The Security Middle Child

How midmarket security teams are managing growth, complexity, and risk

March 2026

intruder

intruder.io

Introduction

The midmarket occupies an uncomfortable position in the security landscape. These are organizations large enough to be attractive targets—with complex digital estates, significant revenue, and valuable data—but not large enough to have the headcount, budget maturity, or tooling sophistication of enterprise security teams. They've outgrown the solutions built for smaller businesses, yet the ones for enterprises weren't designed with them in mind.

Much like middle children, they’re often overlooked—caught between organizations larger and smaller than them. That’s why we call them the security middle child.

To understand what's really going on inside these organizations, we surveyed over 500 senior security decision-makers across the US and UK, spanning fintech, financial services, healthcare, manufacturing, professional services, retail, and SaaS. The picture that emerges is one of growing pressure—91% saw their digital estate grow over the past 24 months, and 42% describe their team as stretched, overwhelmed, or consistently behind. Yet confidence is high—89% say budgets are increasing, and 94% are confident in their ability to catch critical risks before attackers exploit them.

This report sets out to answer:

- Does confidence reflect operational reality?
- What's causing the strain on teams?
- Are the tools teams are investing in solving the right problems?
- Are the right people in the room when these decisions get made?

> **Midmarket companies are being treated as the middle child when it comes to cybersecurity solutions. They are overlooked by vendors focused on Fortune 500s or SMBs, while they are just as important and just as vulnerable to attackers.**
>
> 
>
> **Chris Wallis**
> CEO and Founder of Intruder

Methodology

This report is based on a survey of 502 senior security decision-makers, conducted by Censuswide in February 2026. Questions covered five core themes:

- How digital estate growth is tracking against headcount
- The state of security posture and confidence in managing critical risks
- The maturity of cybersecurity processes and tech stacks
- Where budgets are headed and how investment priorities are shifting
- How cyber risk is being discussed and escalated within organizations

Job roles	Cybersecurity Managers / Directors / Leads / VPs, CISOs (or CISO-equivalent)
Company size	• 400 - 6,000 employees
Annual revenue ($)	• 50M - 100M (25%) • 100M - 500M (43%) • 500M or over (32%)
Geographies	• US (60%) • UK (40%)
Sectors	• Financial Services (14%) • Fintech (14%) • Healthcare (14%) • Manufacturing (14%) • Professional Services (14%) • Retail (14%) • SaaS (14%)
Security team size	• 2 - 5 (19%) • 6 - 10 (65%) • 11 or more (15%)

Projecting confidence, but is it justified?

Leaders project optimism

Midmarket security leaders defy the stereotype of an overworked, underfunded team. 89% say that budgets are increasing. 70% say that headcount has kept pace with estate growth. 94% say they're confident in their ability to identify and remediate critical risks before attackers exploit them—51% very confident.

Operators express concern

Dig deeper and that confidence is unevenly distributed. 65% of C-level respondents say they're very confident in their ability to catch critical threats. That figure drops to 55% among directors, 46% among senior managers, and 36% among middle managers.

An exposure window that's too long

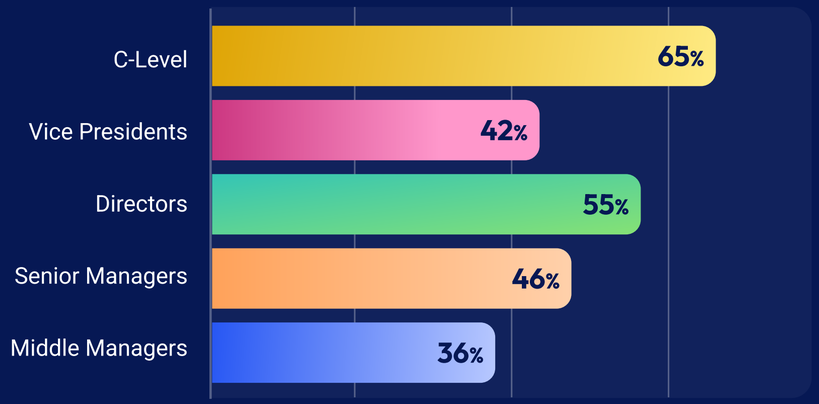
The skepticism of those closer to the work appears warranted. 51% of respondents say it would take approximately a week to assess their exposure to a critical zero-day. In a threat landscape where exploitation can follow disclosure within 24-48 hours, a week is too long.

Unjustified confidence

That's not the only gap. 28% of respondents cite lack of visibility into what's exposed as a top operational challenge, 18% are tracking internet-facing assets manually, and 9% are running multiple cloud environments without a unified view of security risk across them. It suggests that for a significant portion of midmarket teams, confidence isn't rooted in visibility—it's grounded in not knowing what they're missing. For attackers, that's exactly where opportunity lies.

"Very confident" in ability to identify and remediate critical threats

% of respondents by seniority

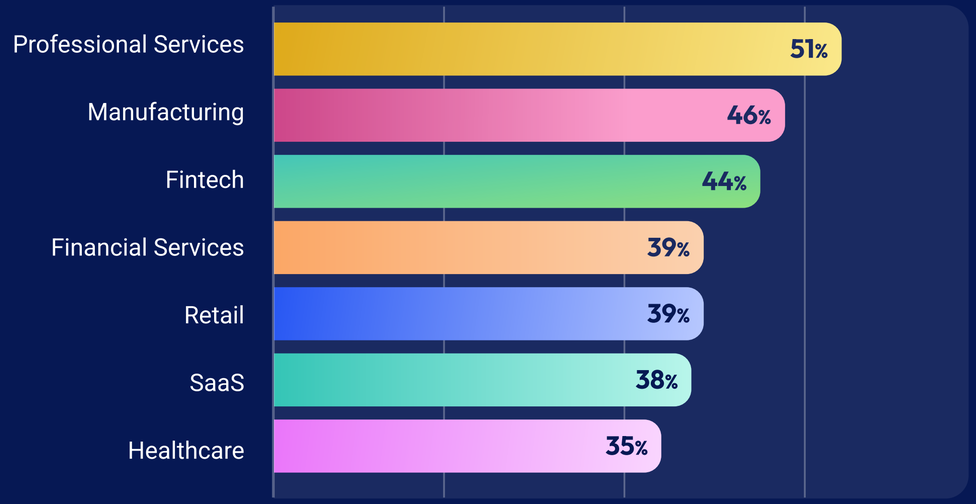


Growing estates, stretched teams

42% of teams are stretched, overwhelmed, or consistently behind

Percentage of teams reporting strain, by sector

Stretched, overwhelmed, or consistently behind.
Overall average (42%)



Digital estates are growing, so are most teams

Midmarket digital estates are expanding fast. 91% of respondents say their estate grew over the past 24 months—38% significantly so. For 70% of organizations, headcount kept pace with estate growth—for 30% of those, it grew faster. For 17%, however, headcount grew more slowly, and for nearly 10% it stayed flat.

Growing teams are still stretched

Despite growing headcount, 42% of teams report being under strain: 21% describe themselves as stretched but coping, 11% as overwhelmed and reactive, and 9% as consistently behind and exposed. Professional services and manufacturing report the highest strain (51% and 46%), while SaaS and healthcare are coping better (38% and 35%).

What's driving the strain? The top challenges teams cite point to operational complexity from expanding estates: 28% lack visibility into what's exposed, 26% say they're navigating too many tools, and 24% struggle with poorly prioritized alerts.

The operational burden is only part of it. 34% cite limited resources and competing priorities as a top challenge—suggesting teams are being stretched not just by what they need to secure, but by how many directions they're being pulled while doing it.

Treating the symptom, not the cause

36% of respondents acknowledge their security posture hasn't scaled appropriately with digital estate growth. For 14%, that gap won't close for at least another six months. However, only 17% are prioritizing headcount this year. The dominant investment priorities are AI and automation (49%) and adding new solutions (33%)—suggesting security leaders are reaching for technology to compensate for people. The data suggests this isn't working: 44% describe a stack that is either outgrown or fragmented.

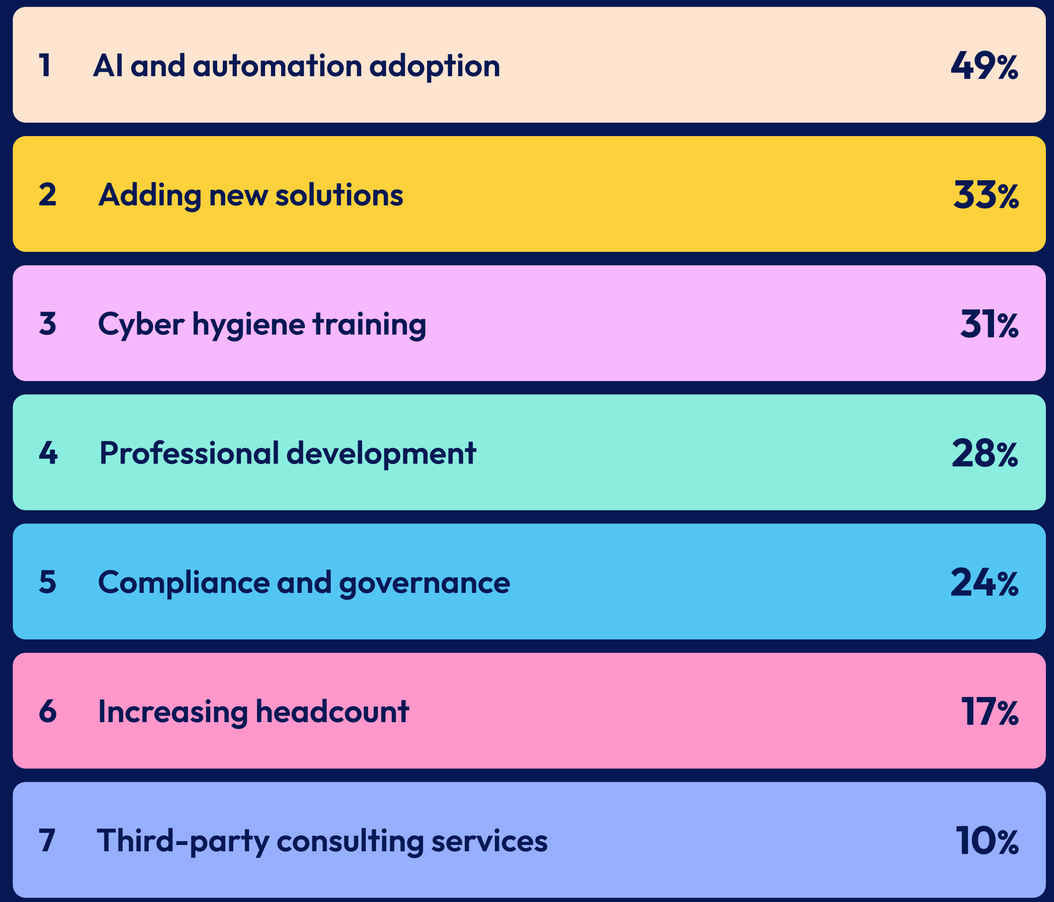
Security investment isn't evenly distributed

The pressure isn't evenly distributed. In healthcare, only 51% kept headcount at pace with their digital estate, and 26% grew more slowly. In SaaS, that figure rises to 86%, with only 10% growing more slowly. The gap is striking in healthcare given the stakes involved.

There's a geographic dimension too. US organizations are more likely to have grown headcount faster than their digital estate (36% vs 22% in the UK). A similar pattern plays out on budget: US organizations are more likely to be significantly increasing security spend (39% vs 30%).

Where security leaders are focusing investment in 2026

% of respondents



More tools, less clarity

44% of teams have either outgrown their stack or stitched it together from point solutions

A fragmented security tech stack

44% of teams have either outgrown their stack or stitched it together from point solutions that don't provide a unified view. This has a cost: 26% cite navigating too many security tools as a top challenge, 24% cite too many alerts with poor prioritization, and 20% cite the inability to measure and report on cyber hygiene. The stack isn't just complex—it's actively getting in the way. And with 33% planning to add more solutions this year, the fragmentation is likely to deepen.

Cloud security spans all sectors

Cloud Security Posture Management (CSPM) is the only tool appearing across every sector. For such a young category to reach universal adoption shows how rapidly cloud has become foundational in the midmarket. Healthcare leads CSPM adoption at 68%—well ahead of the next-highest sector at 56%—likely reflecting how regulatory obligations like HIPAA are driving cloud security maturity.

The AI question

41% report using AI pentesting, and it appears in the top five most-adopted tools for fintech, manufacturing, and retail. Given the category only emerged 12-18 months ago, it's unclear whether teams are using true AI pentesting or applying the term more loosely. But the intent is clear: nearly half (49%) cite AI and automation as their top investment priority for 2026, suggesting security leaders are looking to AI to help them do more with less.

That said, AI pentesting only breaks into the top five for organizations with $500M+ revenue—implying it’s currently most accessible to companies with the most resources. Adoption also increases with team size: 49% of organizations with 11+ security staff report using it, versus just 25% of teams with 2-5 people. This raises a question: for the smallest, most stretched teams AI is supposed to help, do existing solutions risk adding complexity rather than relieving pressure?

Top 5 tools by industry

% adoption by sector

Financial services

Cloud Security Posture Management (CSPM)	51%
Data Security Posture Management (DSPM)	51%
Vulnerability Management (VM)	50%
Security Information & Event Management (SIEM)	44%
Web Application Firewall (WAF)	43%

Fintech

Cloud Security Posture Management (CSPM)	56%
Web Application Firewall (WAF)	53%
AI Penetration Testing	47%
Security Information & Event Management (SIEM)	43%
Attack Surface Management (ASM)	40%

Healthcare

Cloud Security Posture Management (CSPM)	68%
Application Security (SAST/DAST)	50%
Web Application Firewall (WAF)	49%
Endpoint Detection & Response (EDR/XDR)	49%
Security Information & Event Management (SIEM)	49%

Manufacturing

Security Information & Event Management (SIEM)	62%
Cloud Security Posture Management (CSPM)	49%
Vulnerability Management (VM)	46%
Data Security Posture Management (DSPM)	46%
AI Penetration Testing	46%

Professional services

Cloud Security Posture Management (CSPM)	56%
Endpoint Detection & Response (EDR/XDR)	49%
Web Application Firewall (WAF)	47%
Security Information & Event Management (SIEM)	47%
Data Security Posture Management (DSPM)	44%

Retail

Web Application Firewall (WAF)	54%
Cloud Security Posture Management (CSPM)	51%
Endpoint Detection & Response (EDR/XDR)	49%
AI Penetration Testing	48%
Security Information & Event Management (SIEM)	45%

SaaS

Cloud Security Posture Management (CSPM)	56%
SaaS Security Posture Management (SSPM)	56%
Data Security Posture Management (DSPM)	49%
Web Application Firewall (WAF)	48%
Application Security (SAST/DAST)	46%

Investing in the wrong places

28% cite lack of visibility into what's exposed as a top challenge—yet Attack Surface Management (ASM) and Continuous Threat Exposure Management (CTEM), the two solutions most directly designed to address it, rank 10th and 13th for adoption. It implies that teams are investing in solutions that don't map to their most pressing problems, while the tools that would actually close the visibility gap remain underdeployed.

Retail and professional services struggle with visibility

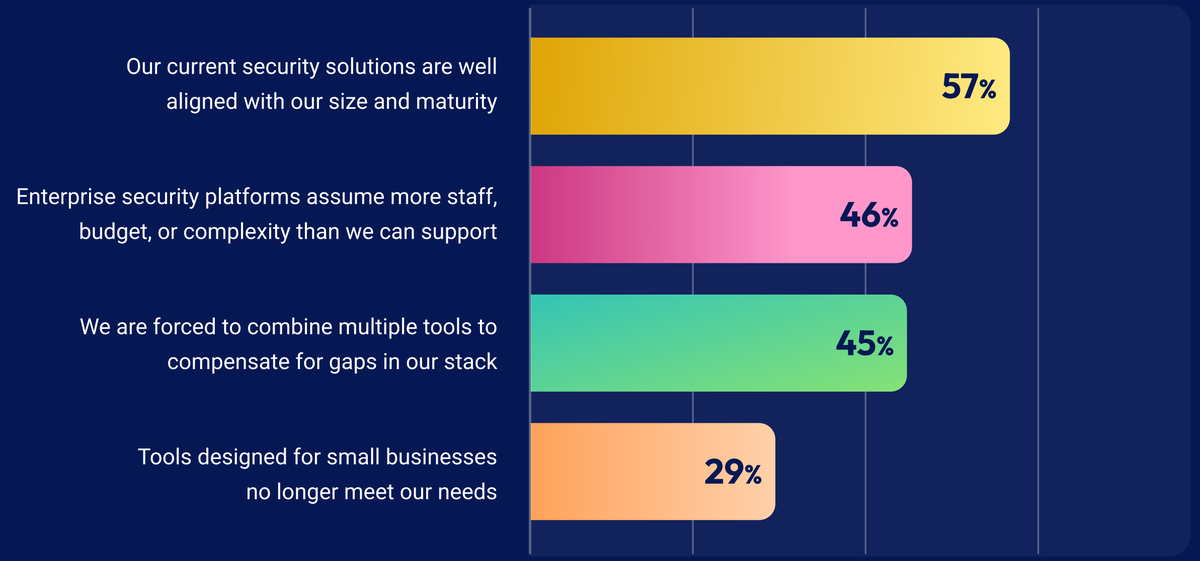
Retail organizations cite lack of visibility into what's exposed as a top challenge more than any other sector (38%), yet only 27% use CTEM. Professional services tells a similar story: 35% cite visibility as a top challenge, but ASM adoption sits at just 26%, the lowest of any sector.

The tools don’t fit

Underpinning all of this is a vendor market that was never really built for the midmarket. 46% say enterprise platforms assume more staff, budget, or complexity than they can support. 29% say SME tools no longer meet their needs. Midmarket teams aren't failing to choose the right tools—the right tools largely haven't existed for them.

46% of respondents say enterprise platforms assume more staff, budget, or complexity than they can support

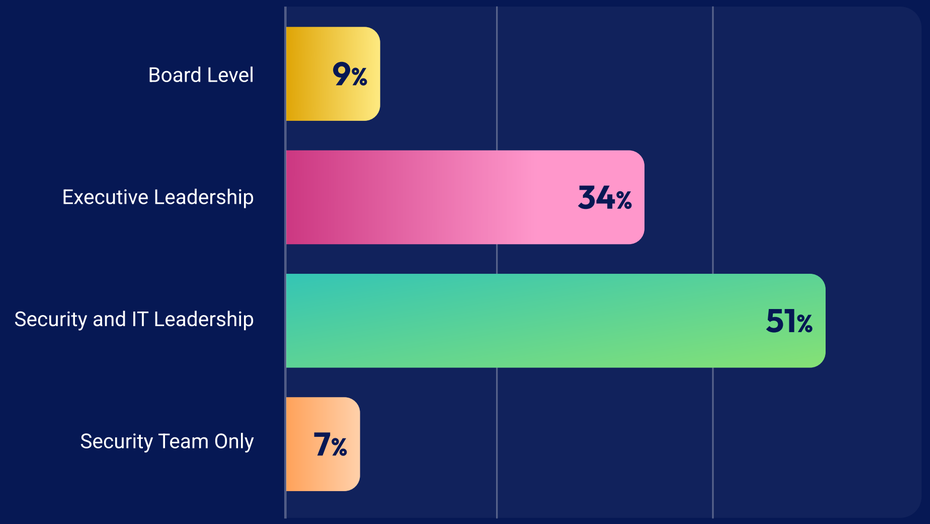
How midmarket security leaders view the vendor market



Cyber risk isn’t reaching the boardroom

UK organizations are more than twice as likely as US counterparts to discuss cyber risk with the board

Where cyber risk is discussed in midmarket organizations



A technology problem, not a business one

Despite growing digital estates and mounting signs that security posture is struggling to keep pace, cyber risk remains largely below the boardroom. Only 9% of organizations discuss it at board level. 34% reach executive leadership. The majority (51%) keep it at security or IT leadership only, and 7% confine it to the security team alone. Without board-level visibility, there's limited organizational pressure to address disconnects between digital estate growth and security capacity.

Bigger teams, more board visibility

16% of organizations with security teams of 11 or more discuss cyber risk at board level, compared to 9% overall.

Evidence of the regulatory effect?

UK respondents are more than twice as likely as their US counterparts to report board-level discussion (14% vs 6%), a gap that may reflect the influence of UK regulatory frameworks.

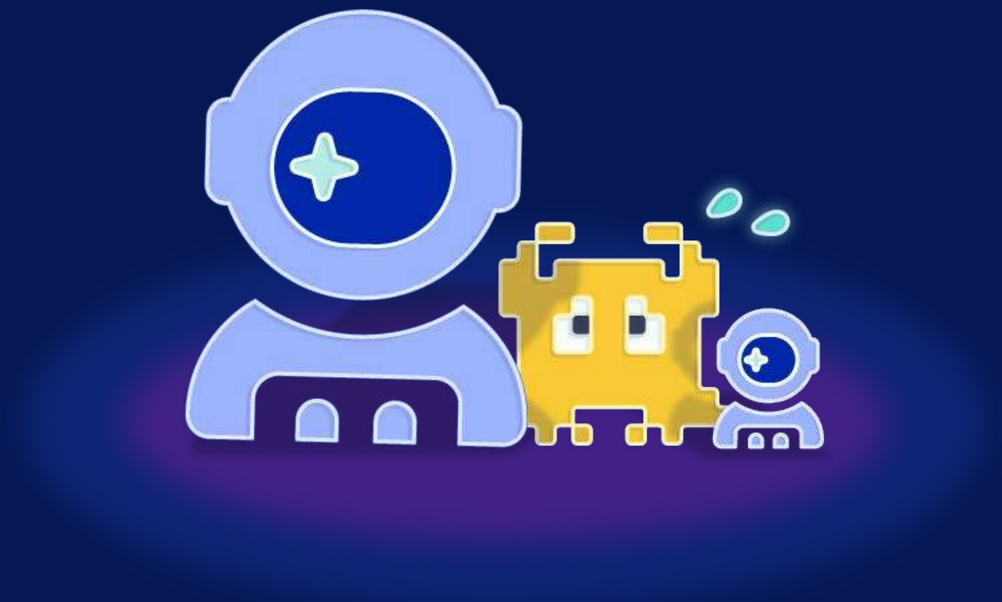
The challenge of being caught in the middle

The data in this report doesn't point to a single problem—it points to four compounding ones. Estates growing faster than teams. Confidence highest where visibility is lowest. Stacks that are fragmented and getting more so. And a conversation about all of it that isn't reaching the people who need to hear it.

These problems reinforce each other. A stretched team reaches for more tools. More tools create more noise. More noise makes it harder to see what's actually exposed. And without board-level visibility, there's no organizational pressure to change course.

The midmarket security gap isn't a spending problem—budgets are growing. It isn't an awareness problem—leaders know the challenges they face. It's a structural one: the tools available to midmarket security teams were never built for the position they're now in.

Until that changes, the gap between how these teams perceive themselves and how they actually operate will keep widening.



About Intruder

Intruder's exposure management platform helps lean security teams stop breaches before they start by proactively uncovering attack surface weaknesses. By unifying attack surface management, cloud security, and continuous vulnerability management in one intuitive platform, Intruder makes it easy to secure your entire infrastructure—from apps and APIs to cloud accounts and employee devices. Designed to cut through the noise and complexity, Intruder enables teams to discover exposed assets, detect misconfigs, prioritize real risks, streamline security workflows, stay compliant, and fix issues fast.

Founded in 2015 by Chris Wallis, a former ethical hacker turned corporate blue teamer, Intruder was selected for GCHQ's Cyber Accelerator and is now protecting over 3,000 companies worldwide.

Start a free trial or book a call with one of our experts at intruder.io

Read our reviews on G2.com