ZERO. Networks

RESEARCH REPORT · MAY 2026

THE STATE OF LATERAL MOVEMENT 2026

The Detection Delusion

Security leaders are more confident in endpoint detection than ever. Attackers are moving laterally right past it. Inside the gap between EDR confidence and east-west reality.

> A survey of 287 CISOs and senior security leaders at organizations with 1,000+ employees, conducted April 2026 by an independent third-party research firm.

88%
are confident their EDR would catch an intruder before serious damage

34%
of confirmed lateral-movement incidents were actually flagged first by EDR

16 hrs
median time from initial foothold to domain-admin-level access

EXECUTIVE SUMMARY

Confidence has never been higher. Neither has the cost of being wrong.

Enterprise security has spent a decade — and by our respondents' estimates, an average of 41% of their security tooling budget — building a detection stack around the endpoint. The result is real confidence: 88% of the 287 security leaders we surveyed believe their EDR would detect an intruder before serious damage occurred, and 92% call endpoint detection the backbone of their defense.

Then we asked the 124 respondents whose organizations suffered a confirmed intrusion in the past 24 months what actually happened. In only 34% of confirmed lateral-movement incidents was EDR the control that raised the first alarm. Sixty-four percent of breached organizations said attackers moved east-west undetected for three days or longer. The median time from initial foothold to domain-admin-level access was 16 hours — meaning in most cases, the attacker finished spreading before the first triage meeting.

The mechanism behind the gap is unglamorous: attackers stopped bringing malware to the fight. 71% of reported incidents relied primarily on legitimate administrative tools and protocols — RDP, SMB, WMI, PsExec, PowerShell — that endpoint agents are explicitly trained to treat as normal. Detection tools hunt for the abnormal. Lateral movement is engineered to look routine.

The market is responding. Cyber insurers now interrogate lateral-movement controls at renewal (57% of respondents), and 62% of security leaders say they are actively shifting budget from detection toward containment — with network segmentation the single most-cited 2026 investment priority. The delusion isn't that detection matters. It's that detection alone was ever going to be enough.

92%
call EDR the "backbone" of their security architecture

64%
of breached orgs saw attackers move laterally undetected for 3+ days

71%
of incidents relied on legitimate admin tools, not malware

62%
are shifting budget from detection toward containment in 2026

FINDING 01

Peak confidence: the endpoint has become an article of faith

A decade of EDR and XDR investment has produced a security culture that trusts the endpoint the way earlier generations trusted the firewall. Nearly nine in ten leaders believe their EDR would catch an intruder before serious damage, and confidence rises with spend: among organizations allocating over half their tooling budget to detection, it reaches 94%.

Confidence in endpoint detection

% OF ALL RESPONDENTS AGREEING WITH EACH STATEMENT · N=287

WHY THIS MATTERS

Confidence shapes budgets. Respondents allocate an average of 41% of security tooling spend to detection and response — more than triple what they allocate to limiting where an attacker can go once inside (13%). When nine of ten leaders believe the endpoint will catch it, the network's east-west corridors stay open by default.

> ***"Every vendor QBR shows me mean-time-to-detect going down. None of them show me how far an attacker gets while we're detecting."***
>
> CISO, RETAIL, 10,000+ EMPLOYEES

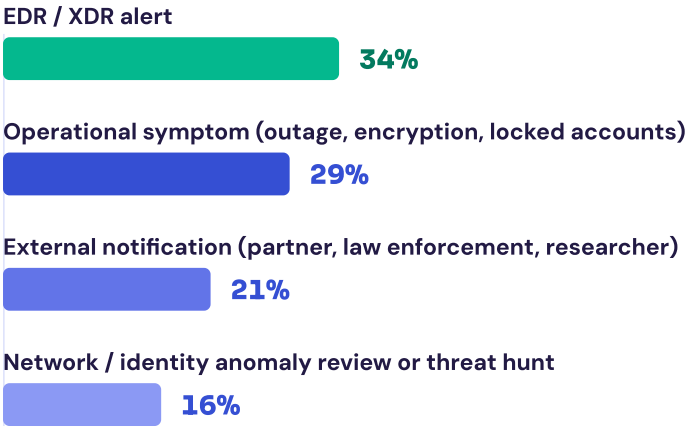
FINDING 02

Breach reality: EDR raised the first alarm in only a third of incidents

Among the 124 respondents whose organizations experienced a confirmed intrusion in the past 24 months, the record diverges sharply from the confidence data. EDR was the first control to flag lateral movement in just 34% of incidents. More often, the tell came from somewhere else entirely — an unexplained outage, a file-share encryption event, or a third party calling to ask why your infrastructure was attacking theirs.

How lateral movement was actually discovered

% OF BREACHED ORGANIZATIONS, BY FIRST SOURCE OF DETECTION · N=124



WHY THIS MATTERS

Half of breached organizations (29% + 21%) learned about lateral movement from consequences, not controls. By the time an outage or an outside phone call is your detection mechanism, containment has already failed — 64% of breached respondents said attackers moved undetected for three days or longer, and the median foothold-to-domain-admin time was just 16 hours.

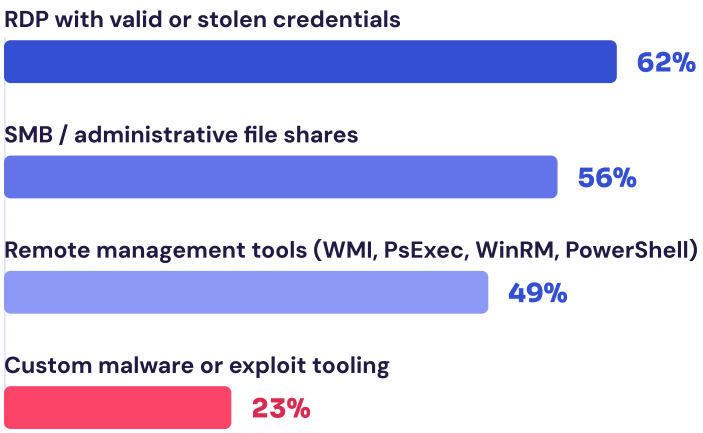
FINDING 03

Attackers stopped bringing malware. EDR is still looking for it.

The uncomfortable engineering truth beneath the gap: modern lateral movement rarely involves anything an endpoint agent is built to condemn. In 71% of reported incidents, attackers moved primarily over legitimate administrative channels — the same RDP sessions, SMB shares, and remote-management tooling that IT uses every day. Signature-clean, behavior-plausible, and invisible until the blast radius makes it obvious.

Channels used for lateral movement in reported incidents

% OF BREACHED ORGANIZATIONS REPORTING EACH CHANNEL · MULTIPLE RESPONSES · N=124



WHY THIS MATTERS

You cannot tune your way out of this. Blocking RDP and SMB behaviorally means blocking IT itself — which is why these protocols stay open and why 71% of incidents ride them. The alternative isn't better detection of legitimate tools; it's making those channels unusable to anyone without verified identity, via segmentation and MFA enforced at the port level.

> ***"The ransomware crew used the exact same remote admin path our own help desk uses. The EDR saw a sysadmin having a busy night."***
>
> VP OF SECURITY OPERATIONS, MANUFACTURING, 5,000–10,000 EMPLOYEES

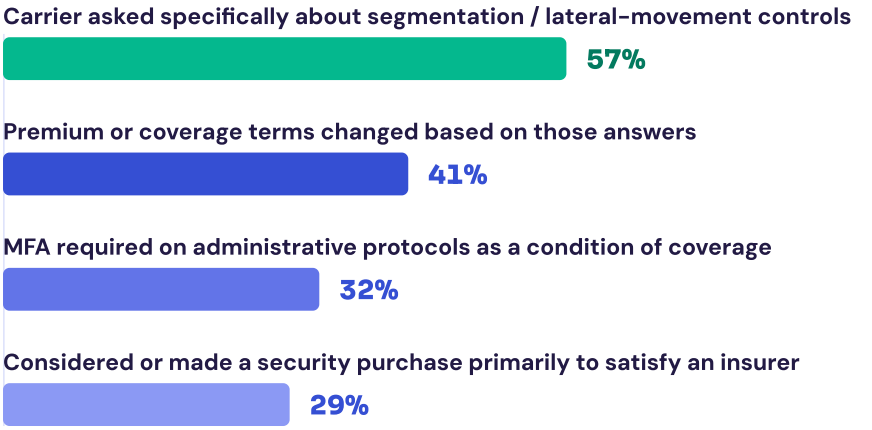
FINDING 04

The insurance market has already priced in the delusion

Cyber insurers see loss data, not marketing. And their underwriting questions have shifted accordingly: away from "do you have EDR?" — nearly everyone does — and toward what happens after the endpoint misses. 57% of respondents say their carrier now specifically probes segmentation and lateral-movement controls at renewal, and for many, the answers are showing up in the premium.

Cyber insurance pressure on lateral-movement controls

% OF ALL RESPONDENTS REPORTING EACH AT THEIR MOST RECENT RENEWAL · N=287



WHY THIS MATTERS

Insurance requirements are becoming a de facto security architecture standard for the mid-market. When a third of organizations must enforce MFA on admin protocols to stay covered — something traditional tools were never designed to do at the network layer — the renewal questionnaire is quietly writing next year's security roadmap.

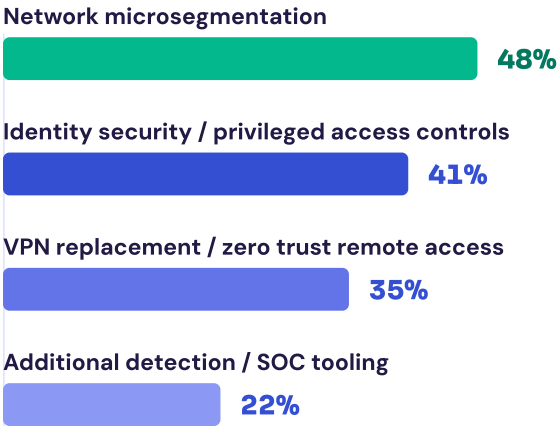
FINDING 05

The quiet rebalance: budgets are moving from detection to containment

Security leaders aren't abandoning detection — they're re-weighting it. 62% say they are actively shifting budget from detection and response toward containment and prevention for 2026–2027. Asked where that money goes, network segmentation tops the list, cited by nearly half of all respondents — ahead of identity security and well ahead of another detection layer.

Top planned containment investments, 2026–2027

% OF ALL RESPONDENTS RANKING EACH A TOP-2 PRIORITY · N=287



WHY THIS MATTERS

This is the first year in our respondents' recollection that a containment technology out-ranked new detection spend. The logic is arithmetic: if the median attacker reaches domain admin in 16 hours and detection fires first only 34% of the time, the highest-leverage dollar is the one that removes the path — not the one that watches it.

> ***"We finally accepted that we can't out-alert a 16-hour attack window. Now the question I ask every vendor is: what does the attacker's next hop look like when it simply doesn't connect?"***
>
> CISO, REGIONAL BANK, 1,000–5,000 EMPLOYEES

WHAT THIS MEANS

Five moves to contain what detection misses

1

Measure dwell math, not alert volume.

Put your own numbers next to the survey's: how long from foothold to domain admin in your last red-team exercise, and what fired first? If detection wins only a third of the time, budget like it.

2

Treat admin protocols as the attack surface they are.

RDP, SMB, and remote management carried 71% of reported incidents. Close privileged ports by default and gate them behind network-layer MFA — verification EDR can't provide and attackers can't imitate.

3

Rebalance the 41/13 split.

Respondents spend 41% of tooling budget on detection and 13% on containment. You don't need parity — you need enough segmentation that a missed detection is an incident, not an enterprise-wide event.

4

Pass your insurer's questionnaire before they send it.

57% of carriers now probe lateral-movement controls. Deploying segmentation and MFA on admin access before renewal converts a premium penalty into negotiating leverage.

5

Demand containment that deploys in weeks, not years.

Segmentation earned a stalled-project reputation the manual way. Automated, agentless approaches now reach full production in about 30 days — make deployment speed a hard requirement, not a hope.

METHODOLOGY

About this study

This study was conducted in April 2026 by an independent third-party research firm on behalf of Zero Networks. Data was collected via a structured online survey supplemented by 18 qualitative interviews with a subset of respondents.

Sample

287 senior security leaders: CISOs (44%), VPs/heads of security or security operations (33%), directors of network or infrastructure security (23%)

Organization size

1,000+ employees required; 34% from organizations with 10,000+ employees

Geography & industries

North America (61%) and Europe (39%); financial services, healthcare, manufacturing, technology, retail, and public sector

Collection

Fielded April 6–29, 2026; respondents screened for direct responsibility over detection, network security, or incident response strategy

Key metrics analyzed

- Stated confidence in EDR/XDR detection versus first-source-of-detection in confirmed incidents
- Dwell time and foothold-to-privileged-access intervals in breaches from the past 24 months (breached subset, n=124)
- Lateral-movement channels reported per incident (multiple responses permitted)
- Cyber insurance renewal requirements and premium outcomes tied to lateral-movement controls
- 2026–2027 budget allocation shifts between detection and containment categories

Percentages may not sum to 100 due to rounding or multi-select questions. Breach-experience analyses reflect the 124 respondents reporting a confirmed intrusion within the past 24 months. Quotes are drawn from qualitative interviews and lightly edited for length.

THE ROAD AHEAD

Detection tells you the attack happened. Containment decides how it ends.

The next intrusion at most enterprises will begin the same way the last one did: a valid credential, a legitimate protocol, an endpoint agent watching what looks like a normal Tuesday. What happens in the 16 hours after that is no longer a detection question. It's an architecture question — and in 2026, the leaders in this study are answering it by closing lateral paths before anyone needs to spot them.

Zero Networks makes lateral movement impossible: automated, agentless microsegmentation that reaches full production in about 30 days, network-layer MFA on the privileged ports attackers depend on, and segmented remote access to retire the VPN. Attacks contained. Weekends retained.

Book a demo → zeronetworks.com

GARTNER PEER INSIGHTS 5.0 · GIGAOM RADAR LEADER · SOC 2 TYPE II · GDPR · PCI DSS