EXTRAHOP

Full Packet Visibility to Supercharge Detection and Investigation

With ExtraHop RevealX™ for Real-Time Hybrid Packet Capture and Decryption at Scale

SOLUTION BRIEF

The Challenge

Your team of cybersecurity professionals faces significant challenges due to the increasing number of cyberattacks leveraging encryption to evade detection. Threat actors use encryption for lateral movement, exploring networks, searching for vulnerabilities, spreading malware, and communicating with command-and-control servers. The lack of comprehensive network packet decryption in your security stack blinds your security teams to malicious activities and obstructs their forensic investigation efforts.

This combination of lack of instrumentation and pervasive use of encryption makes detecting and investigating encrypted threats incredibly difficult. For instance, the 2024 BlackCat ransomware attack on Change Healthcare used stolen credentials for lateral movement across the network, as well as 11 different encryption techniques throughout various stages of the attack.

The escalating use of encryption in cyberattacks poses a significant threat to your organization. Current data reveals that 87% of threats are delivered via encrypted channels, with 79% of those communications being malware-free in 2024. Threat actors are exploiting over 100 other protocols to conceal their activities through encryption, contributing to reports indicating that 41% of attacks bypass existing security defenses. Examples include:

- Application protocols, such as LDAP, MS-RPC, and SMBv3.
- Critical Active Directory protocols, like Kerberos, LDAP, SMB, and RPC.
- Remote Command Execution protocols, including SMB, WMI, and DCOM.

The Solution

ExtraHop RevealX natively decrypts and decodes over 100 protocols, eliminating the performance and operational challenges from relying on third-party tools. This provides unparalleled on-demand visibility that enables you to detect common encrypted attacks that your other tools miss, such as Kerberos Golden Ticket Attacks, PowerShell Remoting, and the abuse of Remote Monitoring and Management (RMM) tools, which have seen a 70% increase in use for endpoint attacks.

ExtraHop also decrypts network traffic at speeds up to 100 gigabits per second. Its wire-speed performance ensures no impact on your network performance or added latency, while maintaining data security with TLS 1.3 and Perfect Forward Secrecy.

KEY STATISTICS

87% of threats are delivered over encrypted channels[1]

Average breakout time from initial access to lateral movement is 48 minutes, with the fastest breakout observed at just 51 seconds[2]

79% of detections in 2024 were malware-free[2]

41% of attacks successfully bypass existing security defenses[3]

The ExtraHop platform continuously updates its cloud-based ML/AI with massive threat intelligence datasets. The result is high-fidelity detections with minimal false positives, something on-device ML cannot achieve due to its limited compute resources and update challenges.

This comprehensive approach to network detection and response (NDR) makes ExtraHop RevealX an essential component for a mature cybersecurity program, enhancing an organization's overall security posture.

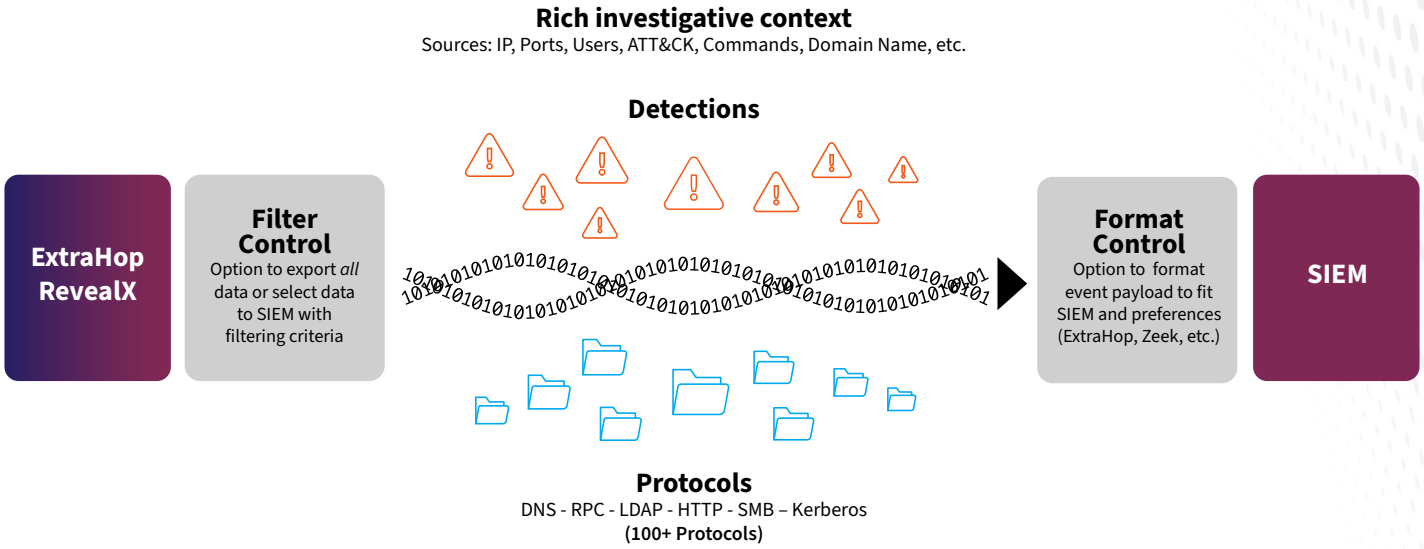

Figure 1: Find, filter, and focus on what matters most using RevealX forensics and workflows, or share relevant data with other tools to get more value from your entire security stack investment.

CUSTOMER BENEFITS

Full packet visibility of encrypted data makes your threat detection and response more effective, your forensic investigations more efficient, and reduces your blind spots to threat actors active in your hybrid network.

By decrypting all relevant network traffic, RevealX also gives you immediate confirmation of malicious activity and breaches, providing "smoking gun" evidence with market-leading packet-level forensics with native, scalable packet capture and integrated workflows.

- **The Smart Triage feature enables you to move quickly from alerts to investigations, reducing significant delays for your analysts to begin work on what matters most.**
- **Your analysts will conduct forensic investigations faster because of their ability to move seamlessly from detections to records to packets in just two clicks.**
- **The investigation process will be streamlined by features like file carving, which enables the direct extraction of only relevant data from packet stores and eliminates the need for separate tools.**
- **They'll also have a better understanding of the scope of an incident with the automatic aggregation of high-risk attack patterns in the Smart Investigations feature.**

The rich, decrypted network data fuels ExtraHop's cloud-based ML/AI and the continuous updating and training of millions of high-fidelity models using your network's unique activity. This cloud-scale ML/AI approach drastically reduces false positives and the resulting alert fatigue for your analysts. It also enables features like Smart Investigations that automatically aggregate context for high-risk attack patterns, reducing alert fatigue and accelerating incident response.

Ultimately, ExtraHop RevealX improves your efficiency and business resilience by providing real-time network insights and high-fidelity ML/AI detections. You will accelerate your mean time to investigate cyber threats and expose hidden risks across your entire network.

USE CASES

Decryption Enables Detection of Common Attacks That Other Tools Miss

Lateral Movement Techniques

- Kerberos Silver or Golden Ticket Attacks
- Kerberoasting
- AS-REP Roasting
- PtH / PtT Attacks
- DCSync Attacks
- PowerShell Remoting

Active Directory Recon Techniques

- BloodHound & SharpHound Detection
- All Object Queries
- Unusual Query Volume
- SMB Enumeration
- PowerShell AD Cmdlets
- Unusual SMB File Access

Persistence Techniques

- RMM Tool Abuse
- Password Spraying
- Unusual RDP Activity
- Skeleton Key Attacks
- Anomalous SSH Tunneling
- Malicious Web Shell Activity
- LOLBAS Attacks

ExtraHop decrypts and decodes 100+ protocols!
(LDAPS, SMB, MSRPC, Kerberos, HTTPS, etc.)

TAKE THE NEXT STEP

For more information and to schedule a demo, visit extrahop.com

1. "ThreatLabz 2024 Encrypted Attacks Report", Zscaler, https://www.zscaler.com/campaign/threatlabz-encrypted-attacks-report
2. "CrowdStrike 2025 Global Threat Report", CrowdStrike, https://www.crowdstrike.com/en-us/global-threat-report/
3. "41% of Attacks Bypass Defenses: Adversarial Exposure Validation Fixes That", Bleeping Computer, https://www.bleepingcomputer.com/news/security/41-percent-of-attacks-bypass-defenses-adversarial-exposure-validation-fixes-that/

ABOUT EXTRAHOP

ExtraHop is the cybersecurity partner enterprises trust to reveal cyber risk and build business resilience. The ExtraHop RevealX platform for network detection and response and network performance management uniquely delivers the unparalleled visibility and decryption capabilities that organizations need to investigate smarter, stop threats faster, and move at the speed of risk. Learn more at extrahop.com.

EXTRAHOP

info@extrahop.com
extrahop.com