ExtraHop + Check Point SOFTWARE TECHNOLOGIES LTD.

FEATURED INTEGRATION

Automated Event-Driven Security for AWS

Take automated action on suspect domains and IP addresses with ExtraHop Reveal(x) for AWS and Check Point®.

Mitigate the Impact and Spread of Successful Attacks

When adversaries exploit vulnerabilities in your perimeter defenses and gain access to critical cloud workloads and data, you need the ability to quickly detect and respond to threats.

Give your cloud-focused security team the complete visibility, real-time detection, and intelligent response they need for event-driven security with response automation powered by the ExtraHop integration with Check Point gateways and AWS.

Reveal(x) for AWS uses Amazon VPC Traffic Mirroring to bring agentless network detection and response (NDR) to the cloud. With passive and continuous monitoring across Amazon VPCs, Reveal(x) for AWS unlocks the ultimate source of truth in the cloud — data from network traffic packets — for securing critical workloads and data in the cloud.

Defense-in-depth exists as a security best practice because perimeter-focused tools alone can't protect your public cloud environment. When combined with Check Point, Reveal(x) for AWS ensures that you have machine learning-powered threat detection that's always on and always ready to help mitigate the impact and spread of successful attacks.

Intelligent Response

East-West Visibility

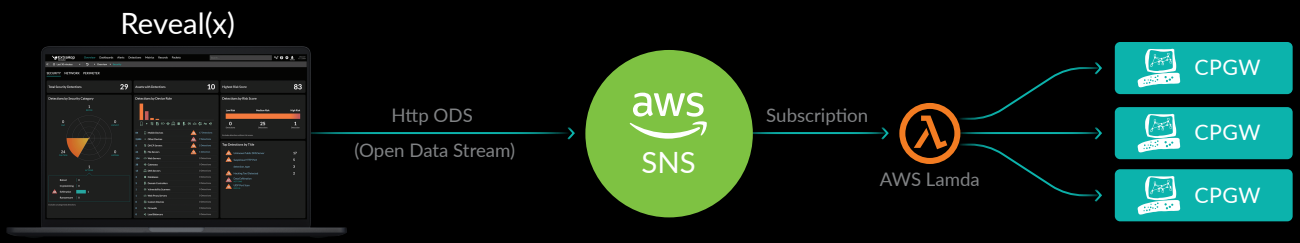
Real-Time Threat Detection

86 RISK

High-Fidelity Alerts

HOW IT WORKS

When Reveal(x) for AWS detects a high-risk security threat, it sends a message through Amazon SNS to a subscribed AWS Lambda function, which sends an Identity Awareness command to all configured Check Point gateways to block the offending domain or IP address.



VISIBILITY

ExtraHop applies analytics and machine learning to all traffic in the east-west and north-south corridors, providing broad visibility, detection, and investigation across the entire attack surface.

SCALABILITY

Native integration with Amazon SNS and AWS Lambda eliminates the need to create direct API calls for targeting individual Check Point Identity Awareness gateways.

FLEXIBILITY

SecOps and DevOps can use these highly customizable notebooks to engage in more in-depth investigation or targeted threat hunting by pooling together data from Reveal(x) and other sources.

KEY FEATURES

The integration with Amazon SNS enables security teams to attach a topic to multiple AWS Lambda functions to notify a SIEM, send email alerts, or create messages in collaboration hubs from Reveal(x) for AWS.

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.

© 2019 ExtraHop Networks, Inc. All rights reserved. ExtraHop is a registered trademark of ExtraHop Networks, Inc. in the United States and/or other countries. All other products are the trademarks of their respective owners.

ExtraHop

520 Pike Street, Suite 1600
Seattle, WA 98101