REALVNC RESEARCH REPORT | 2026

Emerging Threats in Remote Access Security

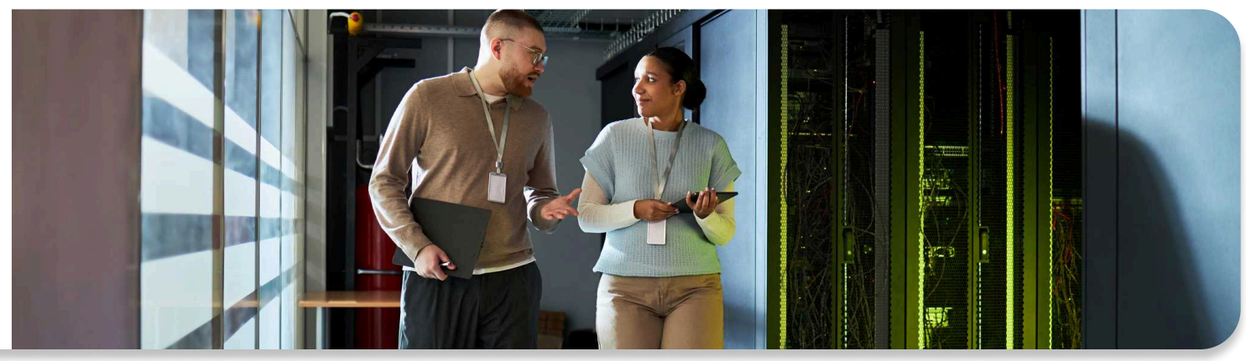
Uncovering the blind spots you can't ignore in the age of AI

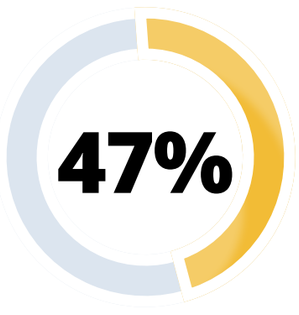
What 323 IT professionals revealed about the threats they fear, the gaps they recognise, and why confidence alone will not protect them.

TABLE OF CONTENTS

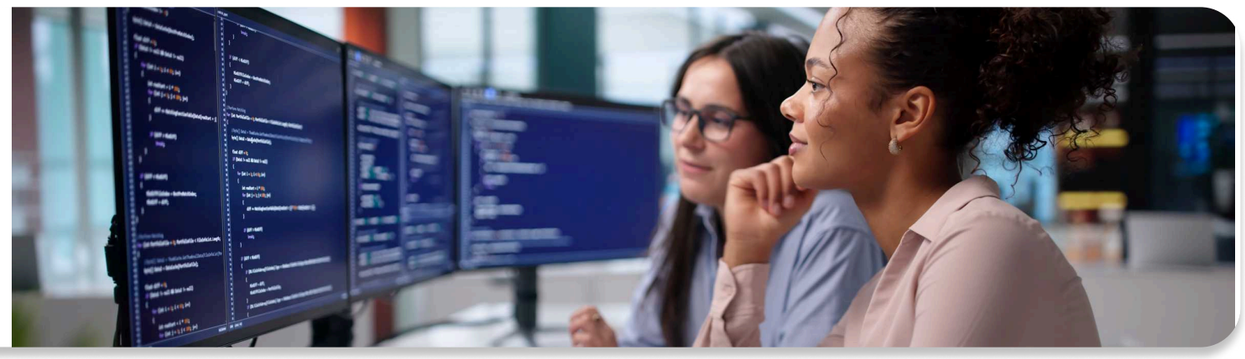
MAIN TAKEAWAYS

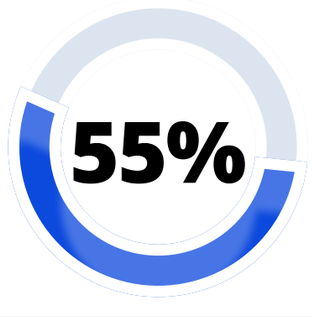
IT professionals surveyed



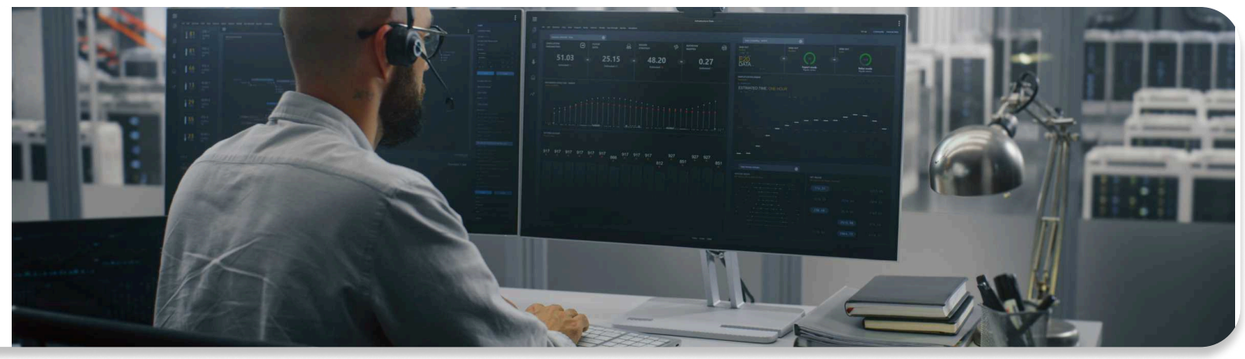


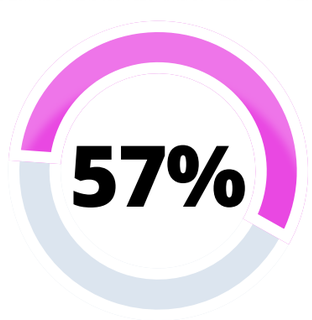
Experienced an incident in the past 24 months



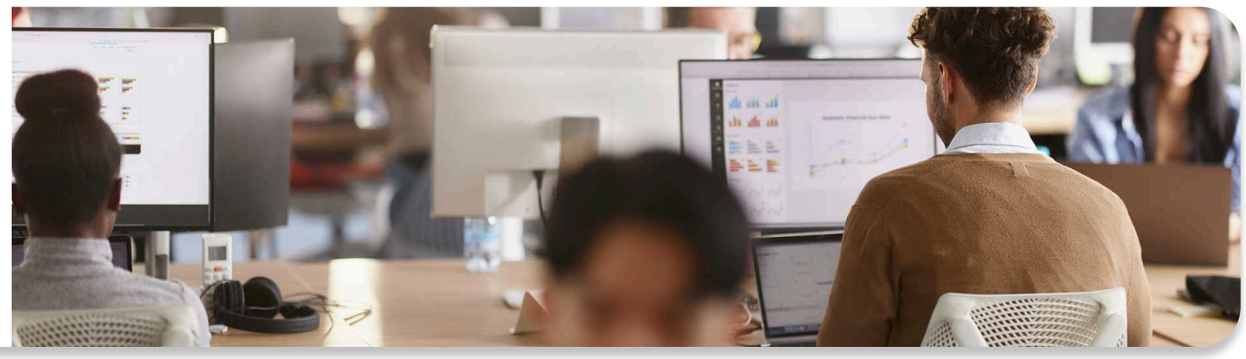


Confident respondents who still experienced breaches





Not confident in their 3-year strategy



EXECUTIVE SUMMARY

There is no denying that the remote access threat landscape is accelerating and becoming more complex every day. Attackers are getting more sophisticated, AI is lowering the barrier when it comes to launching complex campaigns, and the hybrid work era that we're living in has permanently expanded the attack surface.

Against that backdrop, one might expect most IT teams to report heightened anxiety about their security posture.

Many do not. And that gap between confidence and reality is the defining feature of the 2026 remote access security landscape.

RealVNC wanted to go deeper, taking the pulse of the threats that the market is currently facing. To do this, we surveyed 323 IT professionals across seven major industries and five company-size bands. We wanted to understand how organisations perceive, experience, and plan to address emerging threats in remote access security.

The findings are organised around five themes:

1. The threat landscape, as IT professionals actually experience it.
2. The confidence paradox and its relationship to real-world incidents.
3. The gap between intended and implemented security controls.
4. The operational burden that actively prevents security improvement.
5. What the next three years are likely to look like for different segments of the market.

EXECUTIVE SUMMARY

The overconfidence finding is not incidental. It runs through every segment of the survey. It's in every role, every industry, every size band, and it points to a structural problem in how security posture is assessed. Teams are measuring activity, not outcomes. They are counting controls deployed, not testing whether those controls actually hold under real-world conditions.

The picture is not uniform across industries.

- Healthcare faces the highest acute anxiety about future preparedness.
- Finance grapples with tool complexity and a distinctive focus of supply chain risk.
- Technology firms are the highest-incident sector, despite significant AI adoption and genuine security investment.
- Manufacturing is falling behind on infrastructure modernisation.
- Retail and Education are anxious about the future, while also facing budget and bandwidth constraints.

The organisations that will navigate the next three years most successfully will be those that move beyond generic security awareness.

This report presents those differences clearly. And that's because the path forward is not a one-size-fits-all. The organisations that will navigate the next three years most successfully will be those that move beyond generic security awareness. And that move needs to be toward architectures, tools, and vendor partnerships that are matched to their specific threat profile, compliance obligations, and operational constraints.

> 47% of respondents experienced a remote access incident in the past 24 months. Among those who described themselves as very or extremely confident in their security, 55% had still been hit.

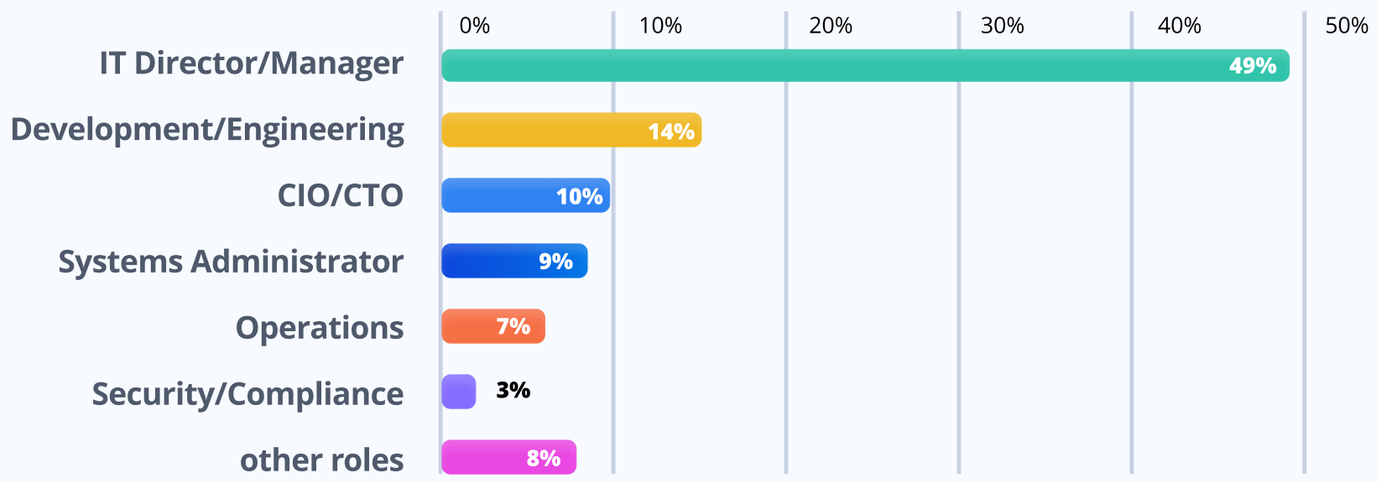
ABOUT THIS RESEARCH

RealVNC commissioned this survey in Q1 2026. The purpose was simple: to understand how IT professionals across industry sectors are perceiving and preparing for emerging threats in remote access security.

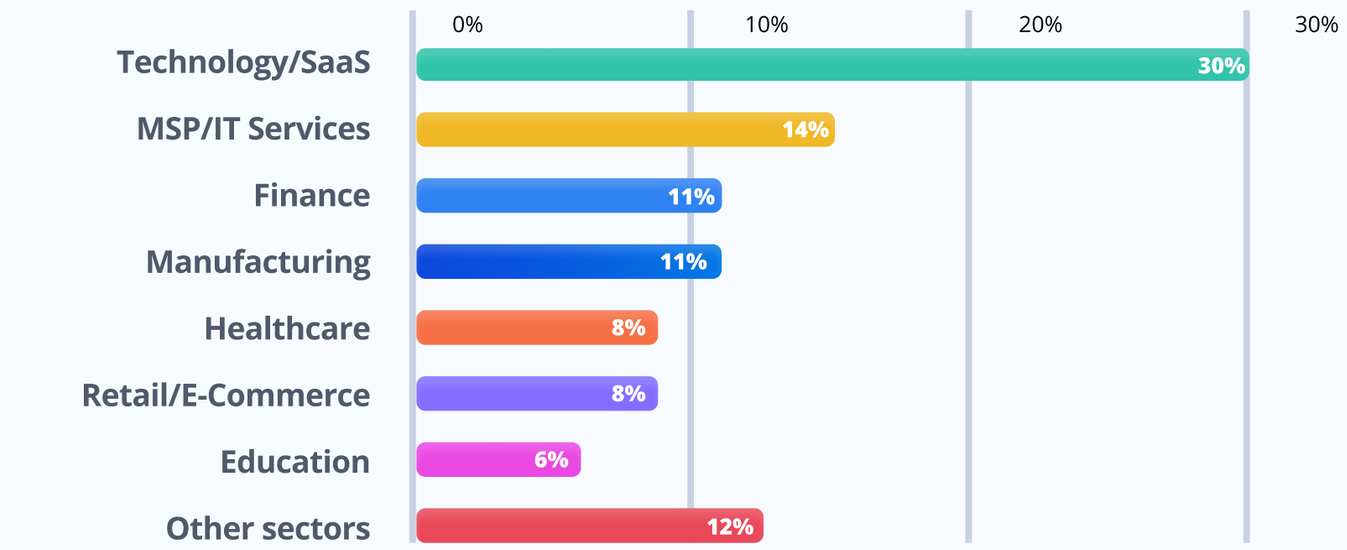
323 qualified respondents, all individuals working in organisations that currently use remote access solutions, completed the survey. These respondents represent a wide range of industries, company sizes, and seniority levels, as seen below.

All findings are based solely on the survey data collected. Percentages are rounded to the nearest whole number. Industry sub-samples are noted where relevant to contextualising the findings. In some cases, graphics show only the most significant findings.

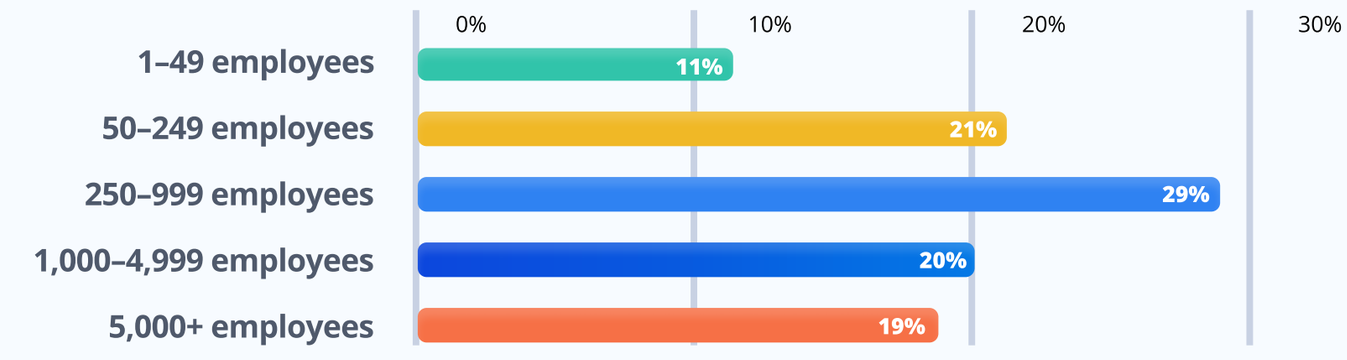
Respondents by role



Respondents by industry



Respondents by company size



CHAPTER 1: THE THREAT LANDSCAPE

Understanding what IT professionals fear in practice, as well as how those fears vary by sector, is the essential foundation for the chapters that follow. The threat landscape of 2026 is not homogeneous. Primary threats vary significantly by industry, driven by their compliance environments, operational models, and the nature of their data. What unites them is the pace of change: a threat environment that is evolving faster than most security programmes can track.

The overall picture

Phishing attacks are the most widely feared threat across all survey respondents, cited by 55% of them. Ransomware follows, at 48%, with AI-driven cyberattacks close behind, at 47%. The proximity of AI-driven attacks, which is a relatively new category, to long-established threats like ransomware, reflects how rapidly the landscape is shifting.

When asked to name the single most significant driver of remote access security **threats over the next 12–24 months**, respondents pointed to the sophistication of **cybercriminals (28%)** and **AI-driven attacks (23%)** above all else. This was ahead of **hybrid work environments (21%)** and **lack of employee training (15%)**. AI-related concerns account for nearly half of all responses about the future threat driver, making it the defining forward-looking theme of this research.

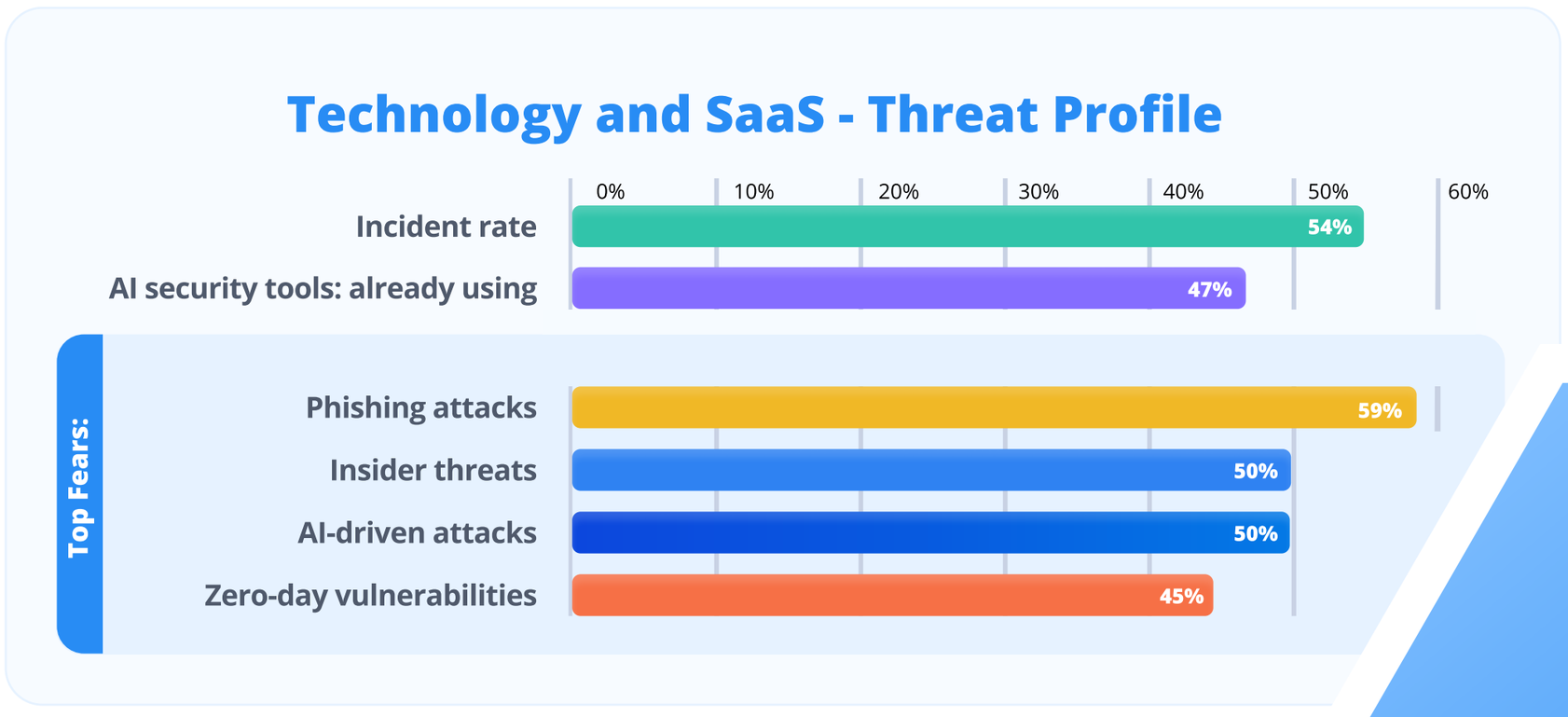
What Do You Fear?

71% of respondents rate a vendor's security track record as either critical or very important in their selection process. Only 2% consider it unimportant. In a landscape where the threat environment is accelerating, who you buy from has become as important as what you buy.

In the following pages, we examine how these threats are perceived by the various industries.

TECHNOLOGY AND SAAS: A HIGH-INCIDENT SECTOR WITH A DISTINCTIVE THREAT PROFILE

Technology and SaaS organisations account for the largest share of respondents and present one of the most striking paradoxes in the survey. This is a sector with (at least in theory), high security awareness, significant AI adoption, and strong confidence in current controls — and yet it has a 54% incident rate, a joint-high of any industry. Let's see how respondents in this sector view things.

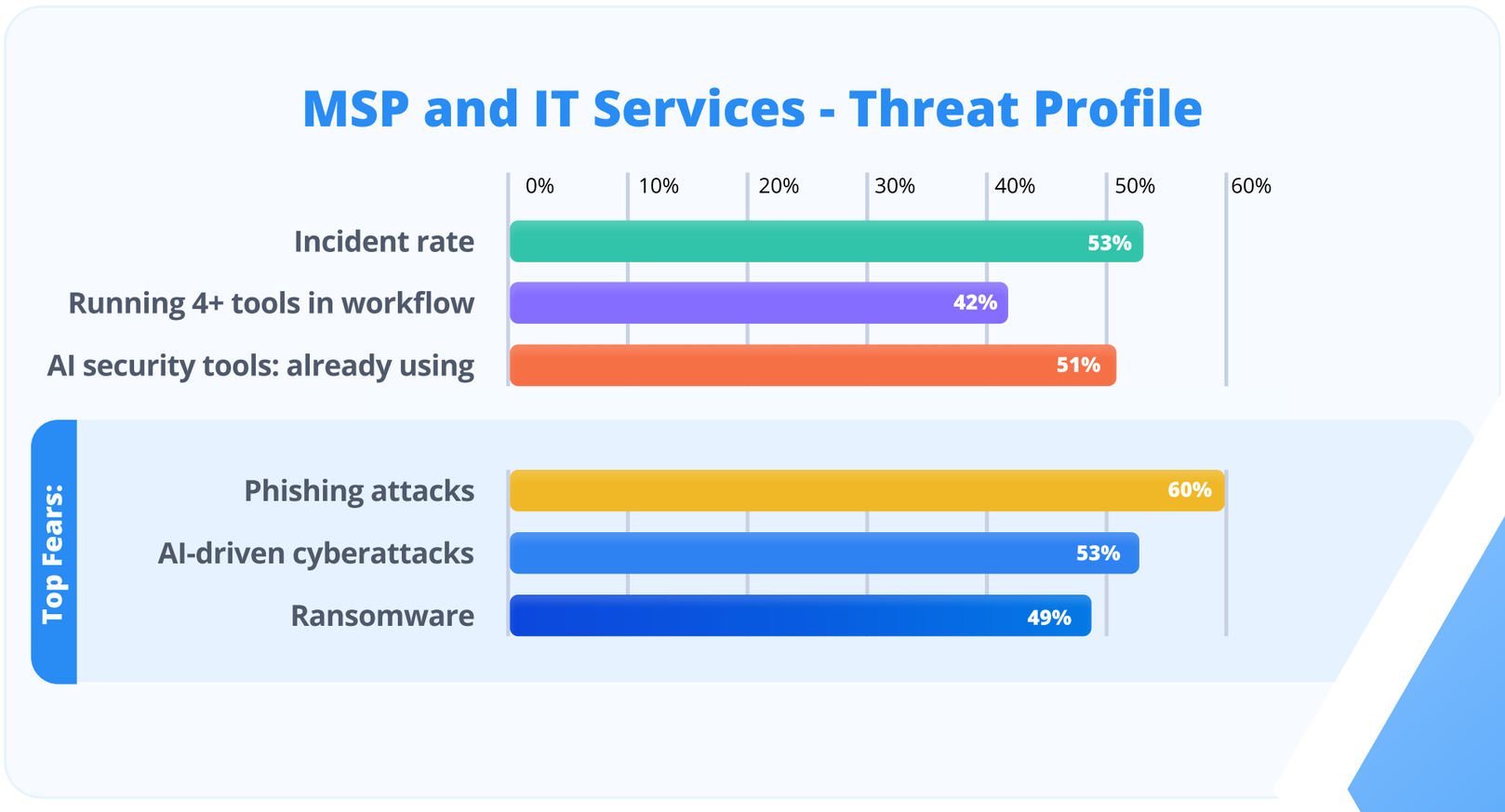


The threat profile here is distinctive. Phishing leads, at 59%, as it does in most sectors. But insider threats (50%) and AI-driven cyberattacks (50%) tie as the second most feared threats. These are levels significantly higher than in most other industries. This reflects the nature of tech organisations: large, skilled workforces with broad system access, high rates of third-party vendor integration, and a competitive culture that can resist friction-inducing security controls.

The primary drivers cited for the future threat environment are AI-driven attacks (25%) and cybercriminal sophistication (23%). Together, they're accounting for nearly half of all responses. Of those who experienced incidents, 60% involved vulnerability exploitation, and 51% resulted in data exposure risk. Both are among the highest rates of any industry. Migration risks (47%) and vendor security review delays (45%) are the sector's dominant operational challenges, suggesting that the security team's ambitions are regularly outpaced by the complexity of the technology environment they are trying to secure.

MSP AND IT SERVICES: HIGH EXPOSURE, HIGH CAPABILITY; STILL NOT ENOUGH

MSP and IT Services organisations have a profile that is simultaneously the most capable and the most exposed by volume. They have the highest AI security tool adoption of any industry - at 51%, the highest proportion auditing monthly - 40%, and the lowest low-confidence rate in current security - 4%. They are, according to their self-assessment, the most security-mature segment in the survey.

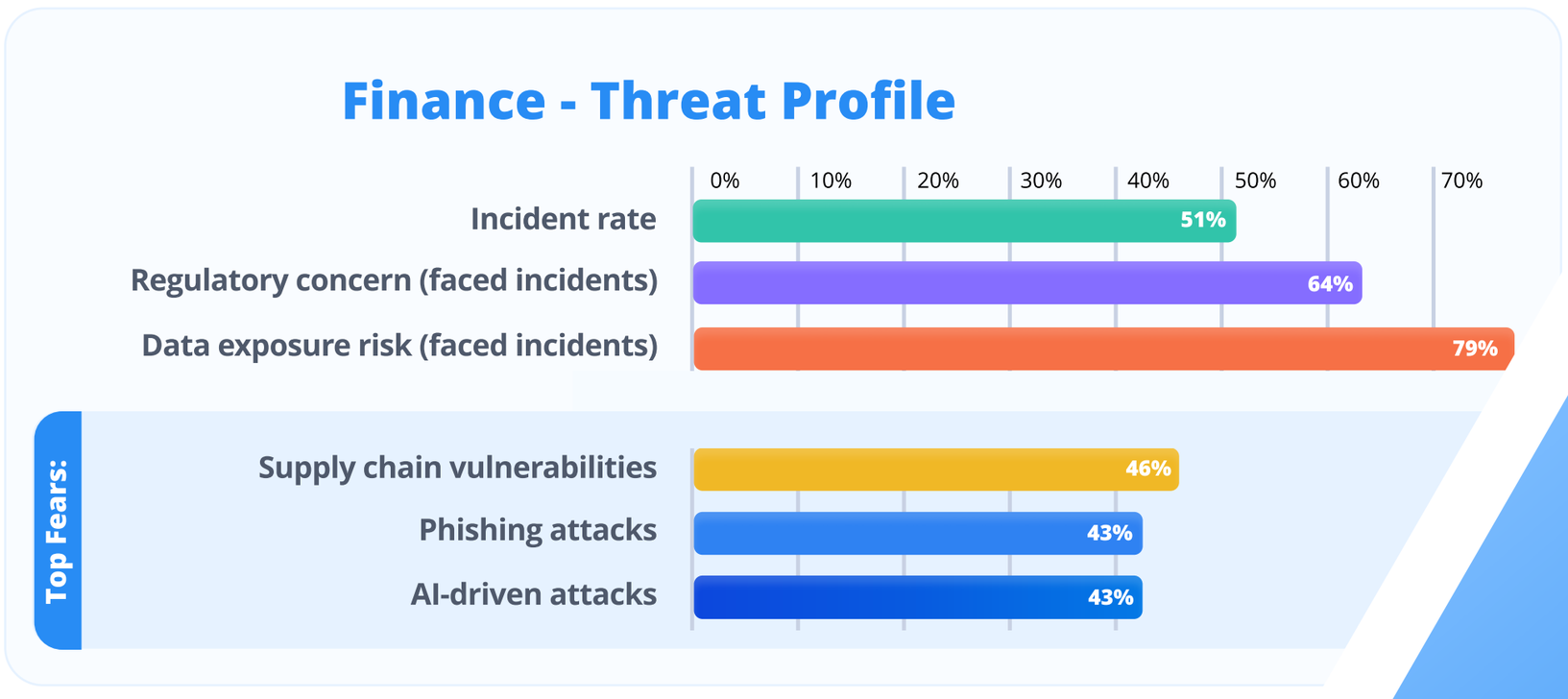


Their incident rate is 53%, which is comparable to the broader survey average. Of those incidents, 67% involved vulnerability exploitation and 54% involved misconfiguration, the highest misconfiguration rate of any industry. This is a segment that knows security deeply, invests in it significantly, and still cannot close the gap entirely. The implication is that knowledge and tooling are necessary but not sufficient: the breadth of environments that MSPs manage (many of which they do not fully control), creates an irreducible exposure.

Vendor security review delays (51%) and migration risks (49%) are the sector's top operational challenges. This is consistent with the demands of managing security across multiple client environments simultaneously. 42% of MSP respondents are running four or more tools in their remote access workflow, the highest tool-sprawl rate of any industry. Zero Trust implementation is the top stated priority at 76%, significantly above the cross-industry average of 58%, suggesting an industry that is actively working to replace perimeter-based assumptions with more rigorous identity and access controls.

FINANCE: SUPPLY CHAIN RISK AND A DISTINCTIVE COMPLIANCE BURDEN

Finance respondents show the most distinctive threat perception of any industry in the survey. While phishing, ransomware, and AI-driven attacks dominate the concerns of most sectors, finance uniquely identifies supply chain vulnerabilities as its top threat at 46%. That's ahead of phishing (43%) and AI-driven attacks (43%). This reflects an industry acutely aware of its third-party exposure: financial institutions routinely extend system access to vendors, partners, and service providers. The reason is not difficult to guess: a breach anywhere in that chain can have severe regulatory and commercial consequences.

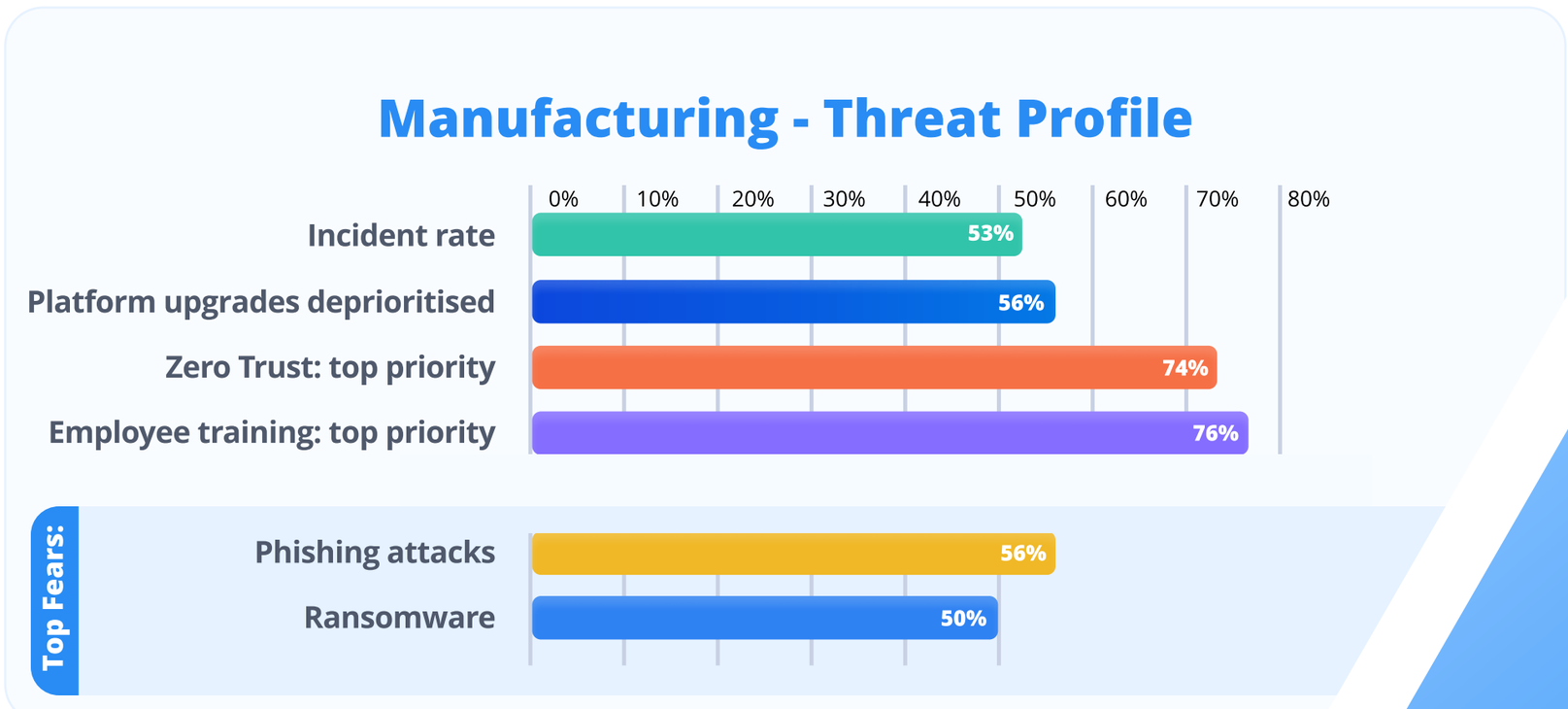


The incident impacts in finance are the most severe of any industry. Among those who experienced an incident, 79% cited data exposure risk - the highest rate of any sector - and 64% cited regulatory concern, compared to a total survey average of 31%. Lost customer trust (58%) also exceeds the survey average of 29% substantially. These outcomes reflect the reputational and regulatory stakes of a data breach in a sector governed by PCI DSS (30%), ISO 27001 (49%), GDPR (32%), and SOC 2 (27%).

Finance respondents are less confident in their current security than most other industries, with only 51% rating themselves very or extremely confident; and of those, 74% had still experienced an incident. Complexity of existing tools is the leading operational challenge at 41%, ahead of budget (38%), suggesting that for finance, the problem is not simply a question of resources but of managing a dense, interconnected technology environment, where change is slow and the cost of disruption is high.

MANUFACTURING: INFRASTRUCTURE DEBT AND ACCELERATING EXPOSURE

Manufacturing respondents combine a high incident rate (53%) with the most significant platform infrastructure lag of any industry. Platform upgrades are the most deprioritised task at 56% (the highest of any sector), and manufacturing is the only industry where platform modernisation outranks security hardening as the dominant operational sacrifice. The implication is a sector operating on ageing infrastructure in an environment of growing threat sophistication.

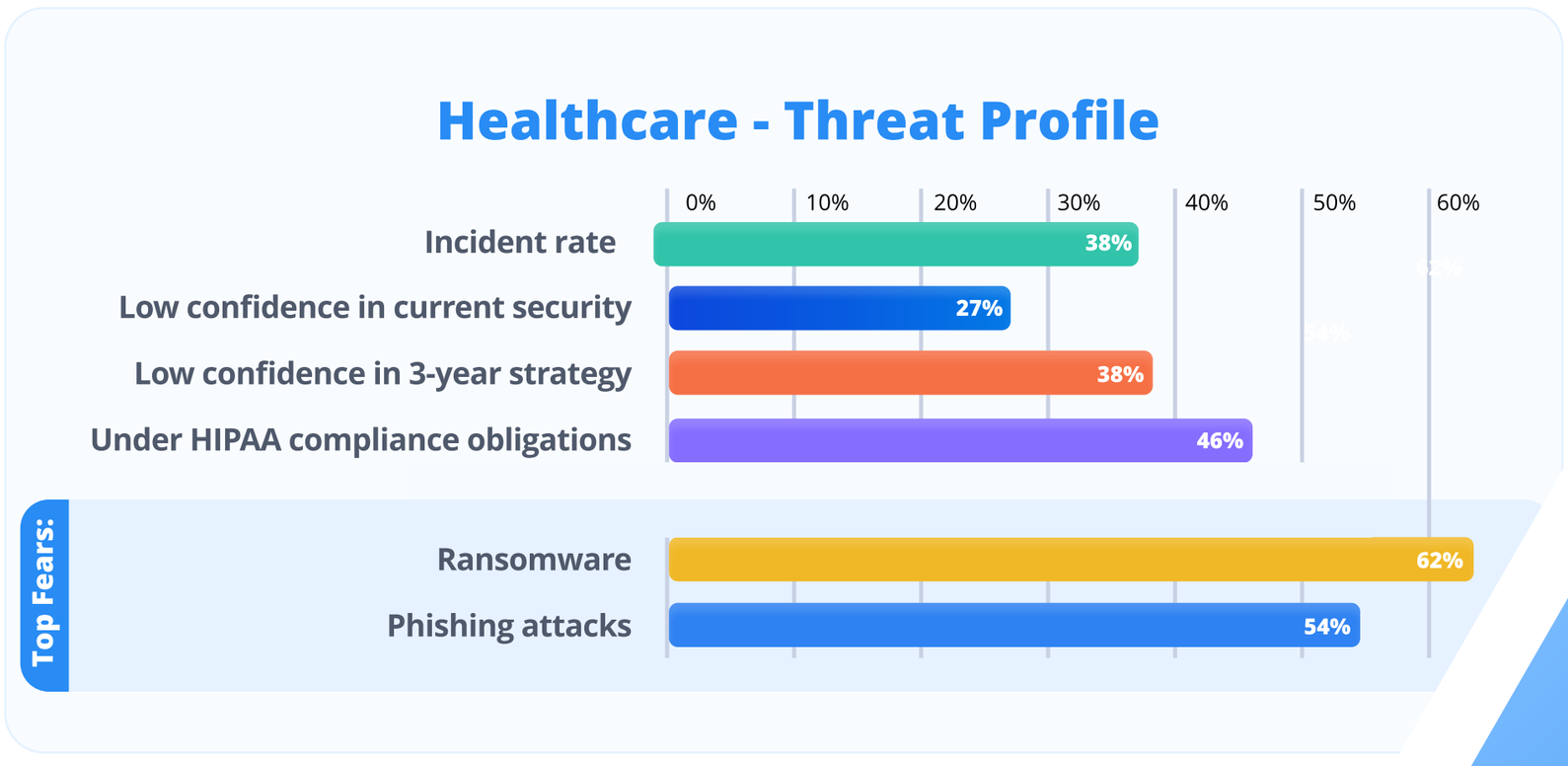


Ransomware (50%) is a more prominent fear in manufacturing than in most other industries, likely reflecting the operational consequences of production downtime that a successful attack can cause. When experiencing incidents, 56% involved vulnerability exploitation and 56% involved a security breach. That's the joint highest breach rate of any industry alongside retail. Manufacturing's compliance landscape is relatively light compared to healthcare or finance; ISO 27001 (35%) is the most common standard, with 15% reporting no applicable compliance obligations. This may contribute to a lower sense of urgency, despite high exposure.

Manufacturing respondents show the strongest commitment to Zero Trust of any sector not in the MSP/IT Services category, with 74% citing it as a top priority. Budget (50%) and lack of skilled personnel (44%) are the twin obstacles, making this a sector that knows what it needs but faces the most significant resource constraints in delivering it outside the smallest company sizes.

HEALTHCARE: ACUTE ANXIETY, HIGH STAKES, AND A COMPLIANCE IMPERATIVE

Healthcare respondents present a uniquely concerning profile. The sector has the lowest incident rate of the high-stakes industries, at 38%. It also has the highest low-confidence rate in current security of any industry, at 27%, and the second-highest anxiety about the three-year outlook at 38%. **Healthcare professionals know their defences are imperfect, and they know the consequences of failure are severe.**

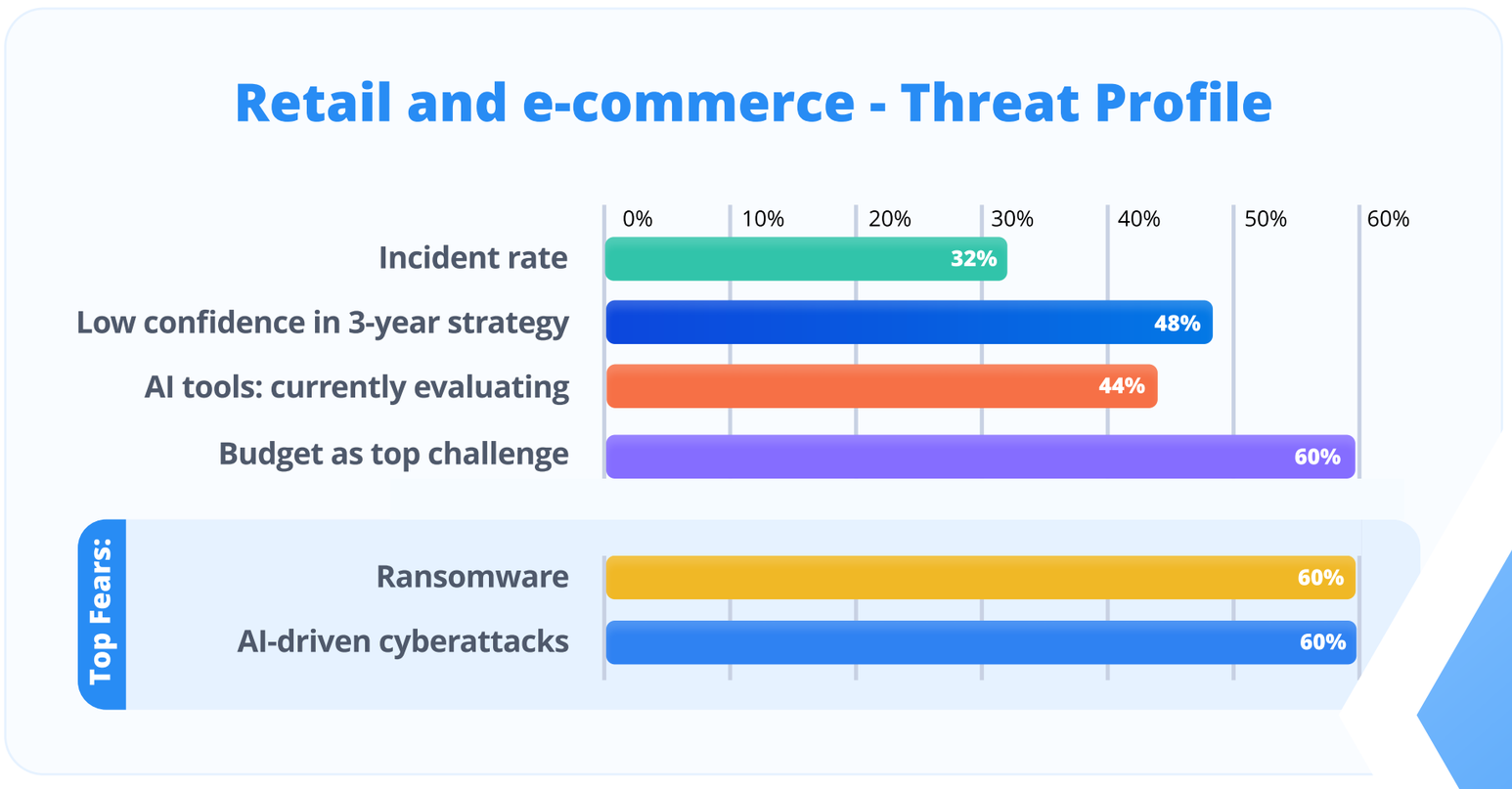


Ransomware is the dominant fear in healthcare at 62%; that's the highest rate of any industry for any specific threat. This is not abstract: the healthcare sector has been a primary ransomware target for years, and the combination of sensitive patient data, life-critical systems, and historically underfunded IT infrastructure makes it acutely vulnerable. Of those who experienced incidents in healthcare, 60% involved a security breach, a higher breach conversion rate than most other sectors. 80% cited data exposure risk as an impact. Among any sub-group in the survey, healthcare incidents produce the most severe data consequences.

46% of healthcare respondents are subject to HIPAA. Monthly audits are conducted by 50% of healthcare organisations, also the highest rate of any sector, suggesting genuine compliance discipline. Yet 23% rate their mitigation effectiveness as low, indicating that discipline in process does not always translate into confidence in outcomes. Budget (38%) and migration risks (38%) are joint top challenges, pointing to a sector that is aware of what needs to change but struggling to fund and execute the transition.

RETAIL AND E-COMMERCE: FUTURE ANXIETY OUTPACES CURRENT CONFIDENCE

Retail and e-commerce respondents present the most striking future-confidence gap in the survey. Only 20% report low confidence in their current security posture. This suggests a relatively composed present. Yet, 48% of retail and e-commerce respondents express low confidence in their three-year strategy, the highest future-anxiety rate of any industry. Retail respondents know that the threat environment is changing faster than their security programme can adapt.

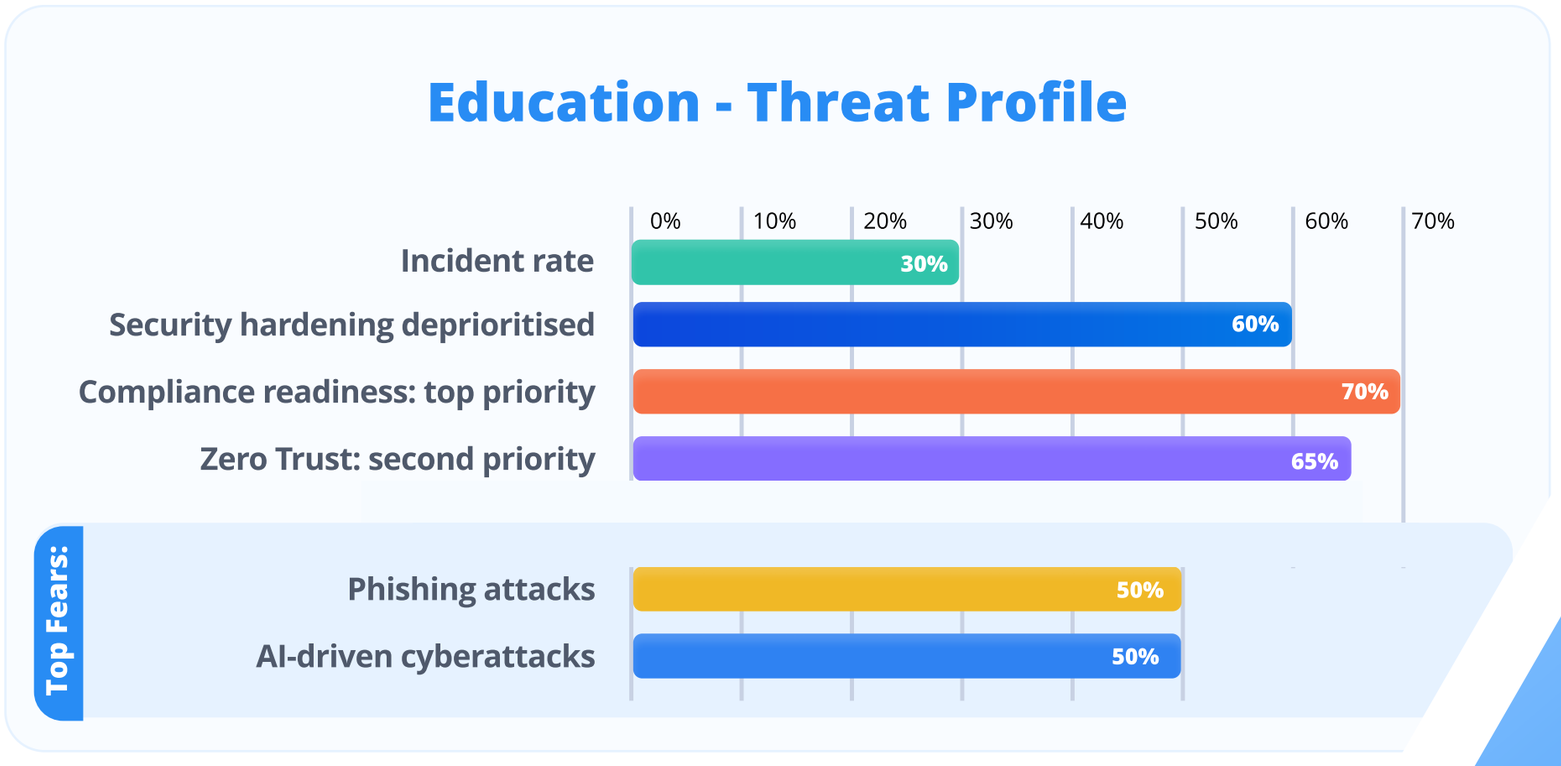


Ransomware and AI-driven attacks are tied as the top threats, at 60% each. This is the highest combined AI-related fear of any industry. Of those who experienced incidents, 62% involved a security breach (the joint-highest rate, alongside education) and 62% cited regulatory concern as an impact, the highest regulatory concern rate of any sector. PCI DSS (20%), GDPR (40%), and ISO 27001 (44%) all apply to significant proportions of retail respondents.

Budget is the most commonly cited challenge, at 60%, the highest across all industries. Retail has the lowest AI security tool adoption at 28%, but also the highest AI evaluation rate at 44%, suggesting that the intention to adopt exists. However, budget and confidence barriers are delaying commitment. Zero Trust has been implemented by only 12% of retail respondents (the lowest rate of any industry). This is a significant gap, given the 60% AI-attack fear rate.

EDUCATION: SECURITY HARDENING SACRIFICED, ANXIETY BUILDING

Education respondents tell a story of present relative stability masking significant future concern. Only 5% report low confidence in current security (the lowest rate of any industry), yet 35% express low confidence in their three-year strategy. The gap is wide, and the numbers that explain it are clear: 60% of education respondents say security hardening is being deprioritised. That's the highest rate of any industry. Budget (55%) and migration risks (50%) are their dominant operational challenges.



The incident rate is the lowest of any industry (30%), but when incidents occur the consequences are serious: of those affected, 67% involved both vulnerability exploitation and security breaches, and 67% cited data exposure risk. This suggests that, while education is attacked less frequently, successful attacks are not minor events.

The compliance picture is complex for education: ISO 27001 (35%), HIPAA (30%, particularly for institutions with health services), NIS2 (25%), and SOC 2 (25%) all apply to meaningful proportions of the sector. Compliance readiness is the single highest stated priority at 70%, ahead even of Zero Trust (65%). This suggests that regulatory compliance is driving the security agenda in education more than internal threat assessment.

Granular access control has been implemented by only 10% of education respondents. This the lowest rate of any industry. Zero Trust by just 15%. These are significant gaps for a sector with growing data obligations and a threat environment in which phishing and AI-driven attacks are jointly cited by 50% of respondents.

CHAPTER 2: THE CONFIDENCE PARADOX AND ITS REAL-WORLD COST

This research shows that that organisations face an accelerating threat environment. But that's not something new. What's new is that the organisations facing that environment have largely convinced themselves they are better prepared than the evidence suggests. The confidence paradox is not a curiosity. It is an active risk factor, and the incident data makes its cost plain.

Current confidence: broadly high, selectively fragile

When asked how confident they are that their current remote access approach meets their organisation's security needs, 66% of respondents described themselves as very or extremely confident. Only 10% expressed low confidence. Taken at face value, this would suggest a market that is managing its risks effectively.

The incident data immediately complicates this picture. Of respondents who described themselves as very or extremely confident, 55% had still experienced a remote access incident in the past 24 months. Across roles, this overconfidence-and-breach rate reaches 77% among CIOs and CTOs; these are the most senior decision-makers in the survey. And it is at 67% among Operations professionals. Even among IT Directors, where the largest sample makes the finding most robust, 61% of confident respondents had experienced an incident.

Nearly half of IT teams have experienced a remote access incident in the past two years. 47% reported an incident, with vulnerability exploitation (42%), security breach (38%), and misconfiguration (35%) as the most common types. The consequences were material: data exposure risk (44%), downtime (37%), and regulatory concern (31%).

Confidence does not reliably correlate with security. It is correlated with the belief that you are secure — and in a threat environment of this complexity, those two things are not the same.

THE RELATIONSHIP BETWEEN TOOL CHOICE, CONFIDENCE, AND INCIDENTS

One of the clearest explanations for the confidence paradox is the relationship between the tools organisations use and their actual incident experience. Organisations primarily using open-source or free remote access tools experienced incidents at a rate of 64%, almost double the 33% rate among those using business-grade commercial solutions. Microsoft RDP users sit at 49%.

Yet open-source users do not report dramatically lower confidence. This suggests that tool familiarity and operational continuity are being mistaken for security assurance. Teams that have used open-source tools for years, and not experienced a visible incident recently, may be carrying a false sense of security. And that's a sentiment that the data does not support.

Tool proliferation reveals a similar pattern. Of respondents running just one remote access tool, 28% experienced an incident. Among those running four to five tools, the rate rises to 67%. Running more tools does not translate into greater security. In many cases, it means larger attack surface, more credential management burden, and more integration risk. The survey data reflects that directly.

Confidence: broadly high, selectively fragile

The overconfidence finding is most pronounced among the roles with the greatest organisational influence over security strategy.

Among CIOs and CTOs, 65% experienced a remote access incident in the past 24 months, the highest incident rate of any role. Of those who described themselves as very or extremely confident, 77% had been breached. Among Operations professionals, 67% of confident respondents had been hit.

> Among CIOs and CTOs who described themselves as very or extremely confident in their security, 77% had experienced a remote access incident in the past 24 months. The people making the investment decisions are the most likely to overestimate the protection those investments are buying.

THE RELATIONSHIP BETWEEN TOOL CHOICE, CONFIDENCE, AND INCIDENTS

This dynamic has clear consequences. If senior leaders are **overestimating security outcomes**, the resulting under-investment and misplaced priorities will cascade downward through the security programme.

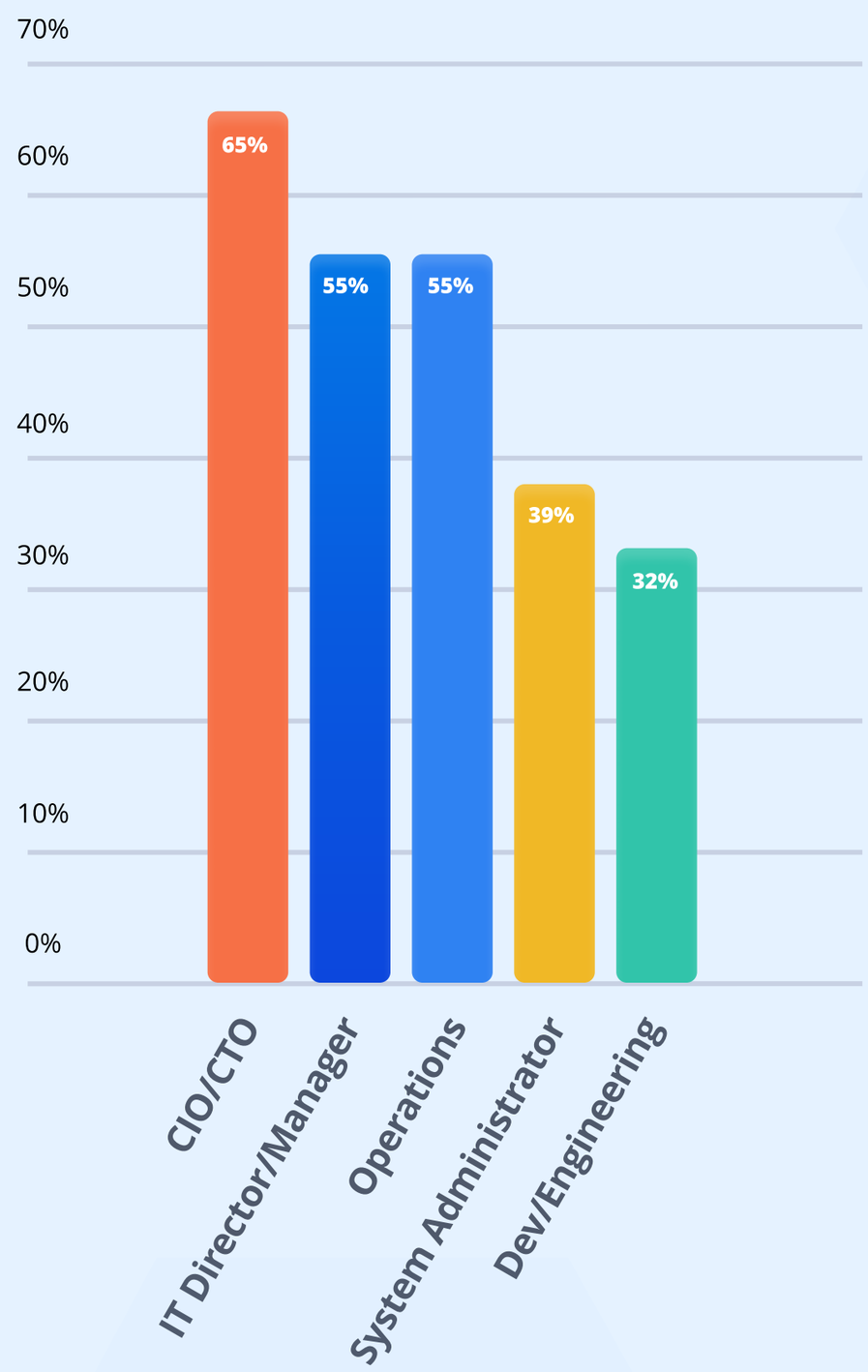
> IT Directors will face pressure to demonstrate security compliance, rather than actually improve it.

Systems Administrators, the people with hands on the infrastructure, will inherit a security debt that their leadership does not fully see.

The Systems Administrator finding deserves attention in its own right. Only 39% of sysadmins reported experiencing an incident, notably lower than the 55% rate for IT Directors. But **14% of sysadmins** said they were **not sure** whether an incident had occurred, the highest uncertainty rate of any role. This is not evidence of lower exposure. **It is evidence of lower visibility.**

> Sysadmins may be managing an infrastructure through which incidents are passing undetected.

Incident rate by role (%)



THE INDUSTRY DIMENSION: WHERE CONFIDENCE AND INCIDENTS DIVERGE MOST

The tension between confidence and outcomes is not uniform across sectors. In finance, only 51% of respondents rate themselves very or extremely confident in current security, which is already lower than the survey average. Yet of those who are confident, 74% have experienced an incident. Finance respondents are more sceptical about their security than most, yet they are still being caught out.

In Manufacturing, 76% express high confidence in current security. It is the second highest rate of any industry, yet the incident rate is 53%, and 62% of confident manufacturing respondents have been breached. The sector's comfort with its current posture is not matched by its outcomes.

Healthcare is the outlier. With 27% reporting low confidence in current security (the highest rate of any industry), healthcare professionals are the most honest in the survey about their own vulnerability. Only 42% of confident healthcare respondents experienced an incident, also the lowest overconfidence-breach rate of any industry. The sector that worries most, it turns out, has somewhat better outcomes than the sectors that worry least.

THE FUTURE: CONFIDENCE GIVES WAY TO ANXIETY

If current confidence is overstated, future confidence is more honest. When asked about the three-year outlook, 26% of respondents describe themselves as not or only slightly confident that their strategy will address emerging threats, compared to just 10% who express the same low confidence about today. Only 16% are extremely confident about the future, compared to 20% who feel extremely confident about the present.

The future-confidence gap is sharpest among Operations professionals (27% low now → 55% for three years), Systems Administrators (18% → 43%), and the 50–249 employee company size band (16% → 51%). These segments represent substantial proportions of the operational IT workforce. They are the teams who will be managing the remote access infrastructure that must withstand whatever the next three years of threat evolution brings.

The gap tells us something important about how IT professionals perceive their own trajectory: they feel capable of managing the present, but they do not believe their current approach is adequate for the future. The organisations that take that signal seriously, and act on it now, will be better positioned than those that wait for the anxiety to become an incident.

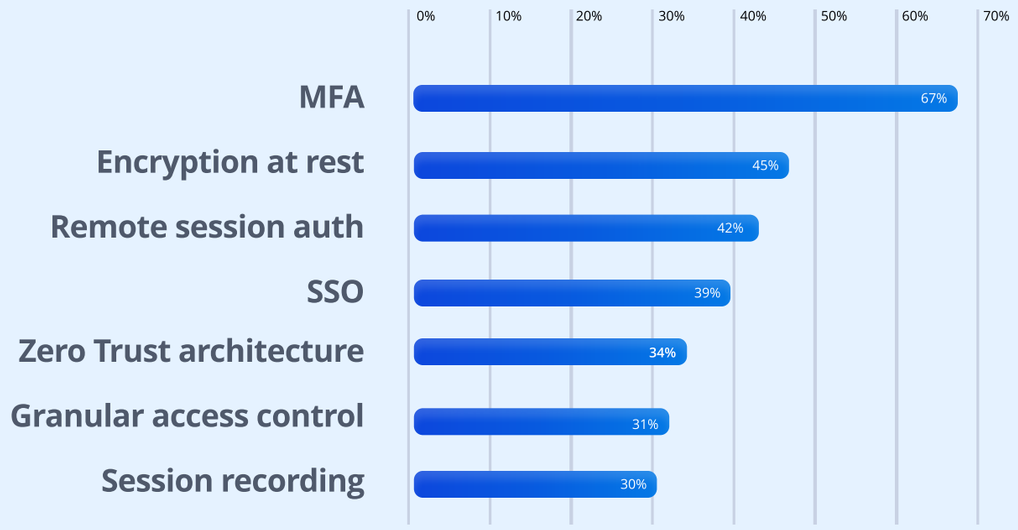
CHAPTER 3: THE SECURITY INTENTION GAP

Across every industry and every role in this survey, there is a consistent pattern: **organisations** know what they need, intend to implement it, but have not yet done so. **The security intention gap**, or the distance between the controls teams consider essential and the controls they have actually deployed, is the operational expression of the **confidence paradox**. It explains, at least in part, why confidence so frequently fails to predict outcomes.

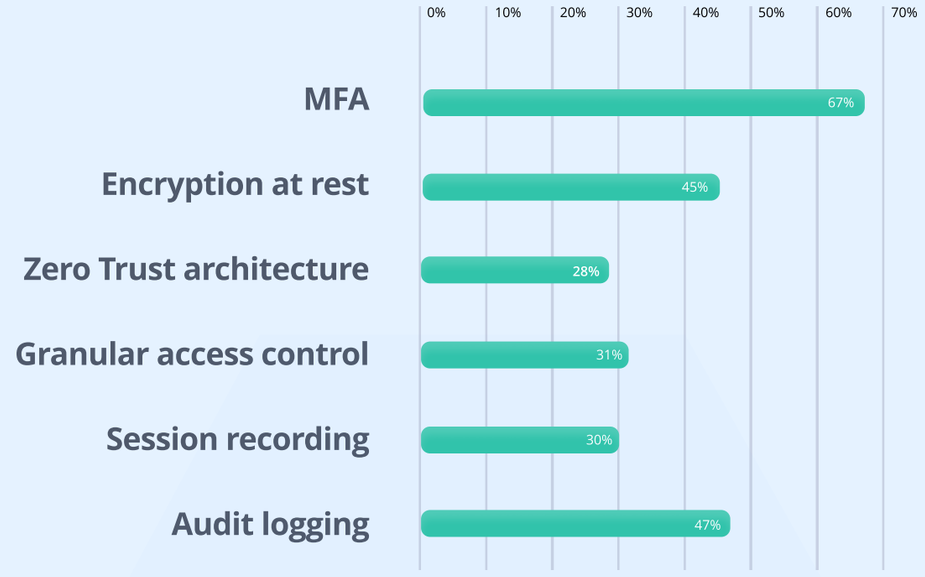
THE OVERALL PICTURE: DESIRE VS. DELIVERY

At the survey level, MFA stands out as a control where intention and implementation are aligned: 67% consider it a must-have, and 67% have implemented it. Beyond MFA, the alignment deteriorates. Zero Trust architecture is considered a must-have by 34% of respondents and a top priority by 58%, yet only 28% have implemented it. Remote session authentication is a must-have for 42%, but does not appear as a commonly implemented control. SSO is desired by 39%. Audit logging has been implemented by 47%, which is a reasonably healthy rate, but granular access control (31% implemented), and session recording (31%), lag behind their stated importance.

Security Intention Gap: Must-Haves



Security Intention Gap: Implemented



The compliance picture reinforces this. 95% of respondents are subject to at least one compliance standard: ISO 27001 (42%), GDPR (33%), HIPAA (29%), SOC 2 (27%), PCI DSS (25%). Only 5% report no applicable obligations. Yet 47% of the same population have experienced incidents with regulatory concern as a consequence. Compliance obligations are not translating automatically into compliance-ready security controls.

In the next few pages, we will analyse all industries in the survey separately from this point of view.

> Tool proliferation sits at the heart of the intention gap. 85% of respondents run two or more remote access tools.
> Among 1,000–4,999 employee organisations, 38% run four or more.
> Each additional tool is a potential gap in coverage, a credential to manage, and an integration to secure.

TECHNOLOGY AND SAAS: THE ZERO TRUST LAG

Technology organisations have the highest MFA implementation rate in the sector analysis at approximately the survey average. Encryption at rest, **at 59%**, and audit logging, at 54%, are relatively strong. But Zero Trust, the control that 60% cite as a top priority, has been implemented by **only 32%**.

> For a sector where insider threats and AI-driven attacks are cited by half of all respondents, the gap between ambition and delivery on Zero Trust is the defining security risk.

The primary obstacles are structural rather than financial. **Migration risks (47%) and vendor security review delays (45%) rank above budget (43%)** as the dominant challenges. This is a sector where the security team's intentions are regularly frustrated by the complexity of the environment they are working within: fragmented tool stacks, legacy integrations, and procurement processes that slow the adoption of newer security architectures.

35% of tech organisations are running four or more tools in their remote access workflow, and **52% have deprioritised security hardening** due to the time spent managing existing security challenges.

This is a compounding problem: the complexity that creates gaps also consumes the bandwidth needed to close them.

MSP AND IT SERVICES: STRONG CONTROLS, PERSISTENT MISCONFIGURATION RISK

MSPs show the strongest overall mitigation profile: encryption at rest at **51%**, audit logging at **47%**, and granular access control at **38%** are all above the survey average. AI tool adoption, **at 51%**, is the highest of any industry. Yet misconfiguration accounts for **54%** of their incidents, which is the highest rate of any sector, and vulnerability exploitation accounts for **67%**. The conclusion is that MSPs have the controls in place but are not always implementing them consistently across all of the environments they manage.

For MSPs, the intention gap is less about what controls exist and more about whether those controls are applied with sufficient rigour across every client environment.

This is a governance and standardisation challenge, not a technology one. **42% of MSP respondents** are running four or more tools in their remote access workflow. This is, by any standard, a level of complexity that increases the likelihood of inconsistent application.

FINANCE: COMPLIANCE INVESTMENT NOT MATCHING CONTROL COVERAGE

Finance respondents have the most stringent compliance obligations and among the most severe incident impacts, yet their control coverage reflects a sector still closing significant gaps. Zero Trust has been implemented by only 27% of finance respondents, despite the sector's acute supply chain vulnerability concerns. Granular access control sits at **32%**, session recording at **32%**, and encryption at rest at **49%**.

The complexity of existing tools is the leading challenge for finance, at 41%.

> The sector's compliance investment has historically led to a fragmented stack of point solutions, each addressing a specific requirement, but without the integration and coverage consistency that a unified architecture would provide.

Lack of executive or board prioritisation (41%) also ranks as a top obstacle, pointing to a sector where the security team's proposals are not always receiving the organisational support needed to execute them.

The irony is visible in the data: finance respondents who experience incidents suffer the most severe consequences: **79% data exposure risk**, **63% regulatory concern**, yet the controls that would prevent those consequences have below-average implementation rates.

> Zero Trust has been implemented by only 27% of finance respondents, despite the sector's acute supply chain vulnerability concerns.

MANUFACTURING: INFRASTRUCTURE GAPS COMPOUND EXPOSURE

Manufacturing's intention gap is shaped by infrastructure debt more than any other factor. Platform upgrades have been deprioritised by **56%** of respondents and security hardening by **47%**.

> Security controls are being deployed on infrastructure that is itself overdue for modernisation. This is a combination that amplifies risk.

Encryption at rest has been implemented by only **29%** of manufacturing respondents, which is the lowest rate in the industry breakdown, and session recording by **26%**. Audit logging at 38% is also below average. These are foundational controls for any organisation subject to regulatory scrutiny or operating technology environments where access control matters. The combination of a **74% Zero Trust priority rating** and **29% Zero Trust implementation rate** represents a gap that is only likely to widen as the threat environment evolves.

Budget **(50%)** and lack of skilled personnel **(44%)** are twin obstacles. Manufacturing is a sector that knows what it needs, cannot fully fund it, and does not have the people to deliver it without additional investment.

HEALTHCARE: COMPLIANCE DISCIPLINE, CONTROL GAPS

> Healthcare has the highest monthly audit rate of any industry at 50%, reflecting genuine compliance discipline under HIPAA (46% of respondents) and other frameworks.

But the control picture is mixed. **Audit logging** is in place at **50%** and **granular access control** at **46%**. Both are above average. Encryption at rest at **35%** and Zero Trust at **23%** are lower, and session recording sits at just **27%**.

Given that **60%** of healthcare incidents involve a security breach, the gaps in Zero Trust and session recording are particularly concerning. These are the controls most directly associated with detecting and limiting the impact of an active intrusion, and they are among the least deployed in the sector with the highest breach-consequence rate.

Healthcare's intention gap is compounded by its operational constraints. Budget **(38%)** and migration risks **(38%)** are joint top challenges.

> In an environment where clinical systems cannot simply be taken offline for upgrades, security modernisation moves slowly even when the intent is clear.

RETAIL: THE LARGEST ZERO TRUST GAP

Retail and e-commerce have the lowest Zero Trust implementation rate of any industry **(at just 12%)**, against a background where **60%** of respondents fear both ransomware and AI-driven attacks. This is the most pronounced single intention gap in the entire survey. The controls that would most directly reduce exposure to the threats that retail fears most are the controls that retail has been least able to deploy.

> The gap between MFA and Zero Trust is also the gap between what retail can afford and what it knows it needs.

Budget **(60%)** is the dominant barrier, and with MFA as a must-have for **76%** of retail respondents (the highest rate of any industry for that control), the sector is clearly not indifferent to security investment. But the gap between MFA (relatively low-cost, well-understood) and Zero Trust (complex, resource-intensive) is also the gap between what retail can afford and what it knows it needs.

EDUCATION: THE GRANULAR ACCESS GAP

Education has the lowest granular access control implementation rate of any industry at just **10%,** and Zero Trust at **15%**. For a sector managing growing volumes of sensitive data, like student records, health information, research data, under frameworks including ISO 27001 **(35%)**, HIPAA **(30%)**, and NIS2 **(25%)**, these are significant exposures.

> The Education sector is caught in a particular bind: compliance readiness is its top stated priority at 70%, but the controls most directly associated with compliance readiness, namely granular access control, audit logging, session recording, are implemented at rates that fall below most other sectors. Budget (55%) and migration risks (50%) explain much of the gap, but so does the absence of skilled personnel (35%) to design and deliver the architectures that compliance requires.

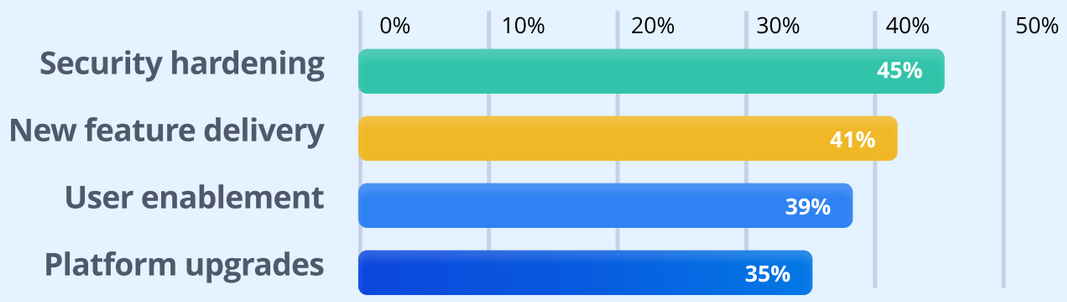
CHAPTER 4: THE OPERATIONAL BURDEN

One of the most counterintuitive findings in the entire survey is this: the effort of managing remote access security challenges is actively preventing organisations from becoming more secure. The time and resource devoted to dealing with security problems is consuming the bandwidth that could be used to prevent them.

SECURITY HARDENING IS BEING SACRIFICED TO ADDRESS SECURITY THREATS

45% of respondents say that security hardening is being deprioritised because of the time spent addressing remote access security challenges. New feature delivery (41%), user enablement (39%), and platform upgrades (35%) are all being pushed back for the same reason. Nearly half of all IT teams are so consumed by responding to security challenges that they cannot find time to make their systems more secure. That is not a resource problem. It is a structural failure.

Deprioritised tasks due to remote access security challenges

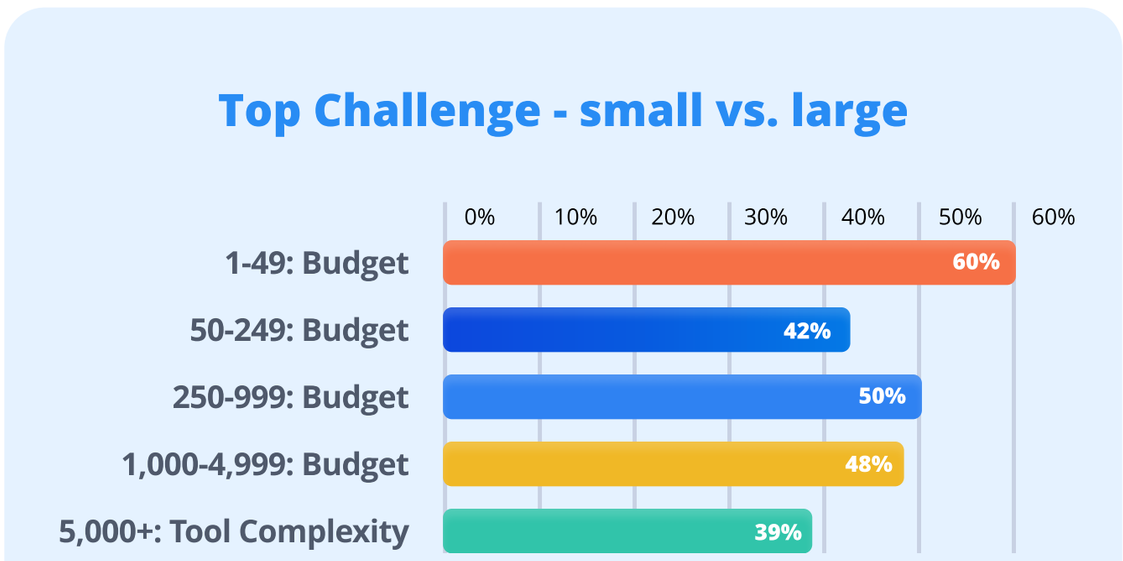


The pattern holds across roles. Among IT Directors, the largest and most operationally exposed segment in the survey, 54% say security hardening is deprioritised. Among CIOs and CTOs, it is 52%, alongside 58% who report new feature delivery being pushed back. For an organisation's most senior technology leaders, this means the security threat environment is directly impeding business delivery.

This is at its worst in education, where 60% of respondents deprioritise security hardening, which is the highest rate of any sector. Manufacturing (47%) and technology (52%) also show high rates. In each case, the operational drain of managing the existing security challenge is consuming the investment that would reduce future challenges.

THE CHALLENGE PICTURE VARIES BY SIZE AND SECTOR

Budget dominates as the primary challenge for organisations of all sizes except the very largest. Among 1–49 employee organisations, 60% cite budget constraints as a top challenge, falling to 42% at 50–249 employees and 50% at 250–999. Only at 5,000+ employees does complexity of existing tools (39%) overtake budget as the leading barrier. The challenge for large enterprises is not finding money, it is managing what they already have.



Among MSPs, vendor security review delays (51%) and migration risks (49%) lead the challenge rankings. This is reflecting the procurement complexity of operating across many client environments. In technology organisations, the same two challenges rank highest at 47% and 45% respectively, pointing to environments where the pace of change is outstripping the pace of security review.

AI adoption is accelerating, but unevenly. 39% of respondents are already using AI-powered tools to support remote access security monitoring or threat detection. A further 25% are actively evaluating them, and 17% have plans to deploy. Only 11% have no plans to adopt AI security tools at all.

MSPs lead adoption at 51%, followed by technology organisations at 47% and manufacturing at 44%. Retail lags at 28% currently using, but has the highest evaluation rate of any industry at 44%, suggesting a sector on the cusp of significant AI adoption held back primarily by budget and confidence barriers.

Microsoft Defender (24%) and CrowdStrike Falcon (16%) lead AI security tool adoption, reflecting the dominance of established security vendors in this space. The fact that 39% of organisations are already using AI for security while 47% are experiencing incidents suggests that AI adoption alone is not yet moving the needle on outcomes. This is consistent with the broader confidence paradox theme running through this report.

AUDIT CADENCE: REGULAR BUT NOT UNIVERSAL

37% of organisations conduct security audits of their remote access solutions quarterly, and 32% monthly. 21% audit annually, and 7% audit rarely or never. Healthcare leads monthly auditing at 50%, consistent with its HIPAA obligations. Finance, at 16% monthly, is notably lower for a sector with comparable compliance obligations. This is a pattern that may reflect the sector's focus on complexity-of-existing-tools challenges rather than process cadence.

The 7% who audit rarely or never represent a meaningful residual risk. These are organisations operating without a systematic view of their own remote access security posture, which is making the confidence paradox almost inevitable. You cannot know whether your defences are working if you are not regularly testing them.

CHAPTER 5: THE NEXT THREE YEARS

The survey's forward-looking questions reveal a market that is clear-eyed about what needs to change, and equally clear about what is getting in the way. The tension between aspiration and reality is visible in every segment, but the specific shape of that tension varies significantly by industry and company size. Understanding those differences is the starting point for building security programmes that are realistic, rather than just ambitious.

OVERALL PRIORITIES: TRAINING, COMPLIANCE, ZERO TRUST, CONSOLIDATION

Across the full survey population, improving employee training (66%), enhancing compliance readiness (60%), implementing Zero Trust architecture (58%), and consolidating remote access tools (57%) are the top four priorities. The convergence around these four themes is not coincidental: each addresses a different dimension of the same underlying structural problem. Training addresses the human attack surface. Compliance readiness addresses the governance gap. Zero Trust addresses the architecture gap. Tool consolidation addresses the complexity that makes all three of the others harder to deliver.

In the next few pages we look at what the priorities are for each industry.

TECHNOLOGY AND SAAS: COMPETING PRIORITIES

Technology respondents identify employee training **(64%)** and tool consolidation **(64%)** as joint top priorities, with Zero Trust close behind, at **60%**. These are consistent with the sector's high insider threat concern and significant tool-sprawl problem. But the obstacles are equally prominent: too many competing security priorities **(46%)**, lack of executive or board prioritisation **(41%)**, and lack of skilled personnel **(40%)** all rank above budget as barriers.

This is a sector where the security team's knowledge and ambitions are not in question. However, organisational bandwidth and executive alignment are the limiting factors. What's peculiar is that technology organisations, which generally have stronger security expertise than most industries, are also the most likely to see that expertise diluted across too many initiatives with insufficient focus.

For technology organisations, the path forward requires prioritisation above everything else. The problem is not knowing what to do. It is in choosing what not to do, and building enough executive alignment to actually execute.

MSP AND IT SERVICES: ZERO TRUST URGENCY MEETS CHANGE RESISTANCE

MSPs place Zero Trust implementation at the top of their priority list - **76%**, significantly above the cross-industry average of **58%**. This reflects both the sophistication of the MSP security community and its awareness of the perimeter-less nature of the environments it manages. Employee training **(69%)** and compliance readiness **(60%)** follow.

The obstacles are telling: too many competing security priorities **(47%)**, resistance to change **(42%)**, and lack of skilled personnel **(38%)**. For MSPs, resistance to change is a particularly significant barrier. These are organisations that often inherit legacy client environments, must manage client expectations around disruption, and face the challenge of standardising security controls across a diverse portfolio. Zero Trust ambitions are frequently stopped by the organisational friction of implementing new architectures across environments where multiple stakeholders have a say, rather than sheer technical complexity.

For technology organisations, the path forward requires prioritisation above everything else. The problem is not knowing what to do. It is in choosing what not to do, and building enough executive alignment to actually execute.

MSP AND IT SERVICES: ZERO TRUST URGENCY MEETS CHANGE RESISTANCE

MSPs place Zero Trust implementation at the top of their priority list - **76%**, significantly above the cross-industry average of **58%**. This reflects both the sophistication of the MSP security community and its awareness of the perimeter-less nature of

The obstacles are telling: **too many competing security priorities (47%), resistance to change (42%), and lack of skilled personnel (38%)**. For MSPs, resistance to change is a particularly significant barrier. These are organisations that often inherit legacy client environments, must manage client expectations around disruption, and face the challenge of standardising security controls across a diverse portfolio. Zero Trust ambitions are frequently stopped by the organisational friction of implementing new architectures across environments where multiple stakeholders have a say, rather than sheer technical complexity.

CHAPTER 5: THE NEXT THREE YEARS

FINANCE: COMPLIANCE AND CONSOLIDATION, BUT LIMITED BOARD ALIGNMENT

Finance respondents prioritise **employee training (65%), compliance readiness (62%), and tool consolidation (54%)**. The compliance orientation reflects the sector's heavy regulatory burden; the training focus reflects awareness that phishing and insider threats, both prominent in this industry's threat profile, are fundamentally human-behaviour problems.

Lack of executive or board prioritisation is the leading obstacle, **at 41%**. It is the highest rate of any industry for that barrier. In a sector where the cost of incidents is demonstrably high (79% data exposure risk, 63% regulatory concern among those affected), the persistence of a board-prioritisation gap is significant. **Lack of skilled personnel (35%) and budget (35%) follow.** This suggests a sector that understands its risks but is not always able to generate the organisational support needed to address them at speed.

MANUFACTURING: AMBITION CONSTRAINED BY BUDGET AND SKILLS

Manufacturing shows some of the strongest forward-looking commitments in the survey: **employee training (76%), Zero Trust (74%), and compliance readiness (68%)** are all above the cross-industry average. The intent is genuine and urgent. But the obstacles are the most constraining of any sector: budget (50%) and lack of skilled personnel (44%) rank one and two.

> Manufacturing's combination of high intent and high constraint creates a particular risk: organisations that know what they need, cannot fully fund it, and cannot find the people to deliver it are likely to make partial investments.

These certainly will create the appearance of progress, but they won't fully close the gaps. Platform upgrades, **deprioritised at 56%**, are a visible symptom of this dynamic. The infrastructure work that would support modern security architectures keeps getting pushed behind more immediate demands.

Too many competing security priorities (29%), is what rounds out the top three obstacles. For a sector where security competes with operational technology management, production continuity, and supply chain demands for attention, focus is as scarce as budget.

HEALTHCARE: WHAT IS NEEDED VS. WHAT IS POSSIBLE

Healthcare respondents prioritise **employee training (65%), compliance readiness (58%), and tool consolidation (50%)**. The training priority reflects the sector's awareness that phishing (54%) and ransomware (62%), which are both human-entry-point threats, dominate its threat profile. Compliance readiness reflects HIPAA and other obligations.

> Budget is the leading obstacle at 46%. This is the highest single-obstacle rate of any industry. Too many competing priorities (42%) and lack of skilled personnel (31%) follow.

In an industry where clinical systems, patient safety, and operational continuity compete with security investment for limited resources, the security team is frequently operating at the margin of what is organisationally possible.

The tension between aspiration and reality is most acute in healthcare's Zero Trust position: Zero Trust is not among the sector's top three priorities (compliance readiness, training, and consolidation rank higher) despite the sector's **62% ransomware fear rate and 23% current implementation rate**. The implication is that healthcare respondents have concluded that Zero Trust is aspirational rather than achievable within their current constraints. So they are focusing on priorities they can realistically deliver instead.

RETAIL: BUDGET AND AI

Retail respondents show the highest employee training priority of any industry, **at 80%**. Now, this a striking finding, given the sector's relatively limited security investment profile. Training is accessible, impactful, and relatively affordable: for a sector where **budget (52%)** and **competing priorities (52%)** are joint leading obstacles, it represents the most reachable priority. **Tool consolidation (60%)** and **compliance readiness (56%)** follow. But retail's most interesting forward-looking indicator is its AI posture: 44% are actively evaluating AI security tools. That is the highest evaluation rate of any industry. However, **only 28%** are already using them. Budget and confidence barriers are clearly delaying commitment, but the intent is there. If and when budget constraints ease, retail may see a rapid adoption wave.

Zero Trust does not appear in retail's top three priorities, despite having the lowest **Zero Trust implementation rate (12%)** and among the highest **future-anxiety rates (48%)** of any industry. This is a pragmatic acknowledgement that with budget and skilled personnel both severely constrained, implementation of Zero Trust is not currently realistic for most of the sector.

EDUCATION: COMPLIANCE-FIRST AGENDA VS. BUDGET ISSUES

Education is the only industry where **compliance readiness (70%)** outranks employee training as the top priority. This reflects both the growing regulatory burden on educational institutions, as ISO 27001, NIS2, SOC 2, and even HIPAA all apply to significant proportions of the sector, as well as the reality that compliance frameworks are often the clearest organisational lever for securing security investment.

> Compliance is being used less as a safety standard and more as a mechanism for survival.

Zero Trust (65%) is education's second priority, and increasing budget for security (60%) is third. The latter is the highest rate for budget as a stated priority of any industry, and a signal that education respondents understand their primary obstacle. Too many **competing priorities (45%), budget (40%), and resistance to change (40%)** are the three leading obstacles, creating a three-way bind between organisational attention, financial resource, and cultural appetite for change.

The distance between education's priorities and its ability to execute them is the widest of any sector. With security hardening deprioritised at 60%, the lowest control implementation rates across most categories, and the most severe budget constraint profile, the sector faces a compounding challenge:

> The sector is falling behind now, and the structural barriers to catching up are significant.

CONCLUSION: A THREAT LANDSCAPE DEFINED BY STRUCTURAL GAPS

The findings of this report do not describe a market in which organisations are unaware of the risks they face. Every sector, every role, and every size band surveyed understands that the threat landscape is both serious and accelerating. The challenges are structural and take different forms in different parts of the market.

In healthcare, the challenge is acute anxiety about the future combined with the most severe incident consequences of any sector, constrained by a budget environment that makes meaningful security modernisation difficult. **Ransomware**, the sector's **dominant fear, at 62%,** is precisely the threat that encryption, Zero Trust, and session recording controls are designed to mitigate. Yet those controls have among the lowest implementation rates in healthcare.

> The gap between the threat that is feared and the defences that are deployed is the defining risk for the sector over the next three years.

In finance, the challenge is complexity. A dense, interconnected technology stack, fragmented by years of compliance-driven point-solution procurement, makes it difficult to implement the integrated architectures (Zero Trust, granular access control, unified audit logging), that the sector's supply chain vulnerability concerns require. The data suggests that the financial consequences of incidents are not yet translating into the executive urgency needed to fund and execute meaningful change.

In technology and SaaS, the challenge is focus. This sector has genuine security capability. It has a high AI adoption, strong awareness, regular auditing. And yet, it has a 54% incident rate and a 59% overconfidence-and-breach rate among confident respondents.

> The problem is not knowledge or intent. It is the difficulty of maintaining disciplined security governance in environments defined by rapid change, tool sprawl, and competing organisational priorities.

Insider threats and AI-driven attacks are cited by half of all tech respondents as top concerns. Those are exactly the threat categories that a Zero Trust architecture is designed to contain. The **60% priority rate** for Zero Trust and the **32% implementation rate** define the challenge.

In manufacturing, the challenge is infrastructure. Platform upgrades, deprioritised at 56%, is a number that means security controls are being deployed on infrastructure that is itself overdue for modernisation. Budget (50%) and skilled personnel (44%) are twin constraints on a sector that shows genuine security ambition: 74% Zero Trust priority, 76% training priority, 68% compliance priority. The aspiration is real; the structural capacity to deliver it is the limiting factor.

In retail, the challenge is future readiness. With the highest future-anxiety gap of any industry (20% low confidence now → 48% for three years), the lowest Zero Trust implementation rate (12%), and the most constrained budget profile, retail is a sector that feels the weight of what is coming but lacks the current capacity to build the defences it will need. The 44% AI evaluation rate is an indicator of direction, but evaluation is not implementation, and the window for preparation is closing.

CONCLUSION: A THREAT LANDSCAPE DEFINED BY STRUCTURAL GAPS

In education, the challenge is compounding. Security hardening, **deprioritised at 60%**, the **lowest granular access control implementation rate at 10%**, and the widest gap between stated priorities (compliance readiness at 70%, Zero Trust at 65%) and implementation capacity. Education is failing to resource its obligations, not to recognise them, and the institutional barriers to change (budget, migration risk, resistance to change all ranking as top obstacles) make the path forward particularly difficult.

> Confidence is not a metric of security; it is a symptom of blindness.

Across all of this, the confidence paradox remains the central theme. 55% of organisations that described themselves as very or extremely confident about their security had still experienced an incident.

The metrics that most IT teams are using to assess their own posture (tool inventory, control checklists, audit completion rates), are not reliably predicting outcomes. A more honest, outcome-focused approach to security assessment is a survival requirement in the present and future environment

> Organisations that will navigate the next three years most successfully are not necessarily those with the largest budgets. They are those that close the gap between knowing and doing, those that treat the confidence gap not as a reason for comfort but as a roadmap for investment.

RECOMMENDATIONS FOR IT LEADERS

1 Audit your confidence, not just your tools. If your team rates current security highly, stress-test that assessment against actual incident history, control coverage, and compliance posture. Confidence without evidence is a liability, and the data in this report makes the cost of that liability plain.

2 Treat tool consolidation as a security priority, not just an operational one. Every additional tool in your remote access stack is a potential gap. Fewer, better-integrated tools with centralised logging and access control consistently outperform large stacks.

3 Close the Zero Trust intention gap. If Zero Trust is on your priority list but not yet implemented, define a concrete roadmap with measurable milestones. Start with the highest-risk access paths: remote vendor access, privileged accounts, and unmanaged devices. Then, build from there. Stating a priority without executing against it is exactly the dynamic that the security intention gap describes.

4 Make vendor security track record a purchasing criterion. 71% of respondents rate this as critical or very important. Apply the same rigour to vendor selection as you do to your own security posture. Demand evidence of update cadence, incident response practice, and compliance certification. The tools you use carry their own risk profile.

The data shows that the incident rate for organisations running four or more tools incidents is at 67%, compared to 28% for those running one.

5 Address the operational burden directly. If security hardening is being deprioritised because of the time spent managing security challenges, that is a structural problem.

6 Communicate the future confidence gap upward. If your team is significantly less confident about the three-year outlook than the current state, what you should be looking at is a board-level conversation. **Frame it as a risk trajectory, not a current status report,** and pair it with a concrete investment proposal that closes the gaps the data reveals.

For more information about RealVNC's approach to secure remote access, or to discuss the findings in this report with our team, visit realvnc.com.

BONUS CONTENT

HOW MYTHOS AND OTHER AGENTIC AI CREATE THE ULTIMATE THREAT FOR LEGACY REMOTE ACCESS

The research you've just read reveals a clear consensus among IT professionals: the remote access threat environment is accelerating, and organizations are struggling to keep up. While much of the anxiety surrounding artificial intelligence focuses on novel attack methods, the most immediate danger lies in how automated systems interact with the infrastructure organizations already have in place.

Recent advancements in automated vulnerability discovery, such as Anthropic's Mythos, represent a fundamental shift in the security landscape. For organizations that rely on open source VNC or older embedded remote access variants, particularly in manufacturing and highly regulated industries, this development demands a serious risk reassessment.

We look at what automated vulnerability discovery means in practice, and why the window for securing legacy remote access is rapidly closing.

The Confidence Paradox

The defining feature of the current remote access security landscape is the confidence paradox. IT leaders express high confidence in their security posture while simultaneously experiencing high incident rates. Automated vulnerability discovery will soon make this paradox much more difficult to ignore.

It is important to understand that these automated tools do not just grab new vulnerabilities out of thin air. What they do is to dramatically lower the cost and the skill barrier required to find and exploit long-standing weaknesses in old codebases. In recent demonstrations, automated agents have hypothesized bugs, written execution scripts, and successfully exploited decades-old vulnerabilities in widely used software.

Flaws that survived millions of automated testing attempts over fifteen years were identified and exploited by these systems in a matter of hours. Furthermore, engineers with no formal security training were able to use these tools to generate complete, working exploits.

This changes the mechanics of cyberattacks. Historically, finding a new exploit in a niche embedded VNC client required a highly skilled researcher. This researcher was spending weeks analyzing code, which was a targeted and expensive endeavor. Soon, it will be a low-cost, automated, process.

The technology simply reveals an insecurity that was always there, making it economically exploitable at an unprecedented scale. If an organization bases its confidence on the belief that its legacy remote access tools are too obscure or too deep

HOW MYTHOS AND OTHER AGENTIC AI CREATE THE ULTIMATE THREAT FOR LEGACY REMOTE ACCESS

inside the network to be targeted, that defensive assumption is no longer valid. These tools never tire and can go on until they find a vulnerability.

Operational Burden

This change of affairs matters enormously for manufacturing and operational technology environments. Industrial control systems, human machine interfaces, and OEM appliances heavily rely on open source VNC variants.

These codebases are often decades old and written with manual memory management. They represent precisely the environment where memory corruption bugs hide, and they are the exact type of flaws automated analysis is great at finding. Vulnerable VNC code frequently gets reused across multiple projects. Because not all developers track upstream library updates, derivative products can remain vulnerable long after the original project issues a fix.

For the manufacturing sector, which our research shows already struggles with infrastructure debt and deprioritized platform upgrades, this creates a massive exposure surface.

The emergence of automated vulnerability discovery collides directly with the operational burden. Security teams are already consumed by managing day to day challenges. When automated systems begin accelerating the pace of vulnerability disclosure, this burden will become hard, if not impossible, to sustain.

In typical corporate IT environments, patch management is a procedural challenge. In operational technology and regulated environments, patch latency is structural. Devices are tied to strict production schedules. Applying a patch to an active manufacturing line is not a standard maintenance task, as it requires a controlled outage.

When attackers operate at machine speed, using automated tools to generate exploits, and defenders operate at a much lower speed, the latter are at a severe disadvantage. This mismatch is exacerbated by unmaintained VNC variants. Older forks have no upstream development, meaning no patches are likely to ever be released. Any newly discovered bug in that codebase becomes a permanent zero day vulnerability for every site still running it.

Compliance and Documentation Weight

For finance, healthcare, and other highly regulated industries, the implications extend far beyond technical risk. Frameworks like NIS2, IEC 62443, and various federal regulations all expect demonstrable control over remote access pathways and rigorous vulnerability management.

A sudden explosion of disclosed legacy VNC vulnerabilities will likely immediately translate into a massive compliance and documentation burden. When systems cannot be realistically patched due to operational constraints or unmaintained software, organizations will be forced to generate endless compensating control documentation, risk acceptance approvals, and auditor justifications. The administrative weight of proving compliance while running inherently vulnerable remote access software will drain the very resources needed to modernize the infrastructure.

This directly highlights the security intention gap identified in our survey. Organizations know they need unified access controls, but implementation lags far behind intention. With automated vulnerability discovery, closing this gap is an immediate operational need, rather than a three-year plan.

Practical Direction for the Next Three Years

Direct internet exposure of any legacy remote access service becomes indefensible in this environment. To protect the organization against the coming wave of discovered vulnerabilities, IT leaders must move from attempting to patch legacy software to isolating it entirely.

First, remove all unsecured remote access services (like open source VNCs) from direct internet exposure. Switch to a modern secure remote access solution that creates a secure tier where remote protocols never go through untrusted networks. This neutralizes entire classes of future vulnerabilities by making them physically unreachable. This solution should enforce multi-factor authentication, record sessions, and apply strict, per-asset authorization before any connection reaches the endpoint.

For more information about RealVNC's approach to secure remote access, or to discuss the findings in this report with our team, visit realvnc.com.