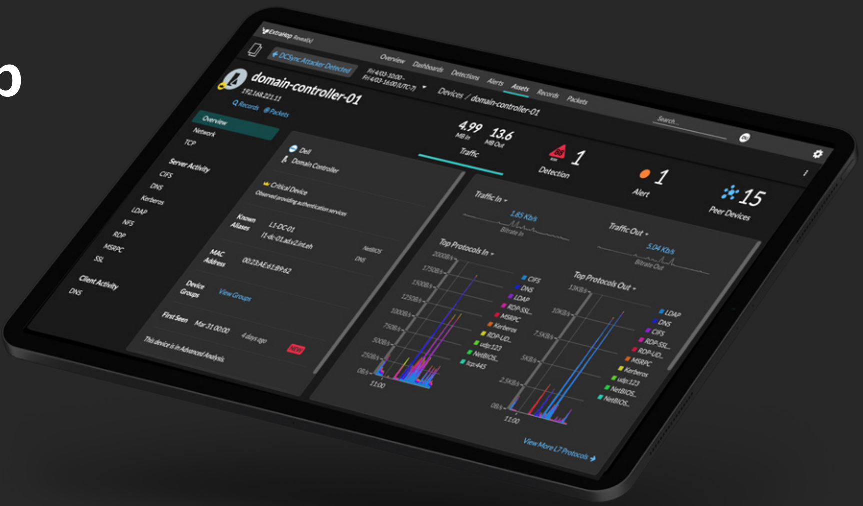
ExtraHop + CROWDSTRIKE

FEATURED TECHNOLOGY PARTNER

# Detect and Contain Threats with ExtraHop and CrowdStrike

Providing real-time network and endpoint threat detection for fast investigation and response



Dell
Domain Controller
Critical Device
Observed providing authentication services
Known Aliases: L1-DC-01, l1-dc-01.adv2.int.eh
MAC Address: 00:23:AE:61:B9:62
Device Groups: View Groups
First Seen: Mar 31 00:00 4 days ago NEW
This device is in Advanced Analysis.

## Challenges

Enterprises are faced with an ever-evolving threat landscape, and attackers are developing sophisticated approaches using encryption, lateral movement and network privilege escalation to evade detection while stealing valuable data. Businesses also struggle to not only maintain a clear picture of managed and unmanaged devices on their network, but also to determine which are being adequately monitored and secured.

## Solution

The integrated solution of ExtraHop Reveal(x) and CrowdStrike® Falcon™ merges complete network visibility, machine learning behavioral threat detection, and real-time decryption with powerful endpoint security and instant remediation. When Reveal(x) detects an urgent threat only visible on the network, it automatically notifies CrowdStrike to contain the impacted devices so analysts can rapidly investigate and resolve threats.

Instantly detect threats in network and cloud traffic — such as privilege escalation, ransomware, strange VPN connection behavior and data exfiltration — as well as on endpoints for faster remediation

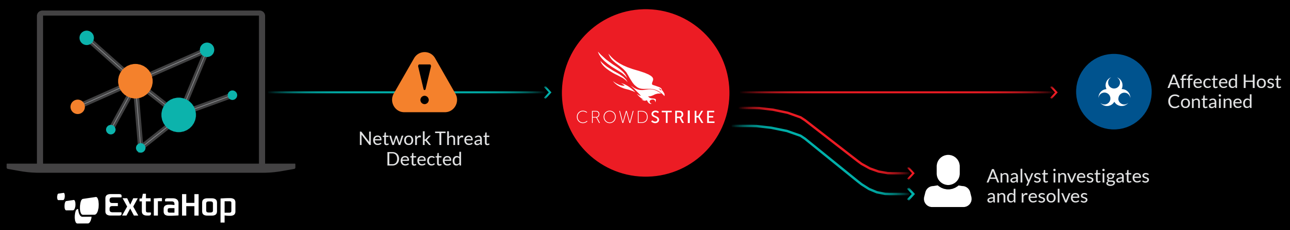
Rapidly respond—contain endpoints with high-severity network threats automatically

Discover and identify all devices on the network, with or without agents — IoT-connected devices (IoT), bring-your-own devices (BYOD) and more

FEATURED TECHNOLOGY PARTNER

## HOW IT WORKS

CrowdStrike Falcon provides endpoint detection and response (EDR) capabilities by continuously monitoring all endpoint activity, and analyzes the data in real time to detect and prevent advanced threats as they happen. When Reveal(x) detects a threat of sufficient severity on the network, it can alert Falcon and trigger a network containment event, stopping the spread of the threat while analysts investigate and remediate the issue.



| Use Case | Solution | Benefits |
|---|---|---|
| Instantly contain threats | Reveal(x) detects threats in network traffic, even if encrypted, and notifies CrowdStrike to quarantine the impacted endpoints | Customers have more time and easier access to all of the details they need, both from the network and endpoint perspectives, to investigate and resolve threats |
| Track IoT, BYOD and other devices without agents | Reveal(x) keeps a list of devices impacted by threats where no CrowdStrike agent was present | Customers gain a view of which devices in their environment are being impacted by threats but are not yet being monitored by CrowdStrike |

## KEY FEATURES

- Detects threats rapidly on both the network and endpoints
- Remediates threats automatically based on confident, low-false positive detections
- Monitors and inventories all devices, whether agent-compatible or not (IoT, BYOD and more)

### ABOUT CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 3 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform. There's only one thing to remember about CrowdStrike: We stop breaches.
Learn more: https://www.crowdstrike.com/

### 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.

ExtraHop

520 Pike Street, Suite 1600
Seattle, WA 98101