrowdStrike, a leader in cloud-delivered endpoint protection. The partnership includes the powerful integration between ExtraHop® Reveal(x)[™] and CrowdStrike Falcon®, marrying best-of-breed cloud-native detection and response capabilities to provide protection from the network to the endpoint. As businesses and government agencies have transitioned employees to remote work and moved more of their operations off premises, it has exposed gaps in availability, access, and security. Adversaries around the world quickly took advantage of the chaos, exploiting misconfigured remote desktop protocol vulnerabilities and ramping up phishing scams. With cloud adoption surging and a major spike in the use of personal computing devices for work, it is more critical than ever for organisations to maintain a clear picture of managed and unmanaged devices on their network, as well as determine which are being adequately monitored and secured. The integration between ExtraHop Reveal(x) and CrowdStrike Falcon merges complete network visibility, machine learning behavioural threat detection and real-time decryption of SSL/TLS sessions to extract de-identified metadata for analysis. This approach provides joint customers powerful endpoint security and instant remediation of threats.

Real-time Detection: The integration allows security teams to rapidly detect threats observed on the network such as network privilege escalation, lateral movement, suspicious VPN connections, data exfiltration and more. It also helps thwart those occurring on the endpoint, including ransomware, local file enumeration, directory traversal, and code execution. This provides complete coverage across the entire attack surface.

Instant Response: When Reveal(x) detects urgent threats it notifies the Falcon platform to contain the impacted devices ensuring analysts can rapidly investigate and resolve threats. This cuts off access to network resources and endpoints before a security incident can turn into a breach.

Continuous Endpoint Visibility: With automatic device discovery and classification, Reveal(x) continuously updates and maintains a list of devices impacted by threats, even on devices where the CrowdStrike agent is not yet present. This alerts CrowdStrike customers to newly connected and potentially compromised devices that need instrumentation for device-level visibility. It also extends edge visibility to include IoT, bring your own device (BYOD), and devices incompatible with agents. “Over the past five years, the security industry has undergone a seismic shift from a model of purely ‘prevention and protection’ to one that additionally delivers detection and response,” said Raja Mukerji, ExtraHop co-founder and Chief Customer Officer. “CrowdStrike and ExtraHop have been at the forefront of that shift, arming security organisations with the situational awareness and control they need to protect businesses and consumers in a perimeterless world. With this partnership and integration, our customers can now detect and respond to every threat from the core to the edge and everywhere in between.” “The threat environment continues to grow in complexity as sophisticated cyber adversaries advance their attack techniques, evading security controls and gaining access to corporate networks,” said Matthew Polly, Vice President of Worldwide Business Development and Channels at CrowdStrike. “Comprehensive visibility and real-time threat detection that allow for fast investigation and response at scale are imperative for organisations to spot and stop threats quickly. Through this partnership, CrowdStrike and ExtraHop are providing customers the ability to identify and respond to malicious activity across the entire attack surface with a fully cloud-native integration that allows them to adapt with speed and agility.” “Sirius is excited to partner with ExtraHop and CrowdStrike to help provide a complete solution for integrating both network and endpoint detection and response,” said Jeremiah Cruik-Salzberg, Senior Director and Security Technologist at Sirius. “This integration provides complete network and endpoint visibility for clients, while helping them automate their response to any issues identified on the network.” “Around the globe, we see organisations working hard to keep up as threats grow more sophisticated, allowing cyber adversaries to set the pace,” said Alex Dodd, Head of Networking and Security at Computacenter. “As such, we are constantly working to collaborate with cyber security leaders like ExtraHop and CrowdStrike who can not only deliver at the speed customers now require but execute the desired business outcomes in every aspect of an organisation.” For more information on the ExtraHop and CrowdStrike integration, visit the partnership page: <http://www.extrahop.com/partners/tech-partners/crowdstrike> or sign up for the upcoming webinar: <https://www.brighttalk.com/webcast/14671/412968> CrowdStrike® and CrowdStrike Falcon® are the trademarks and/or registered trademarks of CrowdStrike, Inc. About ExtraHop ExtraHop delivers cloud-native network detection and response to secure the hybrid enterprise. Our breakthrough approach applies advanced machine learning to cloud and network traffic to provide complete visibility, real-time threat detection, and intelligent response. With this approach, we give the world’s leading enterprises including The Home Depot, Credit Suisse, Liberty Global, and Caesars Entertainment the perspective they need to rise above the noise to detect threats, ensure the availability of critical applications, and secure their investment in cloud. 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: @ExtraHop © 2020 ExtraHop Networks, Inc., Reveal(x), Reveal(x)360, Reveal(x) Enterprise, and ExtraHop are registered trademarks or marks of ExtraHop Networks, Inc. ENDS

Contacts

David Bass

+61 2 9922 6820

mailto: david@basspr.com.au