corelight



White paper

Detecting lateral movement: East-west network visibility

Attackers don't just break in; they move. East to west, system to system, deeper into your network. And that internal lateral movement is precisely where most security tools lose visibility.

Key takeaways

- 96% of lateral movement does not trigger alerts in traditional security tools (Gigamon, 2024 Hybrid Cloud Security Survey).
- EDR and perimeter tools provide incomplete east-west coverage in the terrain where lateral movement actually happens.
- Network Detection and Response (NDR) closes that gap through multi-layered detection, combining behavioral rules, anomaly detection, and machine learning (ML) to surface lateral movement that no single method can catch alone.

1. WHAT IS LATERAL MOVEMENT IN CYBERSECURITY?

Lateral movement is the phase of a cyberattack in which an adversary, having already gained a foothold inside your network, systematically navigates from system to system in search of valuable data, elevated privileges, and the access required to complete their mission. It is not the break-in. It is the internal movement that often follows initial access.

Unlike the initial intrusion, which crosses a perimeter, lateral movement travels east-west, not in and out through the network boundary, but laterally between internal systems. A compromised workstation becomes a launchpad for reaching a domain controller. A service account becomes a key to an administrative share. Each hop extends the attacker's reach and deepens the damage they can cause. Understanding how attackers move, and what they use to do it, is the foundation of effective detection.

Common lateral movement techniques and examples

- **Credential-based attacks:** Kerberoasting, Pass-the-Hash, and Pass-the-Ticket allow attackers to use valid credentials that look identical to legitimate logins, with no malware required.
- **Protocol abuse:** RDP, SMB/admin shares, and WinRM are legitimate protocols repurposed for movement, and their traffic can blend in with normal administrative activity.
- **Living-off-the-land (LotL):** Attackers use native OS tools like PowerShell instead of custom malware, leaving nothing new on disk for endpoint tools to flag.
- **Protocol tunneling:** Attackers obscure traffic within legitimate protocols, concealing movement from tools that inspect only headers or network flow metadata.
- **Staging and pre-exfiltration:** Data is aggregated and compressed on internal staging servers before it leaves the network, a step that is often the last opportunity for detection.
- **Ransomware deployment:** Lateral movement is the critical enabling phase of many ransomware attacks, as attackers traverse the network to maximize encryption scope before triggering the payload.

Stages of lateral movement

Lateral movement unfolds in stages, each building on the last:

- **Reconnaissance:** The attacker maps the internal network, identifying active systems, open ports, shared resources, domain structure, and high-value targets. This is often the first application of living-off-the-land techniques: Native OS commands and built-in Windows tools used to enumerate the environment without introducing new software.
- **Credential access:** Attackers harvest valid credentials to enable movement without triggering malware-based alerts. Techniques include Kerberoasting, credential dumping via tools like Mimikatz, and Pass-the-Hash.
- **Privilege escalation:** The attacker elevates from standard user access to administrative or domain-level privileges, unlocking access to a wider range of systems and data. The same credential-based techniques that enabled initial movement, including Pass-the-Hash and Kerberoasting, are frequently used here to acquire higher-value credentials.
- **Lateral movement execution:** Using the credentials and privileges gained, the attacker moves from system to system, putting protocol abuse into action. RDP, SMB, and WinRM (legitimate administrative protocols) carry the movement, making each hop indistinguishable from normal IT activity at the endpoint level.
- **Staging and pre-exfiltration:** Before data leaves the network, it is aggregated and compressed on internal staging servers, ready for extraction. File transfers over SMB or administrative shares make this stage visible at the network layer, even when endpoints show nothing unusual.

2. WHY LATERAL MOVEMENT IS HARD TO DETECT: THE EAST-WEST VISIBILITY GAP

Lateral movement is hard to detect because it happens in the one place most security tools were not built to watch comprehensively: East-west traffic between internal systems. Perimeter tools don't see it at all; EDR sees only fragments of it on managed devices. And because that terrain is largely invisible, the techniques that exploit it, including valid credentials, native tools, and standard protocols, go undetected not because they are inherently uncatchable, but because the full network behavior that would reveal them as anomalous is often not being monitored.

The two security controls most commonly used for detecting lateral movement are endpoint detection and response (EDR), which monitors activity on managed devices, and perimeter tools, such as firewalls and intrusion detection systems, which monitor traffic entering and leaving the network. Both provide significant value across a broad range of security use cases, but both have structural limitations when it comes to lateral movement detection.

EDR sees east-west activity partially and from one side only

On managed devices, EDR can observe network connections and some lateral movement indicators, but only from the perspective of the endpoint where the agent is installed. It cannot see both sides of an east-west session simultaneously, provides no coverage for unmanaged devices, and cannot observe the network-layer protocol patterns that reveal lateral movement techniques at scale. Those unmanaged devices often become the path of least resistance for lateral movement.

The perimeter is no longer the boundary that matters. The boundary that matters is inside.

Perimeter tools see the boundary, not the interior

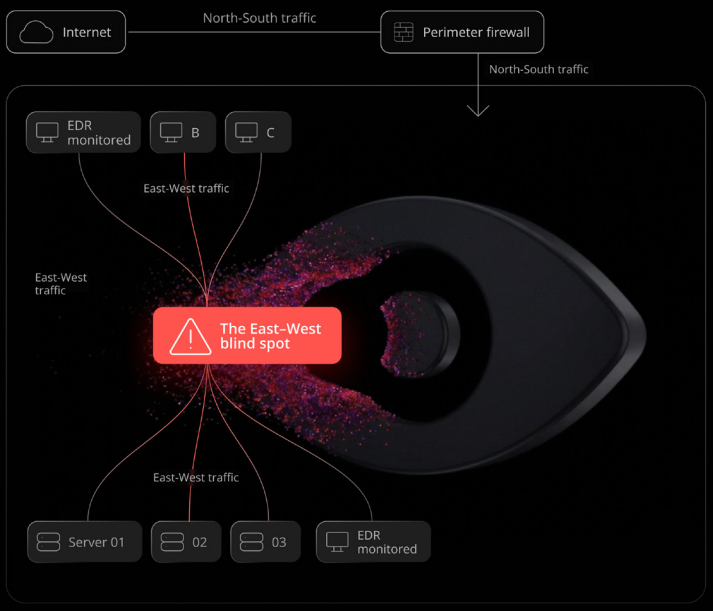
Firewalls and IDS/IPS monitor north-south traffic, which enters and leaves the network. Lateral movement never crosses that boundary. Once an attacker is inside, every subsequent move is east-west and completely invisible to tools designed to watch the edge.

The result

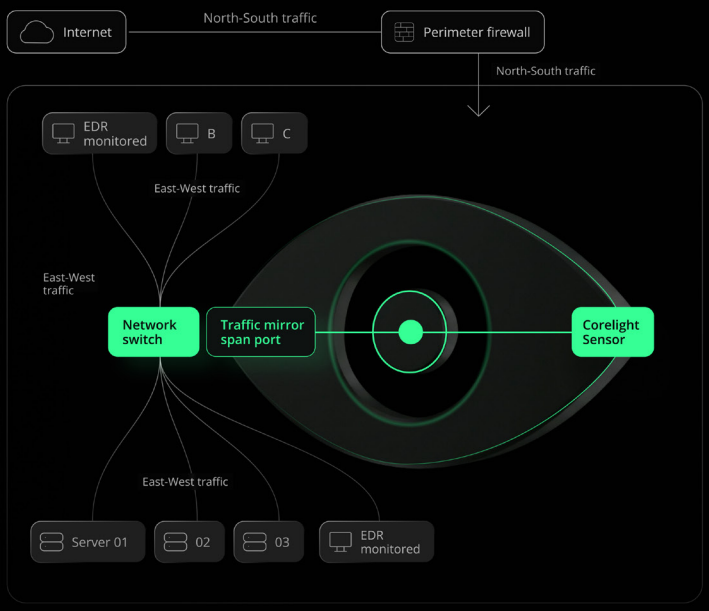
EDR and perimeter tools do share some coverage: EDR can detect certain lateral movement indicators on managed endpoints, and perimeter tools catch exfiltration as data crosses the boundary. But the overlap is narrow and the gaps are structural. The result is two tools with incomplete coverage: EDR sees fragments of east-west activity on managed endpoints, perimeter tools see none of it, and neither provides the network-wide, session-level view that reveals lateral movement as a pattern rather than isolated events.

Closing this gap requires a dedicated detection layer built specifically for east-west traffic, one that EDR and perimeter tools are not designed to provide. That is one of the roles of Network Detection and Response (NDR): not a replacement for existing controls, but the added layer that makes them complete.

Before Corelight:
The East–West blind spot



With Corelight:
East–West visibility



North-south vs. east-west traffic

Most security tools are built around north-south traffic. Lateral movement happens in the other direction entirely, including across cloud environments where east-west traffic flows between workloads and services that traditional perimeter tools never see:

	North-south traffic	East-west traffic
Direction	Into and out of the network perimeter	Between internal systems
Monitored by	Firewalls, IDS/IPS, web gateways	NDR (perimeter tools have no visibility)
Role in lateral movement	Initial access and exfiltration only	Every stage of lateral movement
What it carries	Inbound attacks, outbound data	Credential use, protocol activity, reconnaissance, staging

The gap in the comparison above is not simply a gap in tools. It is a gap in terrain. No amount of investment in endpoint or perimeter security addresses the east-west blind spot. That requires a different category of solution entirely. Gartner defines NDR as products that "continuously analyze raw network packets or traffic metadata between internal networks (east-west) and public networks (north-south)." The existence of NDR as a distinct analyst-recognized market category is itself evidence that east-west monitoring is a gap traditional tools do not fill.

Network Detection and Response (NDR) addresses this gap directly. Where EDR watches managed endpoints and perimeter tools watch the network boundary, NDR watches the network itself, monitoring east-west traffic between internal systems in real time, across managed and unmanaged devices alike. It is the detection layer purpose-built for the terrain where lateral movement actually happens.

3. HOW TO DETECT LATERAL MOVEMENT: ADDRESSING THE EAST-WEST NETWORK VISIBILITY BLIND SPOT

How NDR detects lateral movement

The east-west visibility gap established in Section 2, the terrain EDR and perimeter tools leave unmonitored, is precisely what Network Detection and Response (NDR) is built to address. NDR complements rather than replaces existing controls: EDR covers managed endpoints, perimeter tools cover the network boundary, and NDR provides continuous visibility across east-west and north-south traffic, monitoring activity in real time across managed and unmanaged devices alike.

To uncover threats in lateral movement, NDR applies multi-layered detection to that traffic through four complementary methods, each catching what the others miss. In today's advanced threat landscape, further complicated by AI-powered threats, no single method is sufficient on its own:

- **Signature-based detection (known tools and techniques):** Fast and effective for known threats, matching network traffic against known-bad indicators, catalogued attack patterns, and file-based signatures including static analysis approaches such as YARA. Where signature-based detection reaches its limit is precisely where lateral movement most commonly occurs: the credential-based and LotL techniques at the heart of most attacks use valid credentials and legitimate OS tools, leaving nothing for a signature to match. This is why the detection layers that follow are essential.
  - Example: During the RansomHub and BianLian ransomware attacks, adversaries used stolen credentials to access SMB mapped drives, subsequently employing net use commands to spread encryption payloads and second-stage malware laterally across the network.
- Behavioral detection **(known traffic procedures):** Expert-encoded detection rules map observed network behavior to MITRE ATT&CK techniques, firing on patterns that match known attack methodologies, including variations that have been slightly modified to evade signatures. Unlike single-indicator rules, behavioral detection examines multiple criteria simultaneously: an indicator alone may be innocuous, but a specific sequence of indicators across specific protocols from a specific source type is the behavioral fingerprint of a known attack technique. Behavioral detection fires immediately without requiring a learned baseline. Implementation varies: some vendors use Zeek scripting to chain these criteria into high-fidelity detections; others use AI-based approaches, which are more resource-intensive.
  - Example: Sliver is a post-compromise toolkit used by nation-state groups including Russian SVR and financially motivated threat actors to conduct reconnaissance, move laterally through the network, and exfiltrate data. It communicates with its control server using HTTP traffic that looks superficially legitimate but contains a distinctive combination of anomalies: GET requests carrying content in the request body (which legitimate browsers almost never do), fixed message sizes that never vary regardless of activity, and browser identity strings that claim to be Firefox but cite version combinations that have never existed. Behavioral detection fires when enough of these criteria appear together to cross a confidence threshold. The combination is distinctive enough that false positives are rare, and the more criteria present, the higher the alert confidence. In one real-world case, Sliver had successfully evaded every endpoint security control on the compromised host and was caught only at the network layer.
- Supervised ML **(behavior and pattern variations):** Supervised ML is trained on historical east-west attack data to recognize lateral movement not by exact signature match, but by behavioral similarity to past intrusions. An attacker who modifies their tooling but follows the same general sequence (reconnaissance, credential access, lateral movement, staging) will still be caught because the overall pattern resembles campaigns the model has seen before. This makes supervised ML particularly effective against sophisticated actors who actively engineer around known detection rules.
  - Example: Before exploiting F5 BIG-IP network devices in October 2025, attackers quietly mapped the network by scanning for open ports, the precursor to targeting US government and critical infrastructure organizations, with an 85% surge in attacks reported. The scanning was deliberately slow and low-volume to avoid triggering obvious alerts. Supervised ML recognized the campaign not from any single suspicious connection, but by reading across

hundreds of connection records simultaneously and identifying a statistical pattern that matched how attackers have scanned networks in past incidents. Each individual connection looked routine; the pattern looked like reconnaissance.

- **Anomaly detection / unsupervised ML (suspicious activity):** Learns over time by establishing behavioral baselines for every device, subnet, and session, flagging deviations from normal east-west traffic patterns that signature and behavioral rules would miss. Most effective against novel and credential-based lateral movement where no prior rule exists. Requires a learning period before reaching full effectiveness.
  - Example: The "Ink Dragon" threat actor (December 2025) gained a foothold inside an organization and moved laterally by hiding malicious functionality inside the organization's own internal web servers, leaving no malware files on disk and establishing long-term access across internal systems. The anomaly engine detected the lateral movement by noticing that an internal host had begun communicating with another internal subnet using a network service that had never appeared in that subnet before. Nothing about the communication matched a known attack pattern. The only signal was that it was new, and new was enough.

Note: NDR may also incorporate additional threat detection layers, including IOCs, threat intelligence, and threat hunting workflows, to support broader north-south and east-west investigation.

The signals NDR surfaces

Across these detection layers, NDR surfaces lateral movement signals that EDR and perimeter tools cannot see completely, with some invisible to both, others only partially visible on managed endpoints:

- SMB sessions and admin share access between internal systems, where the network-wide pattern across multiple devices is only visible at the network layer

The table below compares the three tool categories across key lateral movement detection capabilities. NDR's coverage advantage reflects its defense-in-depth detection approach; no single detection layer achieves these results alone:

Detection capability	EDR	Perimeter tools	NDR
SMB / admin share lateral movement	Partial†	None	Full
Kerberos attack detection	Partial†	None	Full
RDP behavioral anomaly detection	Partial†	None	Full
Credential-based attack detection	Partial†	None	Full
Living-off-the-land (LotL) detection	Partial†	None	Full
Encrypted traffic analysis (TLS/JA3/JA4)	None	None	Full
Protocol tunneling detection	None	None	Full
East-west traffic visibility	Partial†	None	Full
Unmanaged device coverage	None	None	Full
Staging server / pre-exfil signals	None	Limited‡	Full

† EDR footnote: "Partial" reflects three distinct constraints: (1) agent coverage, because EDR only monitors managed, enrolled devices; (2) session visibility, because EDR observes east-west connections from one endpoint's perspective only, never the full session; and (3) protocol-level gaps, because certain network-layer signals require wire-level observation that endpoint telemetry cannot replicate.

‡ Perimeter footnote: "Limited" indicates perimeter tools observe the outbound exfiltration phase only, not the internal lateral movement that precedes it.

- Kerberos ticket anomalies indicating credential-based attacks in progress, captured network-wide across all devices regardless of management status, providing complete session-level visibility that EDR sees only partially on managed endpoints
- RDP connections to unusual or previously unseen destinations, since anomalous lateral connection patterns across subnets require network-level observation
- Executable file transfers moving between internal systems, visible at the network layer before execution occurs on the endpoint
- Protocol tunneling, where encapsulation behavior between internal systems is invisible to endpoint tools
- File transfers to staging servers as a pre-exfiltration signal, visible before data leaves the network
- Encrypted traffic anomalies, including TLS metadata and JA3/JA4 fingerprint patterns captured network-wide without decryption; no endpoint equivalent exists
- Anomalous VPN usage and producer-consumer ratio imbalances, including directional and volumetric anomalies only observable at the network layer
- Unusual SSH clients or connections to new internal destinations

These signals are captured in structured network logs, including SMB file movement, Kerberos authentication events, connection metadata, SSL/TLS sessions, and RDP activity with each recording a different dimension of attacker behavior at the network layer. NDR continuously ingests and correlates these logs, applying detection rules and behavioral models to surface threats and anomalies, linking related events via the Unique Connection ID, and enabling analysts to reconstruct the full attack path from initial reconnaissance through staging in a single query rather than across multiple tools. In addition to the built-in detections, NDR can often be used for proactive threat hunting. Step-by-step hunt queries using logs in a SIEM can be found in our threat hunting blog post.

Detection coverage: EDR vs. perimeter tools vs. NDR

The tools that best detect lateral movement, C2, and data exfiltration work together as a layered stack: EDR monitors managed endpoints, perimeter tools monitor north-south traffic, and NDR provides visibility into the east-west activity those tools can miss.

4. HOW TO MITIGATE LATERAL MOVEMENT: BEST PRACTICES

Mitigating lateral movement requires both architectural decisions and operational discipline, and the speed of modern attacks means these practices must be in place before an attacker arrives, not after. With average breakout times now measured in minutes, the window between initial access and full lateral movement is narrower than most incident response processes can close.

Architecture and access controls

- Segment the network into discrete zones with enforced boundaries between them
- Apply least privilege to all accounts and service credentials
- Apply zero trust principles by verifying every user and device continuously rather than granting implicit trust based on network location; limits the blast radius of a compromised credential even when lateral movement has begun

Corelight helps security teams close the east-west visibility gap with network evidence, multi-layered detection, and structured logs built for investigation.

- Disable or restrict administrative protocols (RDP, SMB, WinRM) where not operationally required
- Audit and remove stale accounts and accounts with excessive privileges on a defined schedule
- Enforce multi-factor authentication on all administrative accounts and remote access pathways

Visibility and detection

- Deploy continuous east-west traffic monitoring, since periodic or perimeter-only monitoring leaves internal movement invisible.
- Establish behavioral baselines for every subnet, user group, and device category before an incident occurs (specific to anomaly-based detection; behavioral/TTP and supervised ML detections do not require baseline establishment).
- Capture structured network evidence across all east-west protocols, including SMB file movement, Kerberos authentication, connection metadata, SSL/TLS sessions, and RDP activity, enabling search and correlation across all entity interactions.
- Monitor administrative share access for connections from non-administrative or unexpected sources.

- Enable anomaly detection for RDP, SSH, executable file transfers, and VPN usage across internal subnets.
- Extend visibility to unmanaged devices, cloud environments, and OT/ICS networks.

Response and containment

- Define and test containment procedures against a defined breakout time window, since lateral movement can progress to full breach in minutes.
- Automate initial alert triage using GenAI-powered tools. Agentic Triage correlates network evidence, executes expert playbooks, and delivers investigation-ready conclusions in minutes rather than hours.
- Correlate network evidence with endpoint and identity data to reconstruct the full attack path.
- Treat network evidence as the authoritative record, since it cannot be tampered with by an attacker who does not control network infrastructure.
- Conduct post-incident review of east-west traffic logs to identify dwell time, movement patterns, and detection gaps.
- Update threat detection rules, training, and models as necessary.

5. HOW CORELIGHT NDR CLOSES THE GAP

East-west visibility as the core capability

Corelight's Open NDR platform provides continuous visibility across east-west and north-south traffic. It is purpose-built for the east-west terrain where lateral movement actually happens, helping to close the visibility gap that EDR and perimeter tools leave open. Corelight captures every internal session, including SMB, Kerberos, RDP, and SSL/TLS, in structured logs with full protocol context across managed and unmanaged devices. More than 70 log types linked by a Unique Connection ID enable analysts to reconstruct the full attack path in a single query.

Its multi-layered detection strategy means each layer catches what the others cannot. Signature-based detection, including YARA static file analysis, catches known malware and tools immediately. Zeek-scripted behavioral detections are packaged as continuously updated Collections covering lateral movement, C2, and exfiltration. Per-environment baselines, anomaly detection, and unsupervised ML surface behavioral deviations that no rule could anticipate. Supervised ML catches evolved attack variants that retain the behavior of past intrusions. Additional layers support broader detection workflows, including IOCs, threat intelligence, and proactive threat hunting capabilities.

6. FAQS

Q1: Why is east-west traffic often a blind spot for security teams?

East-west traffic moves between internal systems and never crosses the perimeter, so firewalls, IDS/IPS, and other boundary tools are simply not positioned to see it. Most organizations have invested heavily in monitoring what enters and leaves their network, but have limited or no dedicated visibility into what moves laterally inside it. Without east-west visibility, the attacker's most productive phase, the internal movement that follows initial access, is entirely invisible.

Q2: What is the role of network evidence in detecting lateral movement?

Network evidence is the most reliable record of lateral movement because it cannot be disabled or tampered with by an attacker who does not control network infrastructure. Endpoint agents can be killed; logs can be cleared; but network traffic, once captured, provides an immutable record of every connection, authentication, and data transfer. Structured network logs, particularly SMB, Kerberos, RDP, and connection metadata, allow analysts to reconstruct what happened, when, between which systems, and in what sequence. This is evidence-based security: detection and investigation grounded in what actually occurred on the network.

Q3: How can you detect lateral movement in encrypted traffic without decrypting it?

Decryption is not required. Metadata patterns in TLS handshakes, including JA3/JA4 fingerprints, certificate characteristics, cipher suite selections, and connection behavior, reveal anomalous patterns that indicate malicious activity even when the payload is encrypted. A C2 implant communicating over TLS produces a distinctive fingerprint in the handshake that differs from legitimate browser traffic, even if the content of the communication is indistinguishable. JA3/JA4 fingerprinting captures these patterns network-wide, providing detection coverage for encrypted lateral movement without the computational cost or privacy implications of full decryption.

Q4: How does NDR complement EDR for lateral movement detection?

EDR sees what happens on managed endpoints; NDR sees what happens on the network, including unmanaged devices, east-west sessions, and activity that occurs after an attacker disables or evades an endpoint agent. The two tools cover structurally different terrain and are most

effective in combination. EDR provides deep process-level visibility on endpoints it covers; NDR provides network-wide session visibility across everything, managed and unmanaged alike. NDR's multi-layered detection, combining behavioral rules, anomaly detection, and supervised ML, means it catches lateral movement through multiple independent mechanisms simultaneously, dramatically reducing the likelihood that any single technique evades detection.

Q5: How can I use Corelight's Zeek logs to find lateral movement in my network?

You can use Zeek logs to hunt for lateral movement by analyzing network evidence across internal connections, authentication activity, file transfers, encrypted sessions, and remote access patterns. Five logs provide the richest lateral movement evidence:

- **smb_files.log:** File path, access commands, and which account accessed which share across all devices on the network.
- **kerberos.log:** Authentication requests, ticket types, encryption algorithms, and anomalous request patterns that indicate Kerberoasting or Pass-the-Ticket activity.
- **conn.log:** Every connection across the network, including source, destination, duration, bytes transferred, and protocol; the foundational dataset for detecting anomalous east-west communication patterns.
- **ssl.log:** Certificate details, cipher suites, JA3/JA4 fingerprints, and TLS handshake anomalies for encrypted lateral movement detection.
- **rdp.log:** RDP session metadata, authentication outcomes, and connection patterns that reveal anomalous lateral RDP usage.

All five are linked by a Unique Connection ID, enabling analysts to pivot across log types and reconstruct the full lateral movement sequence in a single investigation without switching tools.

Q6: How does lateral movement by an insider threat differ from an external attacker, and why is NDR better positioned to detect it than EDR or perimeter tools?

At the network layer, insider threat lateral movement is behaviorally similar to external attacker lateral movement, with the same valid credentials, the same legitimate protocols, and the same east-west traffic patterns. This is precisely why EDR and perimeter tools struggle to detect it. NDR addresses this through all four of its detection layers: behavioral/TTP-based rules catch known insider threat patterns immediately; anomaly detection / unsupervised ML flags deviations from the insider's own established behavioral baseline, such as unusual data access volumes, systems accessed outside normal patterns, atypical working hours; supervised ML recognizes variations of known insider attack sequences; and signature-based detection catches any known tools the insider may deploy. The behavioral deviation, not the individual action, is the signal. For a deeper treatment, see Corelight's insider threat white paper Corelight's Threat Hunting Guide.

Q7: How can I detect lateral movement if I can't put an agent on every IoT/OT device?

If you can't deploy agents everywhere, network-level visibility becomes essential. NDR monitors traffic between systems directly, including unmanaged devices, IoT, OT, cloud workloads, and systems where endpoint agents are impractical or unavailable. That allows teams to detect suspicious east-west activity, such as unusual SMB sessions, RDP connections, Kerberos anomalies, protocol tunneling, and staging behavior, without relying on endpoint coverage alone.



To learn more about detecting lateral movement, request a demo at

https://corelight.com/contact

info@corelight.com

The Z and Design mark and the ZEEK mark are trademarks and/or registered trademarks of the International Computer Science Institute in the United States and certain other countries. The Licensed Marks are being used pursuant to a license agreement with the Institute.

All rights reserved. © Copyright 2026 Corelight, Inc.