

UK cyber resilience crisis deepens as SMBs struggle with alert overload, cloud blind spots and insider threats, reveals TrustLayer

Monday 4 August, 2025

TrustLayer's Cyber Resilience Report 2025 exposes the widening gap between security expectations and operational realities.

London, UK – 4 August 2025

TrustLayer today launches its fourth [UK Cyber Resilience Report](#), revealing UK SMBs face a critical crossroads in cybersecurity.

The report identifies an alarming disconnect between what security teams are tasked to protect and what their technology stacks enable them to achieve. With security budgets shrinking by an average of 16.6%, and alerts rising by 7% year-on-year, UK SMBs find themselves increasingly outmatched by the speed and scale of cyber threats.

According to TrustLayer's findings, visibility gaps in cloud applications, fractured security toolsets, and unmanaged insider threats are placing enormous pressure on teams already stretched thin. The report warns that outdated and disconnected tools are no longer merely inefficient; they represent a strategic risk.

"Cybersecurity has fundamentally changed, but the way organisations build their defences has not kept up," said Ed Macnair, CEO at TrustLayer. "Attackers leverage automation and AI at massive scale, exploiting blind spots created by siloed tools. Meanwhile, SMBs are trapped in reactive mode, managing alerts rather than stopping breaches. This approach isn't sustainable."

Email, cloud and insider threats dominate

TrustLayer's research highlights three key threat areas where defences consistently fail:

- **Email attacks remain rampant:** More than one-third (36%) of organisations reported serious security incidents stemming from email, almost double the rate reported four years ago. Despite continued investment, email-based breaches are still slipping past legacy defences.
- **Cloud visibility is dangerously limited:** 77% of SMBs cannot continuously monitor cloud data and container risks, leaving substantial security gaps. With business-critical operations increasingly moving to the cloud, these blind spots are becoming primary targets for threat actors.
- **Insider risks escalate:** Nearly one in three (30%) data loss incidents originate from employees, either unintentionally or maliciously. Weak governance, combined with limited internal controls, is amplifying risks from within the organisation itself.

Alert fatigue and burnout: The hidden human cost

It's not only technology under strain; human capital is fraying at the edges. TrustLayer found that nearly half (43%) of cybersecurity teams have faced middle-of-the-night alerts, disrupting sleep and contributing significantly to stress and burnout.

Ryan Murphy, Director of Sales at TrustLayer, explained, "This isn't merely a technology issue. It's fundamentally human. Alert overload has created a culture of firefighting and fatigue. If we continue down this path, we'll see capable professionals leaving cybersecurity altogether, deepening the skills crisis."

Simplification is survival

Encouragingly, TrustLayer's report identifies a pivotal shift in the mid-market towards simplifying security architecture. Over half of SMB security leaders have started to consolidate their stacks, moving towards integrated platforms to reduce noise, eliminate overlaps, and strengthen overall resilience.

Mark Prater, CFO at TrustLayer, reinforced the economic urgency behind consolidation: "Cybersecurity spending must demonstrate clear value. SMBs don't have the luxury of redundant

Media:



Related Sectors:

Business & Finance :: Charities & non-profits :: Computing & Telecoms :: Education & Human Resources :: Government :: Public Sector & Legal ::

Related Keywords:

Cyber Resilience UK 2025 :: SMB Security Trends :: UK SMB Cybersecurity :: TrustLayer :: Cloud Blind Spots :: Email Attacks ::

Scan Me:



tools or expensive integration projects. They need a platform that delivers simplicity, clarity and protection from day one.”

A clear blueprint for cyber resilience in 2025

To combat the mounting challenges, TrustLayer’s report provides actionable guidance. It outlines five clear steps SMBs must prioritise immediately:

- Platform consolidation: Eliminate disconnected, overlapping tools to ensure seamless visibility and rapid response.
- Selective automation: Automate processes that create manual bottlenecks or drain limited resources.
- Cloud policy enforcement: Move beyond mere visibility to proactive, automated posture management across cloud environments.
- Human-centric operations: Protect security teams from burnout by designing workloads around people, not products.
- Strategic investment: Direct budgets toward initiatives with tangible operational impacts, rather than chasing fleeting security trends.

“The future of cyber resilience isn’t more tools, more alerts, or more complexity,” Macnair concluded. “It’s fewer tools that do more. It’s clarity, visibility and control. Above all, it’s recognising that cybersecurity is fundamentally about enabling your business to thrive—not just survive—in a threat-rich world.”

[Download the full report here.](#)

About TrustLayer

[TrustLayer One](#) is the layered cloud security platform that helps mid-market organisations protect everything that matters — from email and web to apps and users. Its unique DirectProtect™ architecture enables rapid deployment without mail flow changes or traffic rerouting.

Trusted by thousands of organisations and chosen by BT as a cybersecurity partner, TrustLayer delivers scalable protection that’s simple, powerful, and proudly British. This is cybersecurity, the direct way.

Company Contact:

[TrustLayer](#)

T. +44 (0)845 230 9590

E. marketing@trustlayer.co.uk

W. <https://trustlayer.co.uk/>

Additional Contact(s):

Lucinda Robinson, Marketing Director - lucinda@trustlayer.co.uk

[View Online](#)

Additional Assets:

<https://trustlayer.co.uk/resource/insight/2025-uk-cyber-resilience-report/>

Newsroom: Visit our Newsroom for all the latest stories:

<https://www.trustlayer-cybersecurity.pressat.co.uk>