EXTRAHOP

2025 ExtraHop Global
Threat Landscape Report

The Growing Threat of Lateral Movement

Table of Contents

The Shift That's Redefining Cybersecurity

If the cybersecurity industry has learned anything in recent years, it's this: Modern cyberattackers have mastered the art of infiltration.

Defenses have historically focused on the perimeter, primarily trying to keep attackers out. But as digital ecosystems have expanded and attackers have grown more sophisticated, it's become clear that the battle must be fought within the network.

Once inside, cyberattackers have a wide expanse to escalate privileges, establish persistent footholds, and locate high-value assets with minimal resistance.

Consider what ransomware groups like Scattered Spider are doing today. They're increasingly **leveraging highly sophisticated social engineering techniques—like credential and session cookie theft—and deploying multi-factor authentication (MFA) attacks to gain initial access** into their victims' corporate environments, then moving across the network to paralyze core business functions and stealing vast quantities of data.

The group's high-profile attacks in 2025 included major intrusions against UK retailers like Marks & Spencer and Co-op, causing an estimated $350 million in financial damages, as well as a significant **breach of Qantas Airways that compromised 5.7 million customer records**.

This raises the crucial question: What if these threat actors could have been caught as they started to move laterally after compromising a given system?

Lateral movement—the process by which attackers navigate the internal network to inventory assets on the network, escalate access privileges, and extract valuable credentials and data—is notoriously difficult to detect because it often mimics legitimate network activity, seamlessly blending in with ordinary, everyday traffic.

Because these threats fly under the radar, what might have been a small compromise often turns into enterprise-wide disruption, resulting in system shutdowns, sensitive data exposure, breach notifications, regulatory fines, and recovery costs that can stretch into millions of dollars.

Modernizing cybersecurity defenses begins with understanding how an attacker's ability to move laterally across a network escalates the impact of a breach. In this context, the **2025 ExtraHop Global Threat Landscape Report** serves as a critical resource, highlighting trends that detail the consequences, opportunities for detection, and key challenges facing security teams in the fight against unchecked lateral movement.

The Price of Undetected Lateral Movement

Lateral movement acts as a force multiplier for threat actors, enabling them to systematically discover and compromise critical systems across the network, **driving up ransom demands, and ensuring prolonged operational downtime**. By silently reaching high-value data and core infrastructure, attackers ensure their hold over the organization is comprehensive, increasing their leverage and making containment exponentially harder.

RECORD RANSOM PAYMENTS

The average ransom payment is now $3.6 million, roughly a million dollars more than the previous year's average payment.

This trend is driven by an unprecedented rise in mega-payments: The percentage of victims paying over $25 million has quadrupled, jumping from 1.2% last year to 5.2% this year.

Once inside the network, **unrestricted lateral movement grants threat actors the necessary time to remain fully undiscovered** while they methodically explore, compromise backups, and finally seize the organization's true "crown jewels," forcing massive, non-negotiable payouts.

CRIPPLING DOWNTIME

Organizations (55%) experience an average of 37 hours of downtime due to security incidents—more than a day and a half of operational paralysis. Nearly a third of organizations have reported downtime extending beyond two days.

Extended downtime, often the result of attackers reaching critical systems through lateral movement, can also affect profits and losses, impacting revenue, productivity, and customer trust. All that attackers need to make it happen is to gain a foothold and to blend in.

THE AVERAGE
ransom payment
WAS MORE THAN
$3.6 million

In 2025, Jaguar Land Rover had to shut down its global IT infrastructure following a major cyber incident that resulted in major **disruptions at key manufacturing sites**.

From Intrusion to Total Compromise

What starts as a small breach can quickly escalate. By the time that defenders notice anything unusual, the attack has often evolved, intensified, and broadened in scope, often to the point of no return. The key to preventing this outcome is thoroughly understanding the root causes of failure and addressing those vulnerabilities early on.

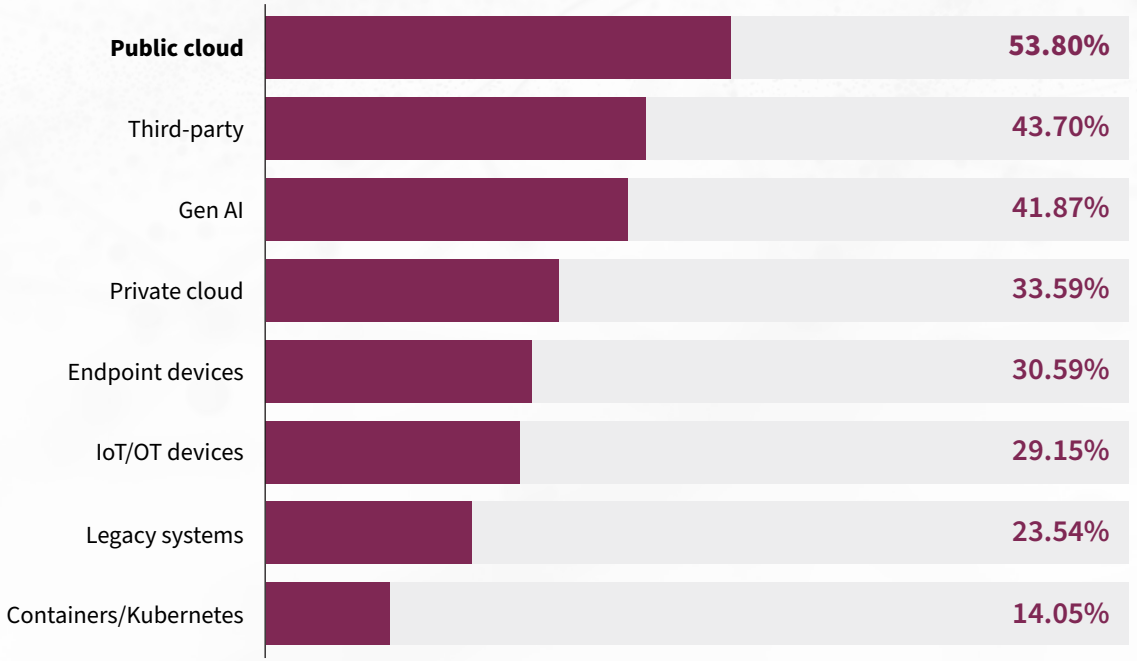
COMPLEXITY CREATES VISIBILITY GAPS

The fundamental design flaw of modern IT—its patchwork architecture, sprawling complexity, and fragmented visibility—makes an organization inherently vulnerable to cyber threats.

When security leaders pinpoint the most dangerous attack surfaces, they name the most complex and interconnected components of this environment: public cloud technologies (53.8%), third-party services and integrations (43.7%), and new vectors like Gen AI applications (41.9%).

The sheer complexity and dynamic nature of cloud-native configurations, integrated partner systems, and API-driven application chains shatter a security team's ability to maintain a complete picture—or even get eyes on them crossing over the perimeter.

Once an attacker gains a foothold, they further exploit this visibility gap. They are able to pivot seamlessly from one host to another, leveraging default trust relationships and internal connection paths. This makes it nearly impossible for security systems to distinguish malicious activity from normal operations, guaranteeing the attack can spread rapidly, virtually undiscovered.



It’s Easy to Hide in Plain Sight

According to our research, attackers are increasingly leveraging compromised credentials (12.2%) as an initial point of entry.

Once inside, those credentials also mean they don’t have to “hack” their way through the rest of the network; they simply log in and immediately begin traversing the network, looking like someone who is meant to be there. This technique transforms a single compromised account into an undetectable, internal threat actor, enabling unfettered lateral movement.

Threat actors are using a multitude of other methods to cover their tracks, all designed to ensure their lateral movement goes undetected.

These include:

Leveraging encrypted channels

Threat actors leverage encrypted channels to cloak their malicious activity, so they can bypass security monitoring systems and stealthily conduct key attack phases like malware delivery and data exfiltration by making their activities appear as legitimate network communications.

Executing living-off-the-land (LOTL) attacks

They use built-in tools like PowerShell, Windows Management Instrumentation (WMI), and Process Executor (PsExec) to avoid detection that would be triggered by introducing new, easily flagged files.

Abusing trusted protocols

They also leverage Remote Desktop Protocol (RDP), Server Message Block (SMB), and Lightweight Directory Access Protocol (LDAP) to move laterally under the guise of routine operations.

Disabling logging and EDR/SIEM alerts

Threat actors tamper with audit trails and security tools to erase footprints, ensuring that security and incident response (IR) teams have a tougher time during the recovery process.

Time Is on the Attacker's Side

Once inside a network, attackers linger—often for weeks at a time.

Our research found that, on average, adversaries maintain undetected access for nearly two weeks before launching a ransomware attack. Sectors with vast digital ecosystems, such as government and education, face even more risk, with average dwell times of 7 and 5 weeks, respectively.

During this period of stealth, adversaries methodically map the entire network, identify high-value data, steal from users, disable security tools, and position themselves for maximum impact. They then move with lightning speed and surgical precision to simultaneously compromise key systems, turning their dwell time into guaranteed and unrecoverable damage.

For attackers, this time is gold. Our report found that nearly a third of respondents (30.6%) only recognized they were being targeted by ransomware during or after data exfiltration had already begun. At that point, recovery becomes not just difficult, but often impossible.

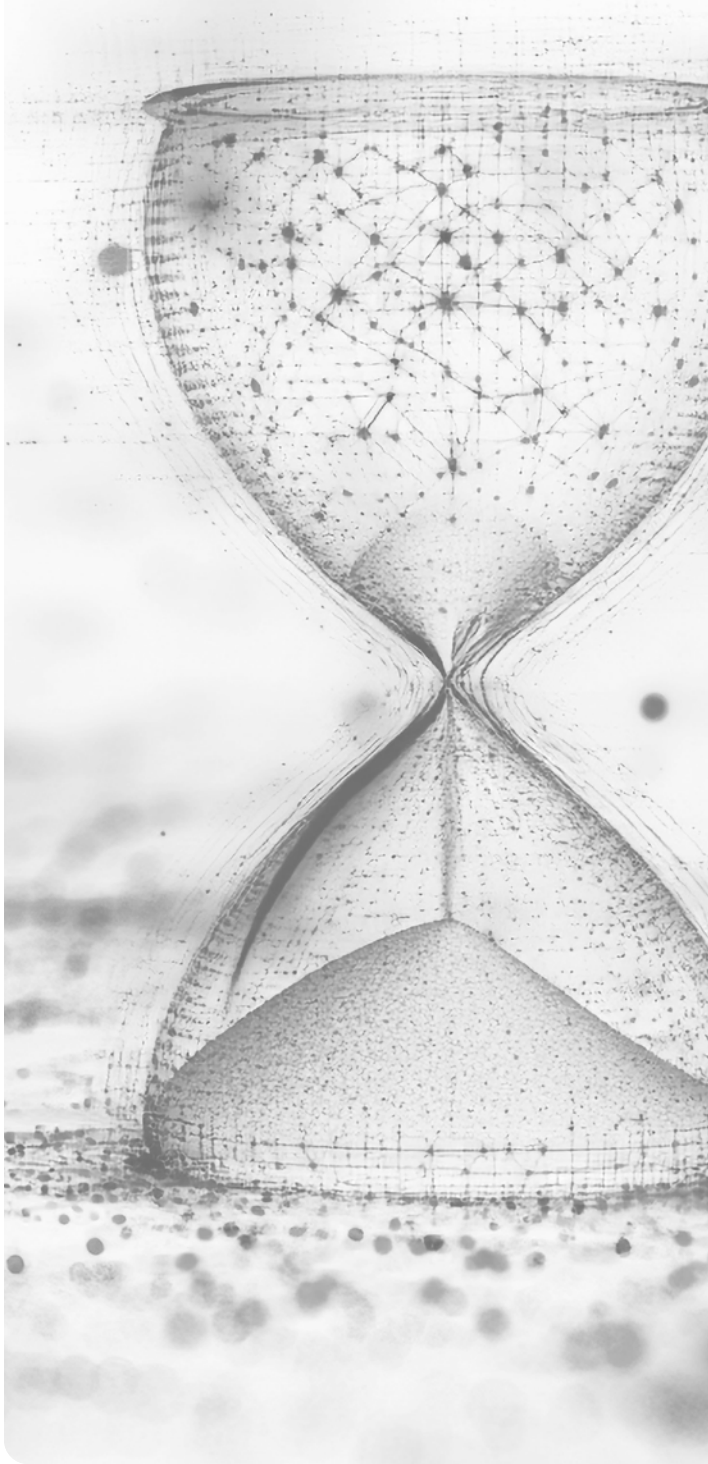
By detecting lateral movement earlier in the attack cycle, organizations can shrink adversaries' operational windows and circumnavigate the most severe outcomes.

SECURITY TEAMS CAN'T KEEP UP

Security teams are racing against the clock, but keep coming up short.

Our findings show that an organization takes an average of two weeks to respond to and contain a security alert, from initial detection to complete resolution. In critical sectors, like government and transportation, that window extends to three weeks.

These delays give attackers ample time to move laterally. The longer it takes to contain a given threat, the more damage that adversaries can inflict behind the scenes.



The Challenge for Security Teams Lies in the Visibility Breakdown

Visibility lies at the heart of the lateral movement detection challenge. When asked what's preventing security and IT leaders from responding quickly to threats, limited insight into the environment was ranked as the primary barrier.

When visibility breaks down, attackers gain ground, moving laterally, escalating incidents, and finding ways to persist.

4 WAYS ATTACKERS GO UNDETECTED

1

They bypass SIEM and EDR tools

Security information management (SIEM) platforms and endpoint detection and response (EDR) can't see into the east-west corridors of your network. Anything traveling within is a blindspot. Attackers take advantage of these gaps, moving through unmonitored spaces to perpetuate credential abuse and to ensure that their lateral movement escapes detection.

2

They hide behind encrypted communications

Adversaries also hide behind encrypted communications to evade detection. This leaves security teams unable to inspect the payload, meaning they can only see the existence of the communication, not its true intent or content.

3

They mask their malicious operations with standard network protocols

Threat actors exploit the inherent trust placed in standard network protocols to successfully camouflage their activities. By tunneling malicious commands and data within the expected framework of common protocols like DNS, HTTP, or SMB, they can make their traffic virtually indistinguishable from routine network activity.

4

They know their path can't be traced

When attackers blend in on networks, security teams often ask themselves, "How did the culprit get here?" and "What vulnerabilities did they exploit, and what were the downstream effects?" This fragmentation makes it nearly impossible for teams to stitch together the complete chain of events, obscuring the attacker's lateral path, final destination, and the full scope of impact across the environment.

Expanding Visibility to Catch Lateral Movement Early

ExtraHop delivers the comprehensive visibility and high-fidelity detection needed to disrupt lateral movement and activity throughout the entire attack kill chain.

Because attackers operate inside encrypted traffic, pivot between endpoints, and exploit typical protocols, most tools miss these movements entirely, leaving security teams without the evidence they need to investigate, respond to, or contain the threat.

To close these gaps and stop lateral movement, organizations need capabilities built for the realities posed by modern adversaries.

Wire-speed decryption

ExtraHop gives security teams visibility into encrypted communications so they can discern if suspicious activity is truly malicious with 100% certainty.

Deep protocol fluency

With the ability to decode 90+ different enterprise protocols, ExtraHop identifies subtle, anomalous behavior that other tools overlook, unmasking behaviors associated with attacks like LOTL.

Full packet capture

ExtraHop provides a complete forensic record of network activity, enabling teams to confidently respond to and contain a threat, and reconstruct the entire attack with zero-doubt validation, confirming the pivot points, the commands executed, and the high-value data accessed.

The Future of Cyber Defense Starts Inside the Network

Visibility into the network's interior is no longer optional. It's a frontline requirement.

As threat actors only get more and more sophisticated, every organization—regardless of industry, size, or geographical location—is at risk. Their ability to hide lateral movement is accelerating, constantly shrinking the time security teams have to respond.

The key to minimizing impact is to detect that movement early. It's no longer just about eliminating the threat entirely; it's about eliminating the catastrophic outcome. Organizations that recognize this critical shift—from perfect prevention to rapid containment—are better equipped to withstand whatever comes next.

Learn how ExtraHop helps customers like Seattle Children's Hospital detect lateral movement and other early-stage attack behaviors.

About ExtraHop

ExtraHop empowers enterprises to stay ahead of evolving threats with the most comprehensive approach to network detection and response (NDR).

Since 2007, the company has helped organizations across the globe extract real-time insights from their hybrid networks with the most in-depth network telemetry. ExtraHop uniquely combines NDR, network performance management (NPM), intrusion detection (IDS), and packet forensics in a single, integrated console for complete network visibility and unparalleled context that supports data-driven security decisions. With a powerful all-in-one sensor and cloud-scale machine learning, the ExtraHop RevealX™ platform enhances SOC productivity, reduces overhead, and elevates security postures.

Unlock the full power of network detection and response with ExtraHop. To learn more, visit extrahop.com or follow us on LinkedIn.

EXTRAHOP®