View in browser

SEP2

Wingman Insights

Tech Driven. People Powered.

January 2026

5 minute read

Happy New Year and welcome to January’s Wingman Insights!

In this edition, I’ve been thinking about how much the security conversation has shifted over the past year. Predictions are everywhere, but what really matters is how we turn those ideas into action.

Our partners, Google, Check Point, and Wiz, have shared their outlook for 2026, and our technical team has taken those predictions and added their own expertise, bringing a practical lens to what these trends mean in the real world. From agentic AI and supply chain compromise to the growing challenge of trust and verification, these aren’t just headlines. They’re issues that will shape decisions in the months ahead.

Read their expert opinions

Which of these trends feels most relevant to you? And what’s missing from the conversation? I’d love to hear your perspective as we kick off the year.

Plus, as we start a new chapter, I’d really value your feedback on Wingman Insights so far. What’s working? What could be better? Share your thoughts.

Paul Starr
Co-Founder and CEO

Cyber Security Trends 2026: Expert Predictions

Google: Scaling Defense with Specialised AI

2025 proved that general-purpose AI has its limits. Large language models can only go so far, and adoption hasn’t reached the levels many expected.

Agentic AI

This year, expect a rise in smaller, specialised AI models built for specific tasks on both the defensive and attacker side. Think AI trained to read firewall logs or monitor IoT networks, outperforming generic LLMs every time. These models will be more mobile, run on restrictive hardware, and could even replace cryptominers as a new attack method.

And then there's trust. With AI-generated content becoming harder to spot, verifying who or what you're talking to will be critical. Personal certificates and signed communications might make a comeback.

How do we turn specialised AI into real defensive outcomes without adding noise? Here's where I'd start.

James Woodward
Head of Technology

Wiz: Resilience in a Cloud-First World

Wiz's predictions speak directly to the real-world challenges security leadership is facing.

Supply chain compromise
Abuse of third-party and supplier relationships will continue to be fertile ground for attackers. Expect further targeting of software and service providers because it works.

Cloud resilience under pressure
Beyond ransomware, threat actors will keep testing the boundaries of cloud immutability and recovery. We need to know our deployments can withstand disruption.

Keeping AI risk in perspective
AI deserves attention, but it shouldn't drown out other risks. Many "new" AI threats mirror long-standing issues - prompt injection is another flavour of input sanitisation. The bigger risks sit wider: breakdown of trust in digital content (yes, maybe blockchain still has a role), and societal disruption from AI-driven unemployment. These demand business and government leadership, not just security controls.

Want to see how these risks stack up against other 2026 trends? Explore the full blog for practical insights.

Jon Cumiskey
Head of Information Security

Check Point: The New Era of AI Governance and Compliance

2025 was about experimenting with AI. In 2026, it’s about governing it. As AI moves from pilots to full integration, standards like ISO 42001 and NIST AI RMF will become the new cost of doing business - driven by customer demand as much as regulation.

Continuous compliance
Point-in-time certifications are over. Compliance will become a continuous process, woven into the fabric of organisations. Security will also move out of the IT silo and onto the Board agenda as supply chain compromises push information security into strategic risk management.

And we can’t forget the basics. Revisiting the “Golden Triangle” of People, Process, and Technology is key - measurable awareness programs, smarter business processes, and critical defenses like MFA and advanced email security will remain essential.

Governance isn’t optional anymore. Find out what leaders are doing differently.

Johan van Rooyen
Principal Security Consultant

"It’s just me and god forbid if I take a holiday, there’s nobody else to cover. So knowing that there’s a dedicated team in there that can ease the workload on me, and allow me to focus on what I need to do to support Personal Group was a no-brainer."

- Jack Marshall, Information Security Analyst at Personal Group

Read our latest case study

News

2025 Cyber Security Service Delivery Review

2025 taught us a lot about what works - and what needs to change - in cyber security service delivery. We're sharing the lessons that shaped our next big moves: the SEP2 app and our agentic SOC, designed to make security smarter, faster, and more connected than ever.

See what we learned and where we're heading

Complimentary Rapid Wiz Stand-Up for Check Point CNAPP Customers

Are you a current Check Point CNAPP customer? We're offering a complimentary rapid stand-up to get you operational on the Wiz platform quickly. Our experts will get you set up, allowing you to bypass the initial complexity and start benefiting from Wiz's powerful security insights.

Claim your free rapid stand-up

Webinar Recordings

Explore our webinars for expert-led, actionable insights, including:

Securing the Cloud with Confidence: SEP2 + Wiz in Action
Navigating DORA and NIS2 Compliance with Drata
When Should a Growing Business Invest in a Security Operations Centre (SOC)?

View all webinars

Follow SEP2 On LinkedIn

Stay in the loop on cyber security events, SEP2 news, and people-powered insights

Connect with us

Thank you for reading this edition of Wingman Insights!

Leave a review so I can continue to improve it.

51a St Paul's Street
Leeds
LS1 2TE

0330 043 7372
info@sep2.security

SEP2

Website LinkedIn