Why building secure AI from the start matters

verizon business

Artificial intelligence (AI) project designers may increase cyber risks if they launch initiatives without embedding robust security and data governance from day one. Research from The Rand Institute's National Security Research Division suggests generative AI (genAI) projects may face higher failure rates than traditional IT projects—up to four out of five—often due to unaddressed vulnerabilities, fast adoption rates, as well as rapid development release cycles of AI features and applications.

So, how can companies secure AI from the start to help ensure success?

Verizon believes the answer lies in a proactive, security-first approach. By integrating advanced cybersecurity and network solutions from the outset, businesses can mitigate risks and unlock genAI's potential responsibly.

The growth of genAI

GenAI is transforming industries across APAC, with IDC estimating the region's AI market could reach $26 billion by 2027. In Australia, nearly 70% of businesses already use AI, and over 85% plan to boost genAI investments this year, per industry insights. This rapid adoption drives innovation, but without proper security, it can expose organisations to cyber threats.

The National Institute of Standards and Technology (NIST) notes that securing AI algorithms remains a complex challenge, with some issues still unresolved. An Economist Impact report highlights that 47% of Australian firms see gaps in their current data and AI governance frameworks—gaps that Verizon's expertise can help close.

Taking a secure step forward

The 2025 Verizon Data Breach Investigations Report found that 54% of ransomware victims had their domains appear in credential dumps, emphasising the critical need to secure credentials in AI systems from the beginning. Verizon's solutions, like automated vulnerability management, can help mitigate these risks swiftly.

Verizon's approach starts with fixing known vulnerabilities fast.

At a recent event in Seoul, Alistair Neal, Verizon's global Head of Information Security, discussed how AI security automation strengthens vulnerability management and governance amid rising threats—particularly with the evolution of new attack strategies like the "RansomHub" platform, which provides ransomware as a service.

Neal argued that AI security automation and changes in the security environment provide great opportunities for companies to expand data sharing and collaboration. However, a systematic approach to data protection and security control is essential. Verizon's proactive monitoring and response capabilities can help businesses stay ahead of such dangers—helping to secure genAI infrastructure before projects scale.

Network transformation is equally vital. As genAI demands grow, organisations need robust, scalable networks. Even with next-generation platforms, expanding attack surfaces challenge security leaders. Verizon's Private 5G Network supports this shift, delivering high-capacity connectivity to handle AI workloads. Verizon's Secure Gateway encrypts data flows, ensuring genAI systems remain protected as they move from pilot to production.

Consider a practical example from NIST's Adversarial Machine Learning report (NIST.AI.100-2): an autonomous vehicle's genAI model misreads a defaced stop sign as a speed limit due to poor training safeguards protecting its classification, which opened up a vulnerability to attackers. Verizon's cybersecurity solutions can help developers test and secure sensitive training data such as these.

Building a comprehensive approach with Verizon

Securing genAI requires a holistic network framework—risk management, data governance and cybersecurity working together from the start. Verizon helps empower APAC businesses with tailored tools and expertise to make this practical.

Cross-functional AI steering teams, supported by Verizon, can help align IT, security and operations to assess risks and refine strategies. Verizon Threat Research Advisory Center (VTRAC) provides real-time threat intelligence, enabling rapid detection of anomalies—like unusual network activity—that could signal an attack. Services like penetration testing, part of Verizon's cybersecurity solutions, expose gaps before they're exploited, helping genAI projects to launch securely.

In healthcare, where AI tools assist diagnostics, accuracy is critical. A Rhode Island pilot study showed false positives rose to 86% when doctors relied on flawed AI outputs. Verizon's Network Security Services safeguard data integrity, helping developers build reliable AI systems from the ground up.

The Australian Department of Industry, Science and Resources warns that system design flaws or data issues can compromise AI outputs. Verizon's cybersecurity assessments help quantify these risks, offering actionable insights to help strengthen genAI deployments without overcomplicating the process.

Verizon's edge in securing AI

Verizon doesn't just identify risks—it helps solve them. With Verizon Private 5G and Secure Gateway Services, businesses gain a secure foundation for AI workloads. The Verizon Threat Research Advisory Center delivers 24/7 monitoring, to help organisations catch threats your business teams might miss. Penetration testing and risk assessments round out a layered defence, tailored to APAC's unique challenges.

This article isn't about stoking fear of genAI—it's about readiness. Verizon's solutions can help genAI projects thrive by embedding security from day one, balancing innovation with protection.

Learn more

Explore how Verizon helps to secure enterprise AI across APAC. Contact your Verizon Business Account Representative. Email us apaccontactus@verizon.com or visit verizon.com/business/en-au/contact-us/