EXTRAHOP

RevealX™ + Microsoft Defender for XDR

Uplifting Security with Integrated Microsoft EDR and ExtraHop NDR

Overview

Are you truly confident you can detect the breach that has already moved past your EDR?

Today's sophisticated adversaries are already inside your network, leveraging encrypted traffic for lateral movement and bypassing your agent-dependent security stack. As a result, you are missing critical attack stages—like reconnaissance and credential theft—because they are hidden in encrypted protocols such as Kerberos and MSRPC that your EDR cannot decode.

This creates significant blind spots:

- **Encrypted Traffic:** Nearly 80% of threats use malware-free techniques that mimic normal user behavior, countering key EDR defenses.
- **Unmanaged Devices:** Dangerous blind spots exist where EDR agents cannot be installed, such as on critical IoT, OT, or unmanaged devices.
- **Operational Burnout:** Security teams spend an average of 14.1 hours per week chasing false positives due to a lack of valuable visibility and context.

ExtraHop RevealX Network Detection and Response (NDR) is the force multiplier you need.

As an established leader in the NDR market, ExtraHop exposes threat activity in these blind spots by integrating deep decryption and agentless network visibility seamlessly with **Microsoft Defender for Endpoint (MDE).** The resulting unified capability provides you with full-spectrum detection coverage across the entire MITRE ATT&CK framework.

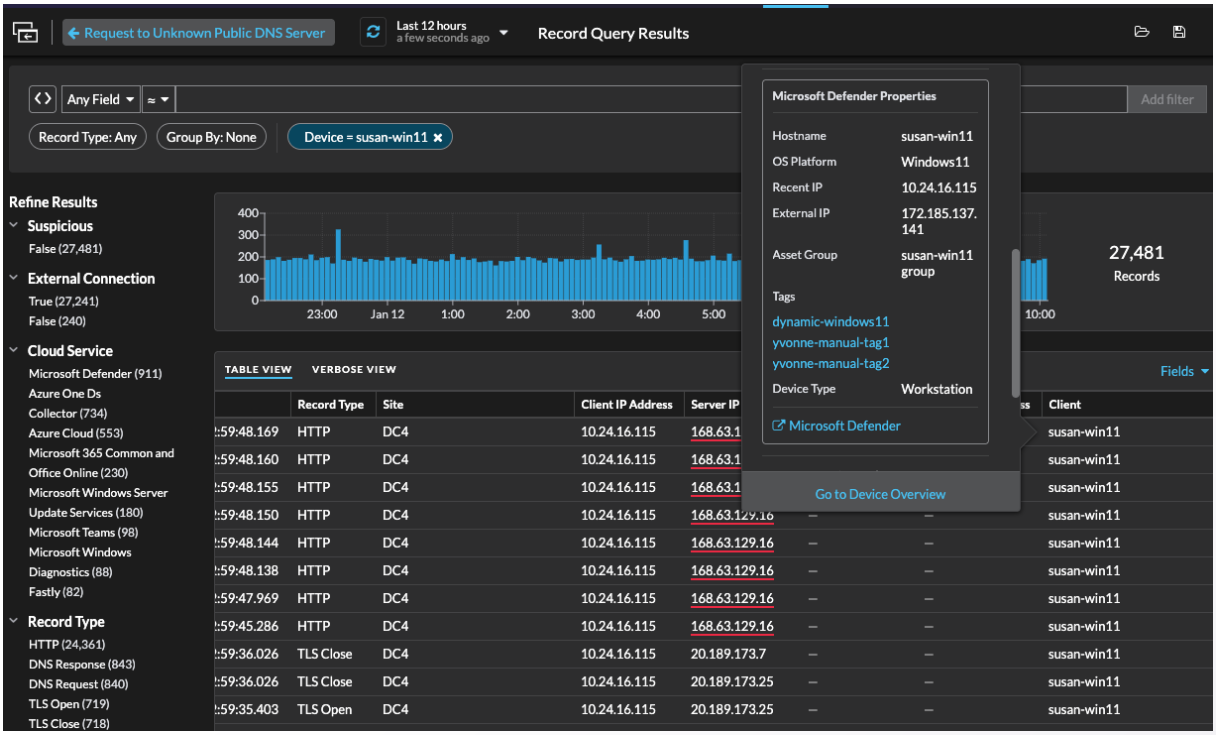

Figure 1. Microsoft Defender provides device data within RevealX NDR, giving analysts invaluable context for observed network activity and trends.

Customer Challenge

You recognize that perimeter defenses are obsolete; the attack surface now extends deep into your network. However, relying solely on Microsoft Defender for Endpoint (MDE) still leaves your organization vulnerable to the most evasive threats. The primary technical gap is encryption: **Over 87% of modern attacks use encrypted channels** to hide internal reconnaissance and lateral movement, leveraging protocols like MSRPC and Kerberos that EDR cannot decode. This means sophisticated credential theft and Living-Off-The-Land (LOTL) tactics are operating silently inside your environment, moving between hosts with zero detection.

Furthermore, EDR is inherently agent-dependent, creating a single point of failure. Adversaries are highly motivated and technically capable of bypassing or disabling endpoint agents as part of their standard attack protocol, instantly collapsing host-level visibility and giving the attacker free rein. Your defenses also vanish entirely for unmanaged critical assets, including IoT, OT, medical devices, and shadow IT, which cannot host an agent but represent high-value targets for lateral movement.

The operational challenge is equally severe. This fragmented view—network blind spots combined with endpoint data silos—results in alert overload and complicated triage processes. Your Security Operations Center (SOC) team is forced to **waste up to 14.1 hours each week validating low-fidelity alerts and false positives,** delaying response to genuine, high-impact breaches. This inefficient, manual correlation process inflates your Mean Time to Respond (MTTR), directly increasing the cost and scope of a potential breach. To secure the modern enterprise, you must bridge the network-to-endpoint visibility chasm.

Key Joint Solution Features

- Microsoft Defender for Endpoint is a cornerstone of modern security, providing essential, host-level telemetry for your EDR defense. However, modern adversaries are adept at bypassing agent-dependent security stacks, creating significant blind spots. Threats often hide in encrypted protocols like Kerberos and MSRPC that EDR cannot decode, or target unmanaged devices (BYOD, IoT, OT) where an agent cannot be installed.
- ExtraHop RevealX Network Detection and Response (NDR) is the force multiplier that eliminates these gaps. As an established leader in the NDR market, RevealX provides agentless, deep decryption and full network visibility, exposing lateral movement and other threat activity that has already moved past EDR.
- The integration of RevealX with MDE bridges the network-to-endpoint visibility chasm. This powerful, unified solution delivers full-spectrum detection and unified forensics by seamlessly correlating agentless NDR detections (network forensics) with MDE's agent-based EDR telemetry. This combination enables faster root cause analysis, ensures security for all assets, and provides defense against encrypted lateral movement. The result is a more streamlined SOC workflow, reduced Mean Time to Respond (MTTR), and a drop in alert fatigue and analyst burnout.

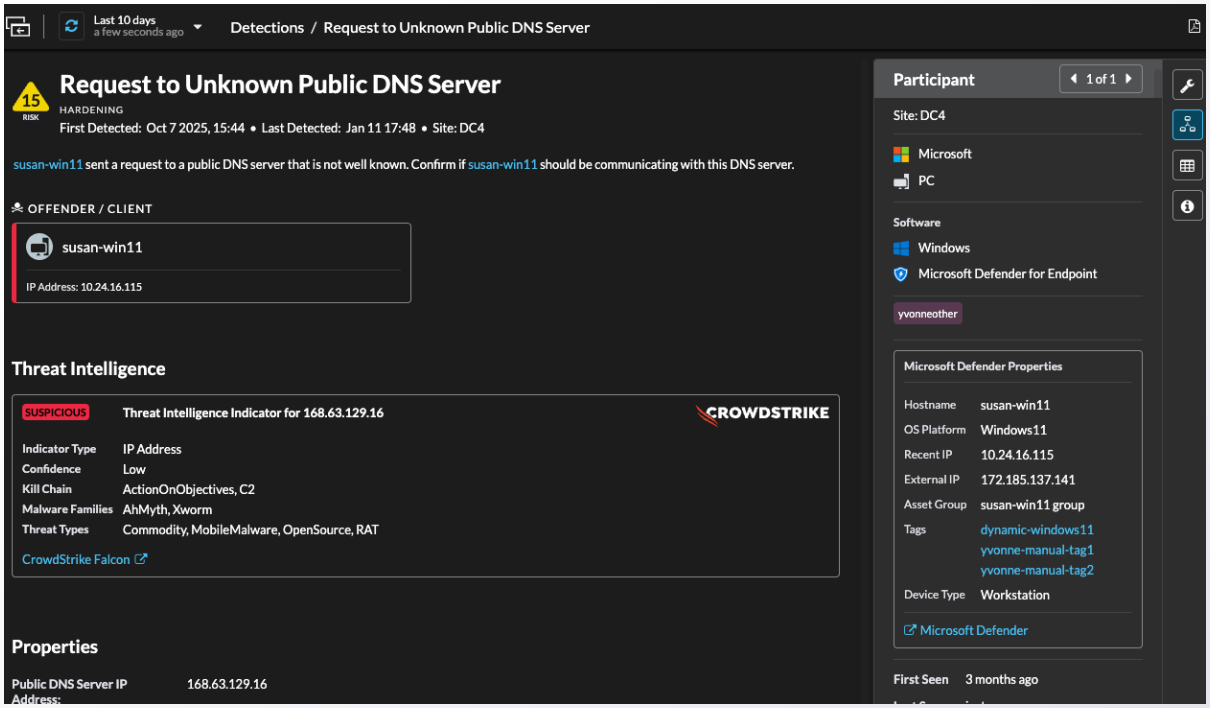

Figure 2. Accelerate alert triage, event investigation, and incident resolution in ExtraHop RevealX through integrated access to critical device telemetry from Microsoft Defender.

Key Benefits	Customer Value	How It Works
Full-Spectrum Detection and Unified Forensics	Provides full-spectrum detection, combining network forensics (PCAP), Layer 7 transaction records, and MDE endpoint data for faster resolution and more confident root cause analysis of missed threats.	Correlating agentless NDR detections (east-west) with agent-based EDR telemetry (host metadata) and fully integrated packet capture and visibility.
Security for Unmanaged IoT, OT, and BYOD Assets	Provides continuous security monitoring and discovery for all devices—including those that cannot host an EDR agent—ensuring no device becomes a silent foothold for attackers.	Agentless, full-coverage NDR monitoring of the network surface.
Defense Against Encrypted Lateral Movement	Utilizes deep packet inspection and true decryption capabilities to expose traffic and reveal threats hidden in encrypted flows like Kerberos and MSRPC that bypass EDR/ETA.	ExtraHop's advanced protocol decoding and decryption engine.
High-Fidelity Detections & Reduced Alert Noise	Applies cloud-scale machine learning (ML) and sophisticated behavioral analytics to raw network data, generating high-confidence alerts that drastically reduce SOC team overhead and alert fatigue.	Machine learning, AI-powered analysis, and precise detection tuning.
SOC Modernization and Greater ROI	Streamlines the SOC workflow by integrating high-fidelity detections directly into existing security ecosystems (like Microsoft Sentinel), ensuring greater ROI from EDR/SIEM investments and reducing operational overhead.	Data sharing and integrated workflows (SOAR/SIEM) that enhance analyst efficiency and efficacy of security tools.

USE CASES

Use Case	NDR Role (ExtraHop)	EDR Role (MDE)	Combined Outcome
Detect Lateral Movement	Detects network anomalies (unauthorized access, policy violations) and behavioral anomalies in east-west traffic.	Provides host telemetry directly to ExtraHop RevealX.	Analysts enjoy direct, on-demand access to endpoint context within RevealX to speed investigation and minimize dwell time.
Secure Encrypted Protocols	Decrypts and analyzes key protocols (Kerberos, MSRPC) to detect C2 activity or unauthorized authentication attempts hidden within normal traffic flows.	Supplies granular host telemetry to confirm whether the process associated with suspicious activity is legitimate or linked to post-exploitation frameworks.	Exposure of sophisticated internal breaches hidden in encrypted flows that bypass EDR-only systems.
Accelerate Triage and Investigation	Provides historical, lightning-fast, searchable network telemetry and full packet-level forensics (PCAP) to establish the full attack timeline and scope.	Delivers on-demand access to endpoint device data in a correlated timeline view to enrich network events.	Reduces Mean Time to Investigate (MTTI) by unifying "inside-out" (network) and "outside-in" (endpoint) views to shatter data silos.
Counter EDR Evasion Techniques	Provides continuous network detection capability and visibility into L7 transactions, acting as the critical layer when the EDR agent is disabled or bypassed.	Supplies on-demand access to rich endpoint telemetry via API.	Ensures full-spectrum coverage across the MITRE ATT&CK framework, closing detection gaps resulting from siloed data.

Conclusion

In today's threat landscape, relying solely on endpoint security creates critical, exploitable blind spots. Without an integrated EDR and NDR solution, you remain vulnerable to sophisticated adversaries who move laterally through your network via encrypted channels and target unmanaged devices that your EDR agent cannot see. This fragmented view forces your Security Operations Center (SOC) to waste time chasing false positives, resulting in increased investigation and response times and a higher risk of costly, impactful breaches.

To secure the modern enterprise, you must bridge this network-to-endpoint visibility chasm. The seamless integration of Microsoft Defender for Endpoint (MDE) and ExtraHop RevealX NDR provides the force multiplier needed to close these gaps. By integrating RevealX with MDE, you gain the complete, high-fidelity security coverage necessary to confidently defeat the most evasive threats.

TAKE THE NEXT STEP

For more information, visit extrahop.com.

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

© 2026 ExtraHop Networks, Inc., RevealX and ExtraHop are registered trademarks or trademarks of ExtraHop Networks, Inc. in the United States and/or other countries. All other products are the trademarks of their respective owners. 1079B 01.23.26