EMERGING THREATS IN TECHNOLOGY & SAAS

The High-Incident Security Paradox

TABLE OF CONTENTS

INTRODUCTION

Technology and SaaS organisations are often viewed as leaders in cybersecurity maturity. They typically adopt new technologies quickly, invest heavily in security tooling, and demonstrate high awareness of emerging threats. Yet the findings from RealVNC's research reveal a more complex picture.

Despite strong confidence in their security posture and relatively high adoption of AI-powered security tools, Technology and SaaS organisations reported one of the **highest remote access incident rates** in the study. Concerns about phishing, insider threats, and AI-driven attacks continue to grow, while operational complexity and competing priorities make security improvements difficult to implement.

This report explores the unique remote access security challenges facing the Technology and SaaS sector, highlighting where confidence, risk, and reality diverge.

Should you want to get a picture of what things look like for other industries, feel free to **check out our free Emerging Threats in Remote Access Security Report and Webinar.**

EXECUTIVE SUMMARY

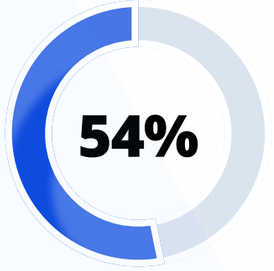
RealVNC surveyed **323 IT professionals** across seven major industries to understand how organisations perceive, experience, and plan to address emerging threats in remote access security. Technology and SaaS organisations made up the largest share of respondents, and their results stand out as one of the study's clearest paradoxes.

On paper, this is a sector that should be ahead of the curve: strong AI tool adoption, high MFA implementation, and broad awareness of the threats it faces. In practice, **54% of Technology and SaaS organisations** reported a remote access incident **in the past 24 months**. This is a joint-high across every industry surveyed, and one that sits alongside a **59% overconfidence-and-breach rate** among respondents who described themselves as very or extremely confident in their security.

The gap is not one of awareness or intent. Technology and SaaS security teams know what the threat landscape looks like, and they know what needs to change. What consistently gets in the way is operational complexity: fragmented tool stacks, competing priorities, and the day-to-day burden of managing existing security challenges, which leaves little bandwidth to close the gaps that matter most, with Zero Trust chief among them.

This edition brings together the Technology and SaaS findings from RealVNC's Emerging Threats in Remote Access Security report. A closing section then looks at how an on-premise approach to remote access can help address several of the specific gaps this research identifies.

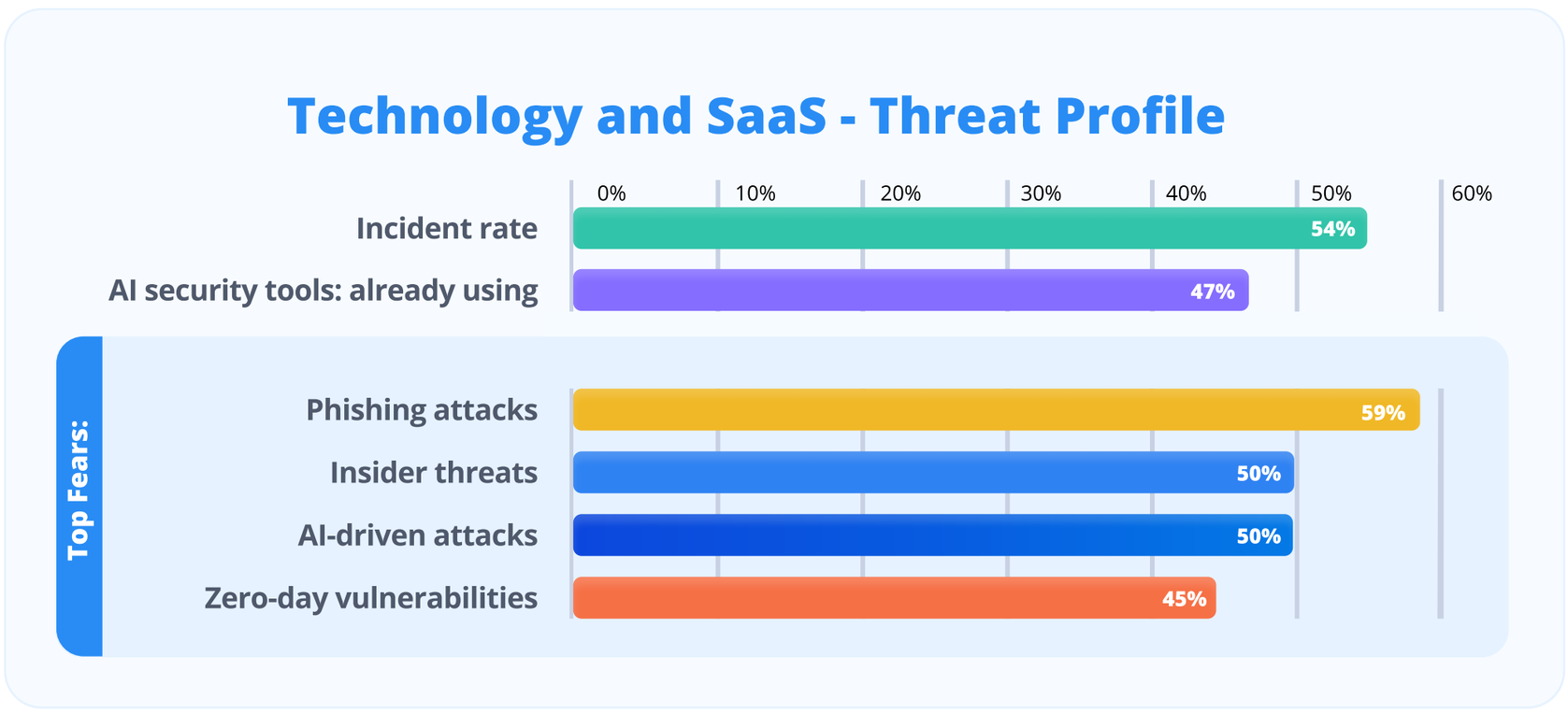
In practice, ***54% of Technology and SaaS organisations*** *reported a remote access incident* ***in the past 24 months***



Technology & SaaS organisations reported a remote access incident in the past 24 months.

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. Yet, it has a 54% incident rate, a joint-high of any industry. Let's see how respondents in this sector view things.

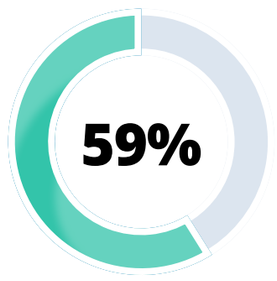


The threat profile here is distinctive. Phishing leads, **at 59%**, as it does in most sectors. But **insider threats (50%)** and **AI-driven cyberattacks (50%)** tie as the second most feared threats. These are levels significantly higher than in most other industries. This reflects the nature of tech 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.

THE CONFIDENCE PARADOX

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.



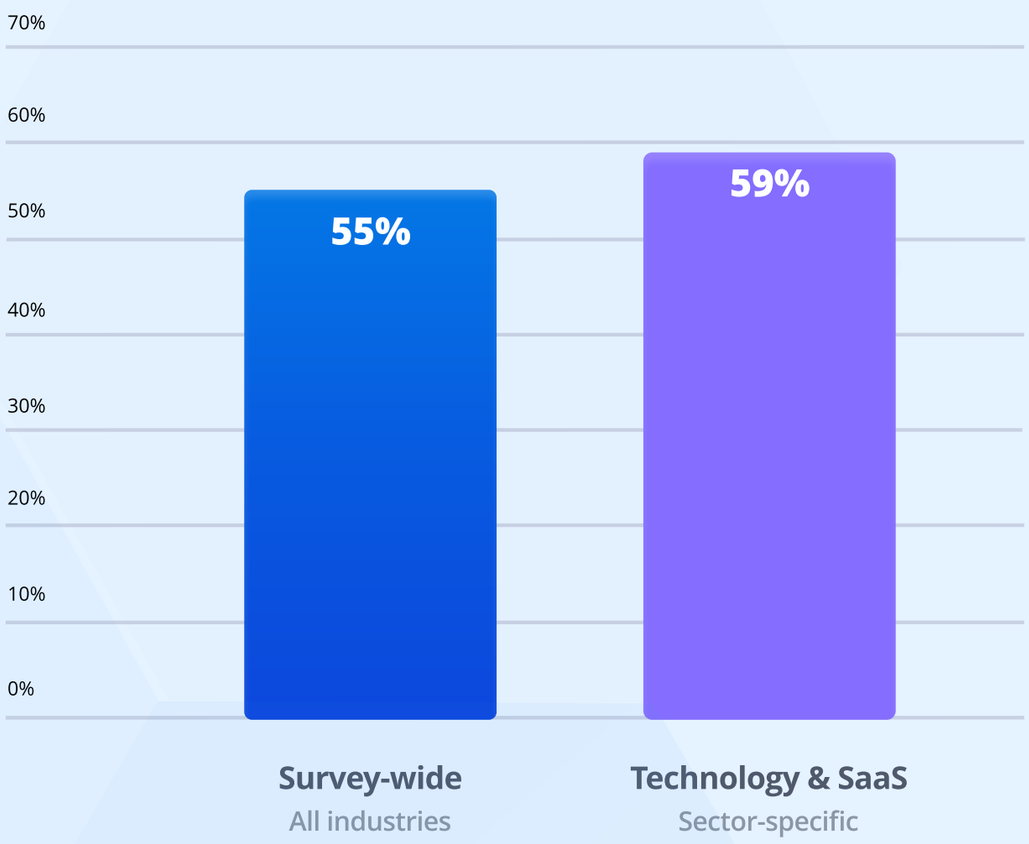
of Technology & SaaS respondents who rated themselves very or extremely confident still experienced a remote access incident

That overconfidence-and-breach rate sits above the survey average. Across all industries, **66% of respondents** described themselves as very or extremely confident in their current security, and of those, **55%** had still experienced an incident in the past 24 months. Technology and SaaS follows the same broad pattern, but more sharply, with a **59%** overconfidence-and-breach rate that sits among the highest of any sector, despite the sector reporting some of the strongest security fundamentals in the survey, including high AI adoption and regular auditing.

Across all industries, ***66% of respondents*** *described themselves as very or extremely confident in their current security,*

Overconfidence and breach rate

Survey-wide vs. Technology & SaaS, percentage of of respondents who rated themselves very/extremely confident, but still had an incident in the past 24 months



THE ZERO TRUST LAG

Technology organisations have the highest MFA implementation rate in the sector analysis. 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.

60%
cite Zero Trust as a top priority

vs

32%
have actually implemented it

The Zero Trust lag: intent vs. delivery

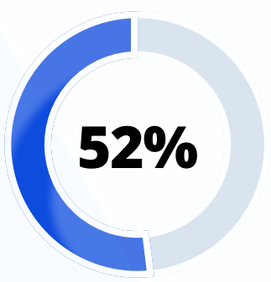
OPERATIONAL BURDEN

52% of Technology and SaaS respondents have deprioritised security hardening due to the time spent managing existing remote access security challenges, one of the highest rates of any sector, behind only **education (60%)** and ahead of **manufacturing (47%)**.

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, prioritisation matters more than any single tool or control. Security teams already know where the gaps are. Closing them depends on executive alignment and the discipline to focus on a few things instead of everything at once.



Technology & SaaS organisations have deprioritised security hardening due to time spent managing existing security challenges

LOOKING THREE YEARS AHEAD

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.

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.

KEY TAKEAWAYS

The Technology and SaaS sector understands the threat landscape better than most. Organisations recognise the importance of Zero Trust, invest in AI-enabled security capabilities, and maintain strong security awareness.

However, awareness alone is not translating into stronger outcomes.

The research points to a recurring challenge: security teams know what needs to be done, but operational complexity, tool sprawl, competing priorities, and implementation barriers continue to slow progress.

As threats evolve and AI accelerates both attack and defence capabilities, the organisations most likely to succeed will be those that focus on simplification, prioritisation, and closing the gap between security strategy and execution.

> The next phase of security maturity for Technology and SaaS organisations is not about adding more tools, but rather about making existing controls, processes, and investments work more effectively together.

The closing section of this report looks at one practical starting point: how an on-premise approach to remote access can help close some of the specific gaps identified here.

> "The problem is not knowing what to do. It is in choosing what not to do, and building enough executive alignment to actually execute."

ON-PREMISE REMOTE ACCESS: A PRACTICAL NEXT STEP

The findings in this report point to a common thread. Technology and SaaS teams already know what needs to change, but they rarely have the operational capacity to act on it. For organisations working through that gap, particularly around Zero Trust, insider threat exposure, and tool sprawl, an on-premise approach to remote access is worth considering.

Keeping remote access on-premise means session data, credentials, and connection activity stay inside an organisation's own network instead of an outside cloud provider. That addresses the insider threat and data exposure concerns that half of all Technology and SaaS respondents named as top fears. Layered with strong encryption, two factor and device level authentication, and the option of an air gapped deployment, it also supports compliance readiness, a priority that 60% of respondents named across the survey for the next three years, including alignment with frameworks like GDPR, HIPAA, and ISO.

Below are five specific pain points this report surfaces, and how the RealVNC On-Prem Management Console addresses each one.

1 **Zones, for Segmented Networks**

Not every network is flat, and not every organisation wants every device talking to every other. Zones let you enforce stricter rules for how traffic flows in segmented or complex topologies and edit them as your network evolves. It's a practical route toward Zero Trust without a full overhaul of your architecture.

2 **Who Accessed That, and When?**

When an incident happens, or an auditor asks who connected to what and when, you need an answer fast. Audit logs give real time records of every connection: when it started, whether authentication succeeded, and when it ended, searchable by date or event type and exportable as CSV. Because users sign in with individual credentials, every connection ties back to a named person.

3 **A Quick Health Check of the Environment**

Rather than piecing together information from multiple sources, the Dashboard gives IT admins a single view of license usage, active and dormant devices, and session counts. That makes it easier to catch problems, like usage creeping toward a limit, before they escalate.

4 **Lots of Licenses and Endpoints**

Licensing is held centrally, so admins upload a key once and devices pick it up automatically when they check in. That removes the need to deploy licenses across every server individually, a task that only gets more tedious as the endpoint count grows.

5 **A Staff Member Left, We Need to Tidy Up**

When someone leaves or changes roles, the console makes it easy to remove access and cancel a device's license without uninstalling anything, including bulk user management via CSV upload. Credentials and licenses don't linger as security or cost liabilities.