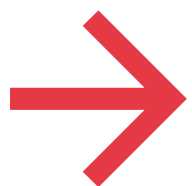




2025 UK Cyber Resilience Report

The state of UK SMB's cybersecurity response





Foreward

Cybersecurity has never been easy. But in 2025, it's been relentless.

The threat landscape is expanding, budgets are under scrutiny and trust in the tools we've banked on for years? It's fading fast.

In the past twelve months, the UK has seen high-profile outages, targeted attacks on public services, and official warnings urging greater digital resilience. Not just across critical infrastructure, but across every layer of the ecosystem.

When you throw in geopolitical instability and political shake-ups, one thing is clear: security leaders are navigating uncertainty on every front. It's a demanding environment, especially when teams are stretched thin.

This year's report doesn't just highlight the usual challenges – alert fatigue, insider threats, skills shortages etc. – but more importantly, it signals a shift in mindset.

No longer are we in an era of point products and patchwork platforms. Instead, security has to work in sync. Leaders are done stitching together disconnected tools. The new way forward is clear: simplify, unify, automate.

This move towards coordinated layers is well underway. Security leaders are looking to strip out the noise, accelerate response time and return control to the teams on the front lines.

Because when chaos is the constant, clarity isn't just a competitive edge. It's how UK organisations can get ahead.



Ed Macnair

CEO, TrustLayer



Contents

01	Threats up, budgets down	4
02	Cyber noise is the new threat	5
03	Security gaps exposed	6
04	The real insider threat	7
05	Fear, fatigue and fallout	8
06	The cloud app dilemma	9
07	The proxy problem	10
08	Security pressure points	11
09	Control through consolidation	12
10	The power of layers	13
11	Your 2025 security playbook	14



01

Threats up, budgets down

The last 12 months have been an uphill battle with more threats and fewer resources. As cybercriminals are scaling up their operations, security budgets are scaling back.

Security leaders are being hit from all sides - AI-driven scam, ransomware, cloud misconfigurations and business email compromise. Attacks are increasing in volume, complexity and impact. But while the threat landscape grows, **the average security budget dropped by 16.6% whilst battling 7% more alerts** compared to the previous year.

Security teams aren't just doing more. They're doing more with less.

➔ Top cyber challenges in 2025

In the last 12 months, which cyber incident has your organisation suffered?

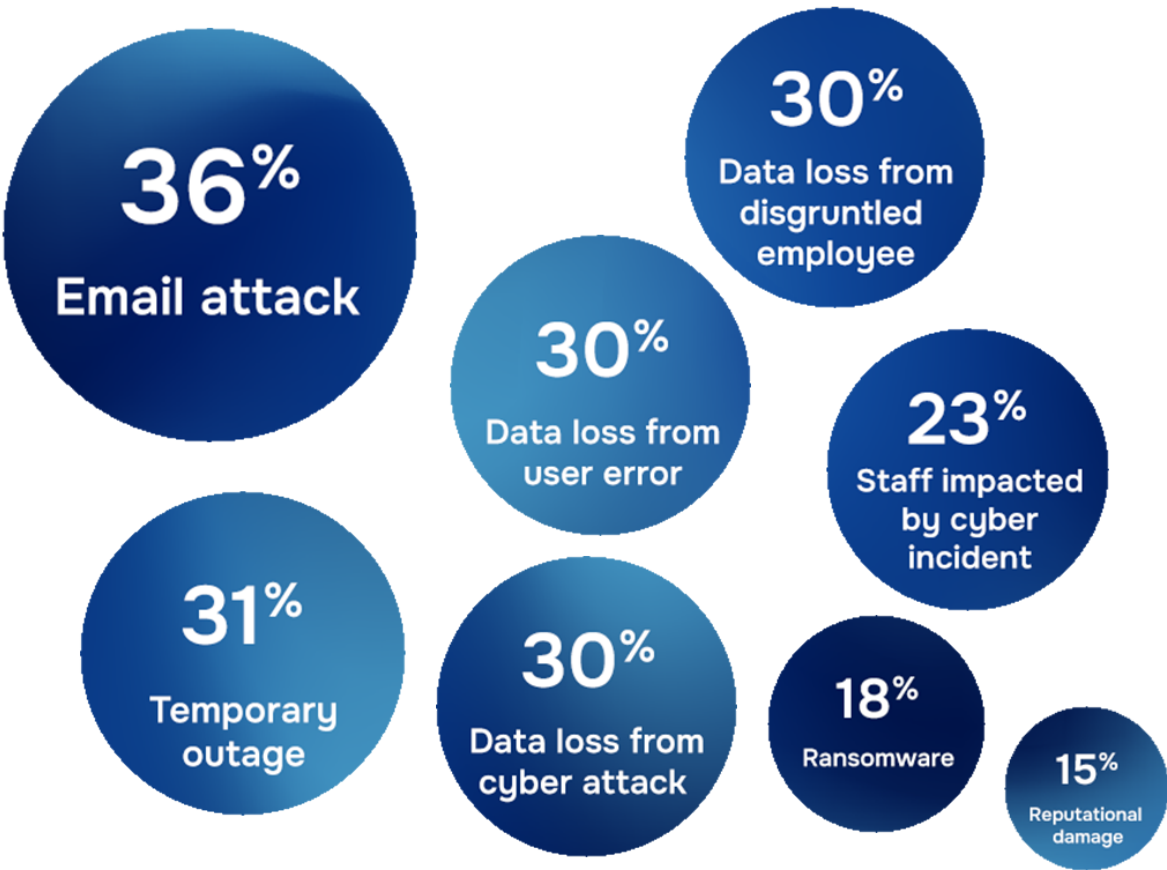


Figure 1. Most common impacts of cybersecurity incidents on UK businesses

01

Threats up, budgets down

The 2025 reality for UK SMBs:



Email attacks still dominate

Email continues to be the leading entry point for attackers. In 2024, **36% of businesses experienced an email-related security incident.** That's more than double the rate reported in 2021.

It's not just volume that's increasing, it's the sophistication. AI is helping attackers craft more convincing phishing messages. Some are now exploiting internal platforms and trusted relationships to bypass traditional filters. The reality? The threat is evolving faster than most defences can keep up.



Operational disruption is rising

The impact of attacks is not just limited to data breaches. In 2024, **nearly a quarter of UK organisations experienced a major outage lasting longer than a day.** That's a 16.2% increase on the previous year.

Shorter outages are even more common. One in three businesses faced downtime of less than a day. As digital reliance increases, single incidents now trigger wider consequences across supply chains and service providers.



The budget gap is growing

The average cybersecurity budget dropped to £80,136 in 2024, down from £96,138 the year before. It is a significant cut, arriving at the exact moment when pressure on security teams is intensifying.

While email protection remains widespread, coverage elsewhere is inconsistent. Just **67% of SMBs have web security in place. Only 58% protect their cloud applications.**

Organisations aren't falling behind due to choice – they're underfunded.

“There's no blank cheque for cybersecurity, and right now, there's even less to go around. What we're seeing is a demand for security strategies that are not only effective, but financially sustainable. As a CFO, that means prioritising spend that reduces risk, protects operations, and supports long-term resilience.”

Mark Prater
CFO | TrustLayer

02

Cyber noise is the new threat

Security teams are facing a growing operational burden. As the volume of alerts rises, it's becoming harder to separate the real threats from the background noise.

The average organisation now receives 875 security alerts a day. That's a **34% increase since 2022**. The figure has risen for three consecutive years as detection tools multiply and the threat landscape continues to expand.

More alerts should mean more protection. In practice, it often means more distractions, more manual work, and a greater chance of missing what actually matters.

For already stretched teams, this is critical. When everything is flagged as urgent, how do you tell what really is?

1. A growing divide between sectors

The impact isn't spread evenly. The private sector has seen a 61.9% surge in daily alerts since 2022, now averaging 1,164 per day. Meanwhile, public sector alerts have dropped by 44%, with teams handling just 359 per day.

Security policies, reporting rules, and attacker behaviour may explain the gap. But the reality is clear: private sector security teams are carrying a heavier operational load.

2. More alerts, less clarity

Teams are seeing that more alerts does not always mean better security. When everything is flagged, it becomes harder to spot what really matters. In fact, **34% of security leaders feel overwhelmed with the level of alerts**.

As the gap grows between attack volume and available resources, the risk of missed incidents increases. Alert overload isn't just inefficient, it's a security risk.

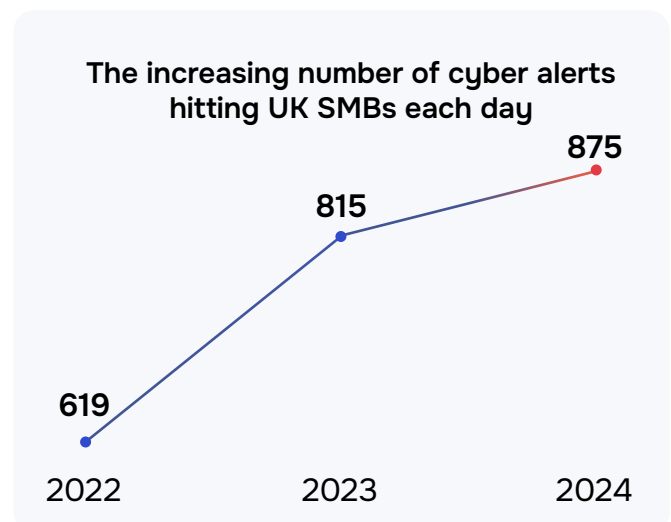


Figure 2. Daily cyber alerts targeting UK SMBs, 2022–2024

03

Security gaps exposed

Hopes have been high after four years of steady improvement, but this year saw a sharp drop in protection levels across the board.

On average, **businesses are now on average 9.7% less protected across all threats** than they were a year ago. It's a worrying shift, happening just as threat tactics become more advanced and more adaptive. So where are security teams falling behind?



Cloud security is still a weak spot

77% of businesses still can't continuously audit their cloud storage and containers.

As organisations increase their reliance on cloud services, blind spots are multiplying – and attackers know exactly where to look.



The struggle to stop CEO fraud

67% of companies were unable to stop attackers impersonating executives, up 11% year-on-year.

With deepfakes and AI-generated phishing in play, these scams are getting harder to detect – and harder to stop.



Email defences aren't keeping up

Despite years of investment in email security, 64% of organisations still can't quarantine suspicious messages. That's a 9% increase from last year.

At the same time, email threats are becoming more targeted, more convincing, and increasingly AI-driven.

The top 5 cybersecurity threats UK SMB's experienced in the past 12 months

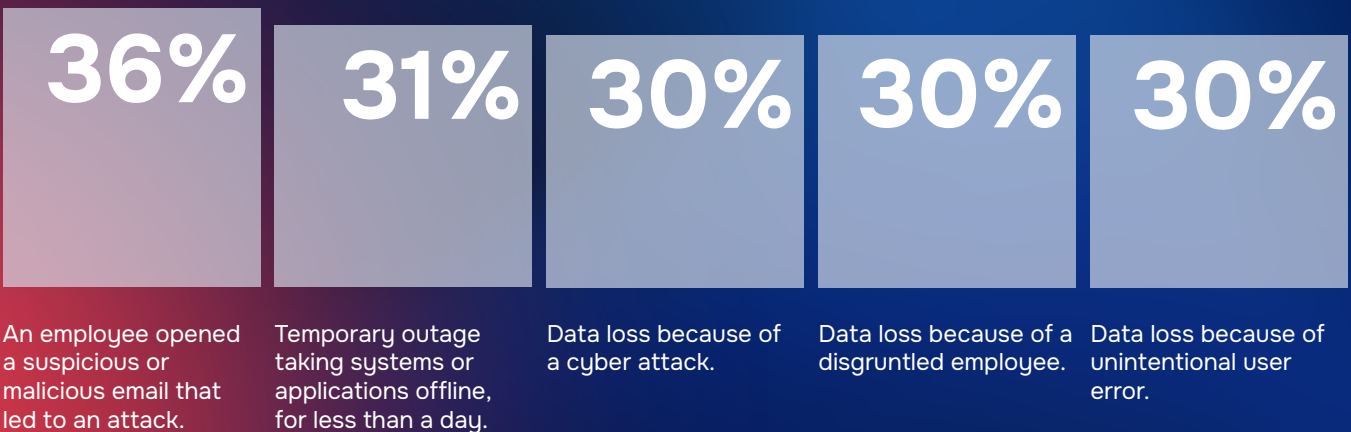


Figure 3. Top cybersecurity threats faced by UK SMBs

03

Security gaps exposed



Ransomware is still getting through

62% of organisations still struggle to stop ransomware.

But it's not just about getting in. Attackers are going after backups, moving laterally across systems, and using multiple channels to increase the damage.



Attackers are exploiting the gaps

More than 60% of companies say they can't fully contain threats that move across email, cloud and web.

When defences are siloed, attackers exploit the cracks between them. Too many businesses are still defending in isolation.

“Alert volume is out of control. We’re asking security teams to operate in a constant state of triage, and it’s unsustainable.

If we want to close the gap between detection and defence, platforms need to do more than just flash up alerts and threats. They need to understand and act on them.”

Gareth Lockwood
Chief Product Officer | TrustLayer

04

The real insider threat

Security teams spend most of their time looking outward – stopping phishing, malware, and external breaches. But some of the biggest risks come from inside the organisation.

Whether through negligence or intent, insider threats are responsible for a significant share of data loss. And many organisations are still struggling to contain them.

Security controls are being ignored.

IT policies only work when they're followed – and in many cases, they're not. **Nearly a third of SMBs say employees are deliberately bypassing security controls**, using unsanctioned proxies and workarounds that expose critical data.

At the same time, weak governance is giving users a free pass to download and run whatever applications they want. Without proper oversight, security teams have no clear view into where sensitive data is being stored, shared, or accessed.

Insider data leaks are on the rise.

Insider threats take two main forms: malicious intent and human error. Both are proving costly. **Disgruntled employees were behind data loss in 30% of organisations. Another 30% reported accidental leaks caused by internal mistakes.** Whether it's stolen IP or an email sent to the wrong person, internal risks are proving just as damaging as external threats.

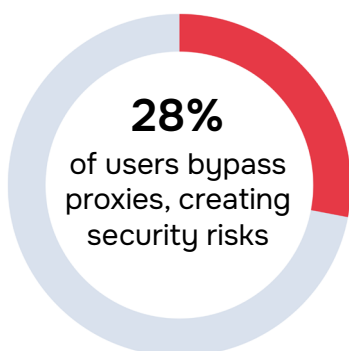


Figure 4. Users bypassing traditional network controls

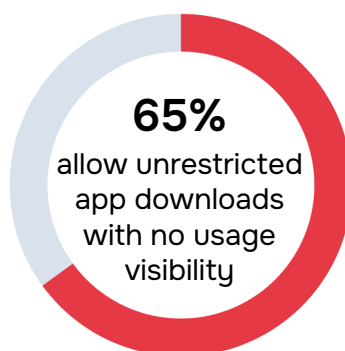


Figure 5. Unrestricted app downloads without visibility



Figure 6. Insider-driven data loss incidents

"Insider risk isn't just an HR issue. It's a security gap hiding in plain sight."

Charles Milton
VP of Strategic Alliances | TrustLayer

05

Fear, fatigue and fallout

Cybersecurity has never been a low-stress job. But this year, the emotional and mental toll is hitting a new high.

For the third year in a row, the **number one concern among cybersecurity professionals is missing a critical alert that allows a threat to slip through**. Nearly half (49%) now cite this fear – a 25% increase since 2022.

It reflects a growing anxiety that the net is widening, threats are evolving, and the margin for error is disappearing.

Pressure points are shifting but not easing.

The stress on UK security teams isn't easing. In some areas, it's getting worse.



43% of security leaders received a call in the middle of the night to investigate an incident – up 50.9% since 2022.



35% had annual leave interrupted due to an alert.



34% reported feeling overwhelmed by the volume of alerts – a slight drop from 2022.



34% suffered sleep deprivation due to cybersecurity concerns – up 52.5% since 2022.

This isn't just disruption, it's burnout. Personal time is under constant threat. Security doesn't clock off, and neither do the people behind it.

Organisations suffering poor morale due to cybersecurity and related compliance

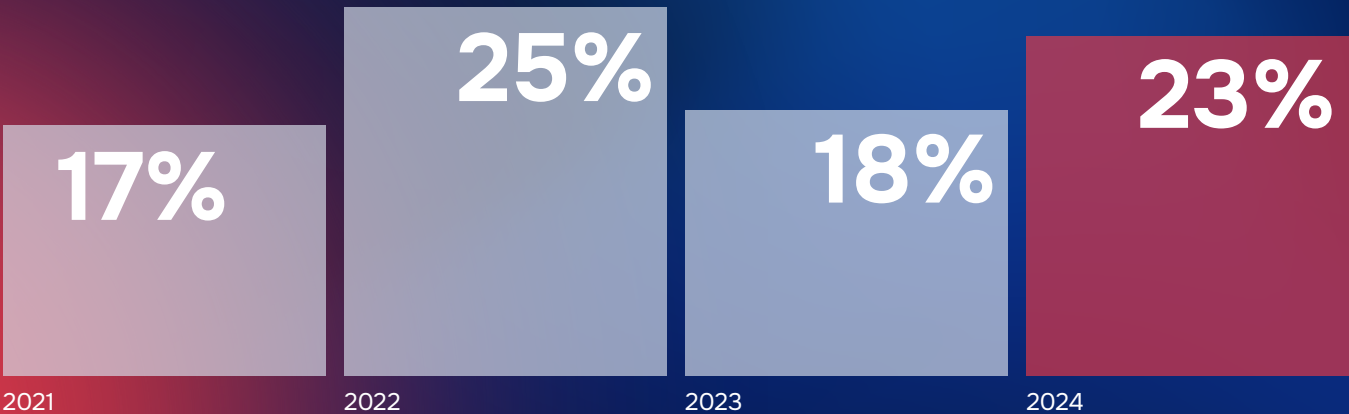


Figure 7. Percentage of organisations reporting low morale due to cybersecurity and compliance pressures, 2021–2024

05

Fear, fatigue and fallout

Morale is taking a hit.

The strain isn't limited to security teams. Morale is falling across the wider business.

Between 2023 and 2024, there was a 7.5% rise in organisations reporting low morale because of a cyber incident and/or resulting compliants. Since 2021, that figure has jumped 39.4% – with customer service and support teams among the hardest hit.

Cybersecurity isn't just a technical problem. It's a people problem. And it's creating cultural and

Cyber professionals who fear missing a cyber alert with their current tech stack:

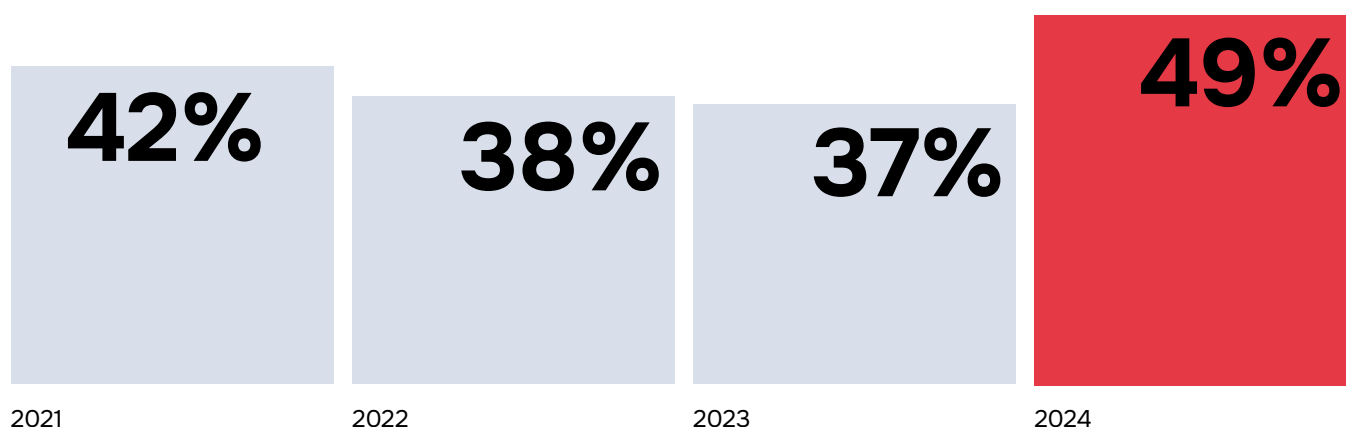


Figure 7. Percentage of cyber professionals concerned about missing alerts due to limitations in their current tech stack, 2021–2024

“Cybersecurity has never been a low-stress job. But now the strain isn't just technical, it's cultural.

The emotional impact is spreading across the business, and it's showing up in performance, morale, and burnout.

We've got to stop treating this as an individual problem. It's a systems issue. Cybersecurity needs to protect people, not just data.”

Lucinda Robinson
Marketing Director | TrustLayer

06

The cloud app dilemma

Cloud apps promised freedom. What they've delivered is complexity.

Mid-sized organisations now manage access to an average of 82 cloud applications, rising to 92 in sectors like finance. But as app numbers grow, the ability to manage them smoothly hasn't kept pace.

Just **35% of organisations report being able to enable secure app downloads within minutes while maintaining full visibility into user activity**. Nearly a quarter still rely on manual approval processes that can take weeks or longer. Just 16% have a seamless process in place with a pre-approved app catalogue.

The result? Slower innovation. Frustrated users. IT teams stuck in firefighting mode..

Beneath the surface, the risk runs deeper.

But the bigger issue is posture. In the past year, misconfigured cloud infrastructure and cloud apps resulted in:



38% experienced critical business disruptions caused by misconfigured settings.



38% of IT teams spent 'excessive' time and effort manually addressing these misconfigurations.



33% reported that misconfigurations were exploited to deploy ransomware or other malicious software.



27% saw audits compromised by misconfigurations that led to gaps in compliance records.

Cloud complexity is breaking more than processes – it's breaking security. From clunky approvals to critical failures, cloud sprawl is stretching both people and systems. And it's only getting harder to manage.

"Cloud apps should drive productivity, not stall it. But the speed of cloud adoption has outpaced most organisations' ability to manage it. Misconfigurations, blind spots and manual processes have become everyday risks – not exceptions.

That's exactly why we prioritised posture management in our 2024 roadmap"

Gareth Lockwood
VP of Product | TrustLayer

07

The proxy problem

Most organisations are still relying on proxies – even as security leaders' confidence in them continues to decline:

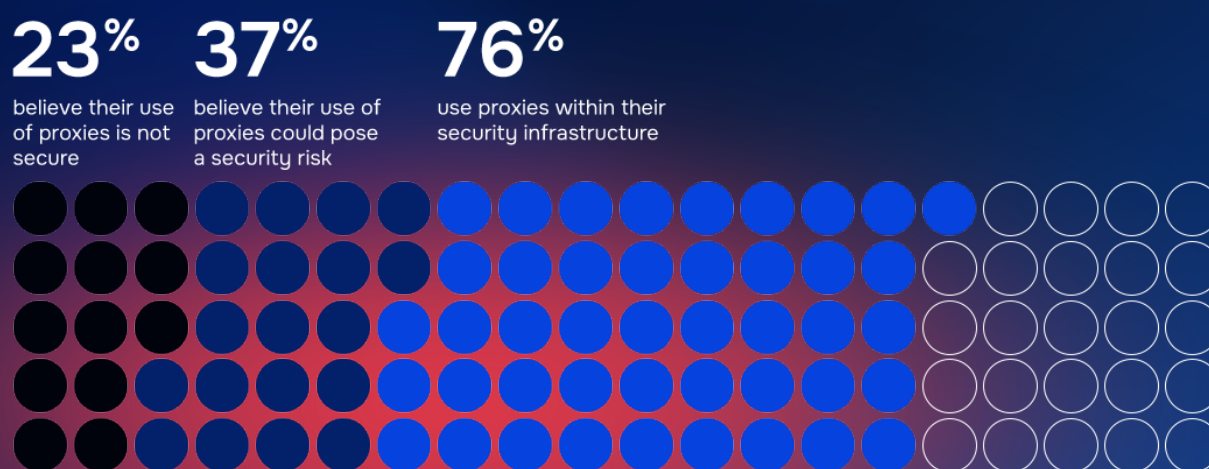


Figure 7. Perceptions of proxy use among organisations, including concerns about security and adoption within infrastructure

76% of businesses still include proxies in their security stack. In the public sector, it's even higher at 80%. But widespread adoption doesn't equal widespread trust and many organisations are starting to question whether proxies are still fit for purpose.

Doubts are growing, fast:

Over a third believe proxies pose a risk because they're prone to becoming outdated.

33% raised concerns about logged activity being accessed by unauthorised entities.

28% say their users frequently bypass them altogether – creating avoidable security gaps.

Even among those still using proxies, faith is wavering. Just **38% believe they're effective even when properly configured**. And that effectiveness comes with caveats. Many limit their use to niche roles like content filtering or anonymisation. That's not conviction, that's compromise.

Proxies are starting to look like a bottleneck.

In a world that demands agility and visibility, proxies are falling behind. They interrupt user experience, are hard to scale, and introduce fragility into environments that need to be resilient.

They've long been the go-to. But that's changing. More organisations are actively exploring alternatives that offer stronger privacy, better performance, and smarter control. Without relying on the middleman.

08

Security pressure points

The pressure on security teams isn't coming from one direction. It's budget, burnout, tech sprawl, and trust – and these five pressure points are starting to hit all at once.

Cloud security expertise is lagging behind adoption

Cloud confidence is falling. As environments grow more complex, many organisations say they no longer have the in-house skills to keep up. It's become one of the biggest concerns for the year ahead – and a growing blind spot in an increasingly cloud-first world.

Cost and complexity are slowing everything down

Security stacks are bloated and stitching them together now feels like a full-time job. Teams are spending more time maintaining their architecture than defending the business. And when budgets are tight, that complexity becomes a blocker to progress.

Internal teams are running on empty

Most security teams are already under-resourced, and they're being asked to do more with less. With so many systems to manage, alerts to triage, and incidents to contain, the day-to-day has become unsustainable. The burnout risk is real, and it's accelerating.

Hiring and retention are getting harder

The talent shortage hasn't improved but it's not just about hiring anymore. Organisations are struggling to hold on to experienced security professionals. And when senior team members leave, they take critical knowledge and context with them.

Automation still isn't trusted

Automation is widely seen as the way forward, but confidence in safe deployment is holding teams back. Concerns around outages, misconfigurations and unintended consequences are slowing adoption, even when the intent is there.

Top cybersecurity challenges for UK security leaders:

- #1 The cost and complexity of cybersecurity tech stacks
- #2 Recruiting specific cybersecurity professionals
- #3 Keeping up with the evolving threat landscape
- #4 Lack of knowledge around AI and its use
- #5 Lack of cloud security expertise

“Security teams aren't short on ambition – they're short on time, talent, and trust in the tools they're using.

This year's challenges go beyond just stopping threats, they're about ensuring the right people, skills, and clarity are in place to maximise the effectiveness of existing technology.”

Ryan Murphy
Sales Director |
TrustLayer

09

Control through consolidation

Security teams are slimming down their stacks – not just to cut costs, but to stay in control.

Since 2021, the average number of cybersecurity products in use has dropped from 24.1 to 20.1 – a 16.6% decrease. Public sector organisations led the way, cutting tools by 33%, compared to just 5% in the private sector.

But this isn’t about cutting corners, it’s about taking control. Fewer tools means fewer silos, tighter integrations, and lower costs. **58% of UK SMBs said cutting costs was the main driver behind reducing their number of vendors, closely followed by 54% who consolidated to strengthen their cybersecurity.**

Consolidation makes it easier for internal teams to manage security day to day – especially when they’re stretched thin. This isn’t just a trend, it’s about survival as alert fatigue rises and the threat multiply. Bringing tools together is one way to regain control without losing visibility or capability. That’s why private sector companies are leading the charge.

But not everyone’s moving at the same pace. Some public sector organisations are now reversing course. In the last year, 86% chose to maintain or even expand their supplier list – possibly due to different internal pressures, or slower adoption of consolidation strategies.

Either way, the direction is clear: security teams are rethinking what belongs in their stack, and what doesn’t.

Reason for reducing vendors:	Private sector	Public sector
To get better cyber protection	49%	80%
To save money	64%	24%
To reduce silos between point products	44%	19%
To reduce vendor management workload	29%	14%

10

The power of layers

Security leaders are moving away from patchwork tools – and towards layered defence built to move as one.

80% of organisations now use cybersecurity products that automatically share event data across channels to stop multi-vector attacks as they happen. The result is faster response, fewer blind spots, and less manual work.

And appetite for that kind of coordination is growing. In 2024, 92% of organisations said they plan to invest in a solution that connects cloud, web and email security – the fourth consecutive year that number has risen.

But while the trend is clear, confidence in how it works isn't always guaranteed.

AI trust is being tested

Confidence in AI faltering. Only 12% of organisations say they have full trust in AI to power their security – down from 16.7% last year.

At the same time, the number of businesses that say they don't trust it at all has more than doubled.

That hesitation isn't about rejecting automation. It's about having transparency, visibility, and the assurance that AI helps rather than hinders. As more security tasks shift towards automation, trust will need to be earned – not assumed.

Consolidation is now a business priority

Security leaders aren't just searching for new tools. They're looking for ways to buy back time, reduce cognitive load, and get ahead of threats that move faster than ever.

That's why coordination matters more than ever. It's not about chasing a monolith. It's about layers that work together, by design.

The challenge now is getting there without losing control, clarity, or confidence along the way.

“Cybersecurity leaders aren't just asking for better tools. They're demanding a better approach. The cracks in traditional security stacks are impossible to ignore, and relying on stitched-together point products is no longer sustainable.

Integrated solutions that bring key protections together are becoming essential. When cloud, web, email and user protection work in harmony, security teams gain the clarity, control and speed they need to stay ahead of what's next. This isn't just a shift in tooling. It's a shift in mindset.”

Ryan Murphy Sales Director | TrustLayer

11

Your 2025 security playbook

Security leaders are rewriting the playbook. It's no longer about stacking tools. It's about building coordinated layers of defence that are agile, intelligent, and human-aware. Here's what that looks like in practice:

01 Consolidate to take control

Start with less, but make it work harder. Consolidating your stack only works when each layer earns its place.

That means picking tools that reduce overlap, talk to each other, and make life easier for the people using them. Less noise with more control.

02 Automate the right things

Automation works best when it clears space, not adds complexity. The goal isn't to replace people, it's to give them time back.

Whether it's triaging alerts or enforcing posture, automate what slows you down so your team can double down on what matters.

03 Tighten your cloud posture

Cloud sprawl creates risk you can't see coming. Strong posture starts with visibility, but it takes policy enforcement and seamless approvals to lock things down.

Make sure your cloud setup is easy to manage and hard to mess with.

04 Design for the human

Security doesn't work without the people who run it. Burnout, alert fatigue and low morale slow everything down. The fix isn't just technical.

Build operations that protect your team as well as your data, and you'll move faster where it counts.

05 Invest with impact

You can't spend your way out of risk. The smartest investments do more than defend.

They connect, adapt and scale without draining your team or your budget. Spend where it gives you space to breathe.

+ Get full-spectrum visibility

You can't defend blind spots. Make sure you have visibility across users, devices, cloud and data. That clarity helps you spot risks early and act with confidence.

+ Build on live intelligence

Security that stands still falls behind. Use real-time insights into user behaviour and emerging threats to keep your defences one step ahead.

The way forward isn't more tools. It's smarter security.

TrustLayer helps you see more, do more and secure more by connecting protection across email, cloud and users. **Let's make 2025 the year security gets smarter.**

Email sales@trustlayer.co.uk or call +44 (0) 845 230 9590.

About this report

The goal of our 2025 UK Cyber Resilience Report is to lay bare how SMBs' cyber readiness has been impacted in the last four years.

It sets out how SMBs fared under attacks in the last 12 months. And why IT leaders desire sophisticated and layered security solutions.

The results represent the opinions of 280 IT leaders working in SMBs across the UK. The research was conducted in partnership with market research specialist, 3Gem between 8th – 21st January 2024.

About TrustLayer

TrustLayer makes it easy for mid-market organisations to secure their environment the direct way.

One platform covers email, web, apps, users and posture, all working together without rerouting traffic or interrupting workflows. Deploy protection quickly and keep it running smoothly, from phishing prevention to app control.

TrustLayer keeps security clear, connected and ready to grow with you. It's cybersecurity, the direct way.



TrustLayer™