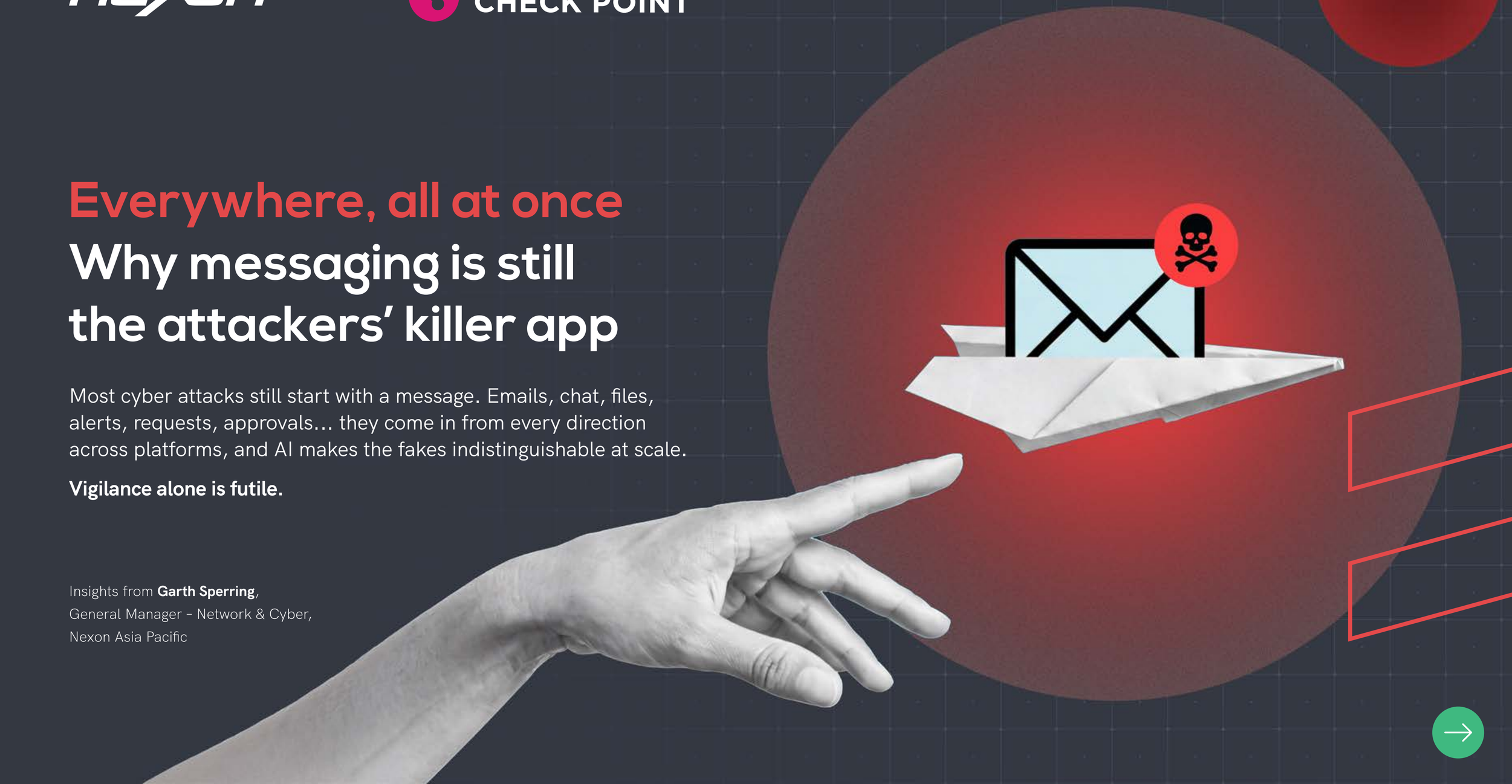
Everywhere, all at once

Why messaging is still the attackers' killer app

Most cyber attacks still start with a message. Emails, chat, files, alerts, requests, approvals... they come in from every direction across platforms, and AI makes the fakes indistinguishable at scale.

Vigilance alone is futile.



Insights from **Garth Sperring**,
General Manager - Network & Cyber,
Nexon Asia Pacific

Messages are still the way in

Cyber security headlines focus on spectacular multimillion-dollar ransom payments, global password breaches, AI-powered nation-state attacks and deepfake scams. But the way attackers actually get into Australian businesses hasn't changed much in twenty years.

Bad actors send a lot of messages. Eventually, someone opens one, clicks, replies or shares a credential. The door gets opened from the inside with no clever tricks.

Nexon's penetration testing across 126 Australian organisations found that phishing and social engineering were the most reliable ways to gain access.[1] These findings are consistent with Check Point Research's AI Security Report 2025[2] and the 2025 Gartner Magic Quadrant for Email Security,[3] which both underline how central email and messaging remain to most attacks.

> We can talk about and prepare for all the sophisticated cyber threats out there, but when we run the simulations, phishing is still where they get in. The attack surface is getting wider, **but email – and increasingly messaging – is still the weakest spot for most attackers.**

[1] Nexon Asia Pacific, 2025 Cyber Security Report
[2] Check Point Research, AI Security Report 2025
[3] Check Point, Leader in the 2025 Gartner Magic Quadrant for Email Security, 2025

Expert contributor

Garth Sperring

General Manager – Network & Cyber, Nexon Asia Pacific

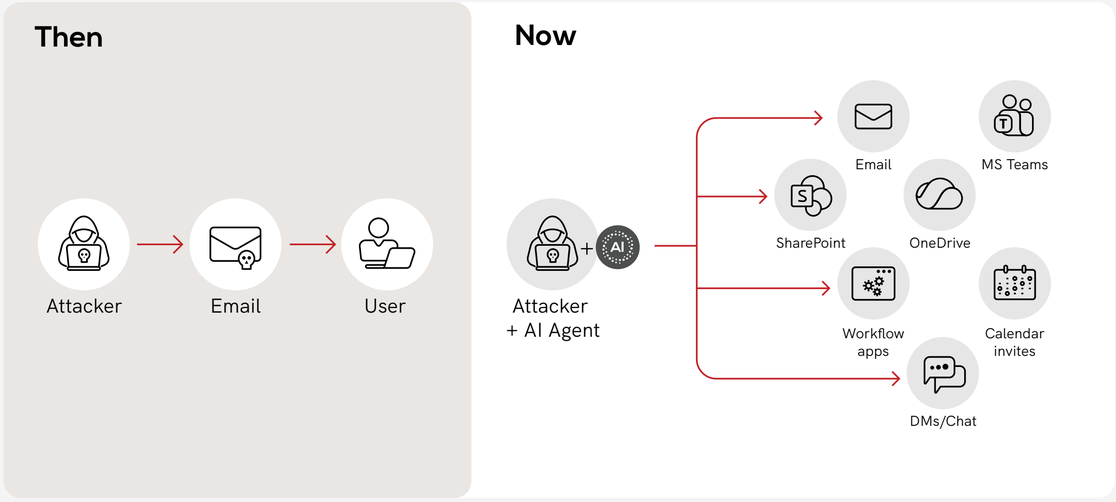
Garth leads Nexon's networking and cyber security practice, overseeing network architecture, SD-WAN, security and managed services. He helps organisations build reliable, secure network foundations for cloud, AI and hybrid infrastructure.

In this guide, Garth shares insights from his experience helping Australian organisations protect their workspaces.

Email is just one of the inboxes

A typical knowledge worker now picks up messages across half a dozen channels in a working day: Outlook for clients, Teams chats for sales, SharePoint project notifications, OneDrive shares for deep work and a stream of DMs across apps and third-party platforms.

While cold emails bring well-known phishing risks, other channels bring their own habits and assumptions about trust. Alerts, reminders and messages from closed platforms, especially from people you know, carry a level of confidence and safety that lowers our guard.



Many organisations that standardise on Microsoft 365 assume this consolidates their messaging into a single, tidy security perimeter. While it does simplify the stack, the collaborative nature of tools like Teams, SharePoint and OneDrive means each became a new pathway in.

Connected tools like workflow systems, project management apps and shared calendars open more conversations. Even Microsoft-powered organisations will have teams or partners using tools like Slack, ClickUp or Monday, or financial systems that route notifications via email.

The AI Security Report[2] outlines how attackers have moved beyond one-off phishing emails and now use AI agents to follow up across multiple channels simultaneously. They'll email a convincing fake invoice, follow up with a personalised Teams message and a chat in a shared workspace, maintaining a credible conversation across all three until someone responds.

> The threat is now embedded across email, collaboration tools, shared files and chat. **If your protection stops at the inbox, you've left the biggest part of the workspace uncovered.**

[2] Check Point Research, AI Security Report 2025

Fakes too good to be untrue

For twenty years, you could pick a dodgy email. The clunky English, fuzzy logo, odd sender address, urgent deadline or Nigerian prince gave it away to anyone who'd been around the block.

Recent research[2] shows how large language models have made it effortless for attackers to craft messages with native fluency in any language or cultural register, and also weave in personal details and real references.

One example named in the report is the Business Invoice Swapper, sold on dark web forums. It scans compromised email accounts for invoices and payment instructions and swaps the bank details. The recipient sees a branded invoice from a real supplier, with language that matches previous correspondence.

The fraud sits inside a real, ongoing business relationship, giving busy people very little chance of spotting it.

> **If you're relying on staff to spot the difference, you're asking them to do the impossible.** What we're seeing now is phishing that genuinely passes the sniff test. The sender looks right, the language sounds right, the timing fits the conversation.

It's not your people's fault

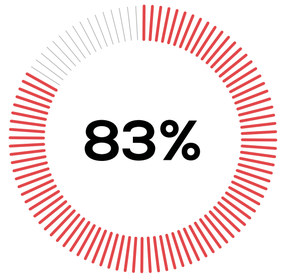
Security awareness training can no longer rely on being able to spot risks. It can teach people to be careful and sceptical, but it's pointless if there are no red flags.

In Nexon's penetration testing, every organisation had at least one vulnerability that could have been prevented with stronger basic foundations, with 83% of phishing attempts in red team exercises gaining credentials.[1]

When real work requests are indistinguishable from scams, people will click, approve and process them, because that's what they are employed to do.

In many cases, attackers aren't hacking in anymore. They're logging in with credentials that someone has been tricked into providing. The traditional security perimeter is gone – identity is the new perimeter, and that's what's under attack.

The key to securing the workspace is to stop unsafe messages before they reach a person.



of phishing attempts in red team exercises gained credentials

> **They're not hacking in, they're logging in.** We're past the point where any amount of training will close the gap. The protection has to be in place before the message ever gets to the user. If it gets to them and it looks real, they'll take action. It's their job.

[1] Nexon Asia Pacific, 2025 Cyber Security Report
[2] Check Point Research, AI Security Report 2025

Protecting the multi-channel workspace

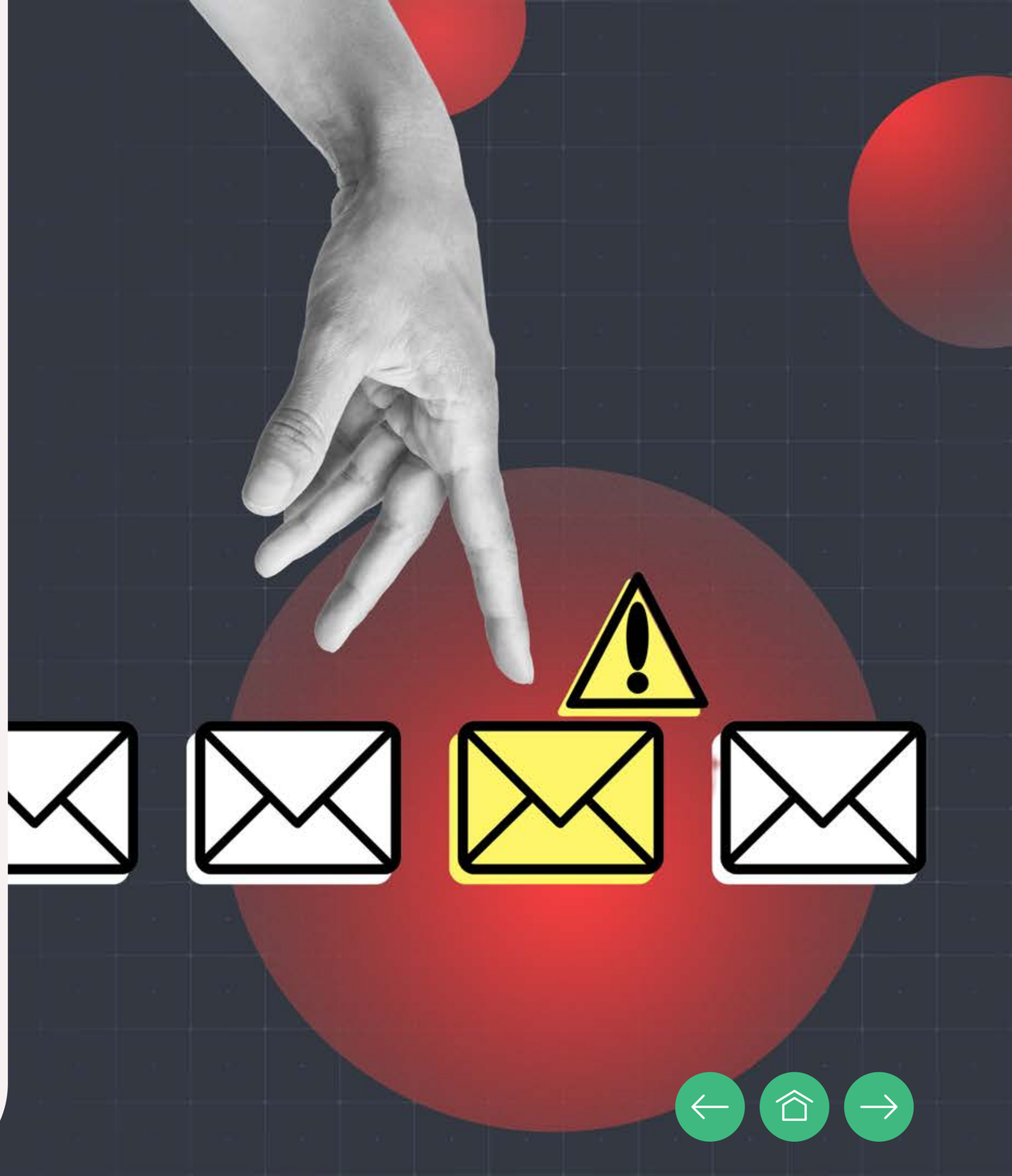
Cyber security has to protect where the work is being done, which is increasingly everywhere all at once and outside the inbox.

For mid-market organisations running Microsoft 365, the built-in security across the platform means the foundations are already in place. The new capabilities added in recent years have brought enterprise-grade security to all subscription levels.

With millions of customers across industries and countries, Microsoft provides broad protection at scale. This is where a specialist email and collaboration security vendor like Check Point is ideal as a layer on top of Microsoft. It's built to catch the long tail of attacks such as targeted phishing, business email compromise, malicious messages and AI-crafted impersonations.

An integration and managed service partner brings these layers together, configuring them for your environment, integrating them with existing systems and keeping the protection tuned as the threats shift.

> Microsoft gives you the foundation, Check Point adds the specialist layer and we make sure it's all set up properly and looked after. **None of those three on their own is enough.**



Always working in the background

For a mid-market organisation already running Microsoft 365, adding specialised email, collaboration and workspace protection makes sense. It doesn't need to be a long or costly project.

99.2% ↓

reduction in phishing reaching the inbox

Check Point's email and collaboration protection connects to Microsoft 365 via API without new software, MX record changes or disruption to user workflow.

It works in the background alongside your existing setup, scanning email and collaboration traffic before it reaches the inbox or the channel. The only change users will notice is that the threats just stop arriving.

Check Point reports a 99.2% reduction in phishing reaching the inbox.[4]

Detection is AI-driven and trained on real-world attacks such as AI-crafted phishing, business email compromise, impersonation and malicious links. More than 50 AI engines keep the protection up to date.[4]

Nexon handles acquiring the Check Point subscription, integrating it with the customer's Microsoft tenant and managing protection day-to-day. For the customer, there's no new platform to learn and no new vendor to manage.

> It's quick to put in, works straight away and can run regardless of what Microsoft licence you're on. You don't need a full security audit before you start, **so it's a painless process.**

Silence is golden

Effective workspace protection means IT teams get fewer "is this real?" tickets to triage, fewer breaches to deal with and hours back in the week. Your team gets fewer suspicious messages to decode and a workspace they can trust.

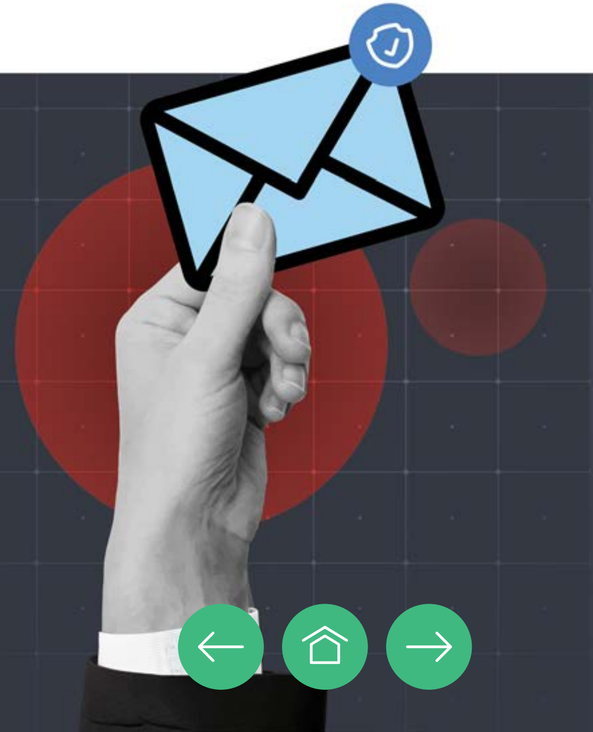
Vaco, a global professional services firm with more than 10,000 employees, reported a 20% reduction in support tickets after deploying Check Point's email and collaboration protection.[5]

20% ↓

reduction in support tickets at Vaco

Closer than you think

If you're already running Microsoft 365, the foundation is in place. Integrating Check Point's specialist email and collaboration protection is a small project with a big return.



[4] Check Point, Email Security solution overview, accessed 2026 (outcomes vary by environment)

[5] Check Point, How Vaco Slashed Support Calls by 20% (While Boosting Email Security), 2024

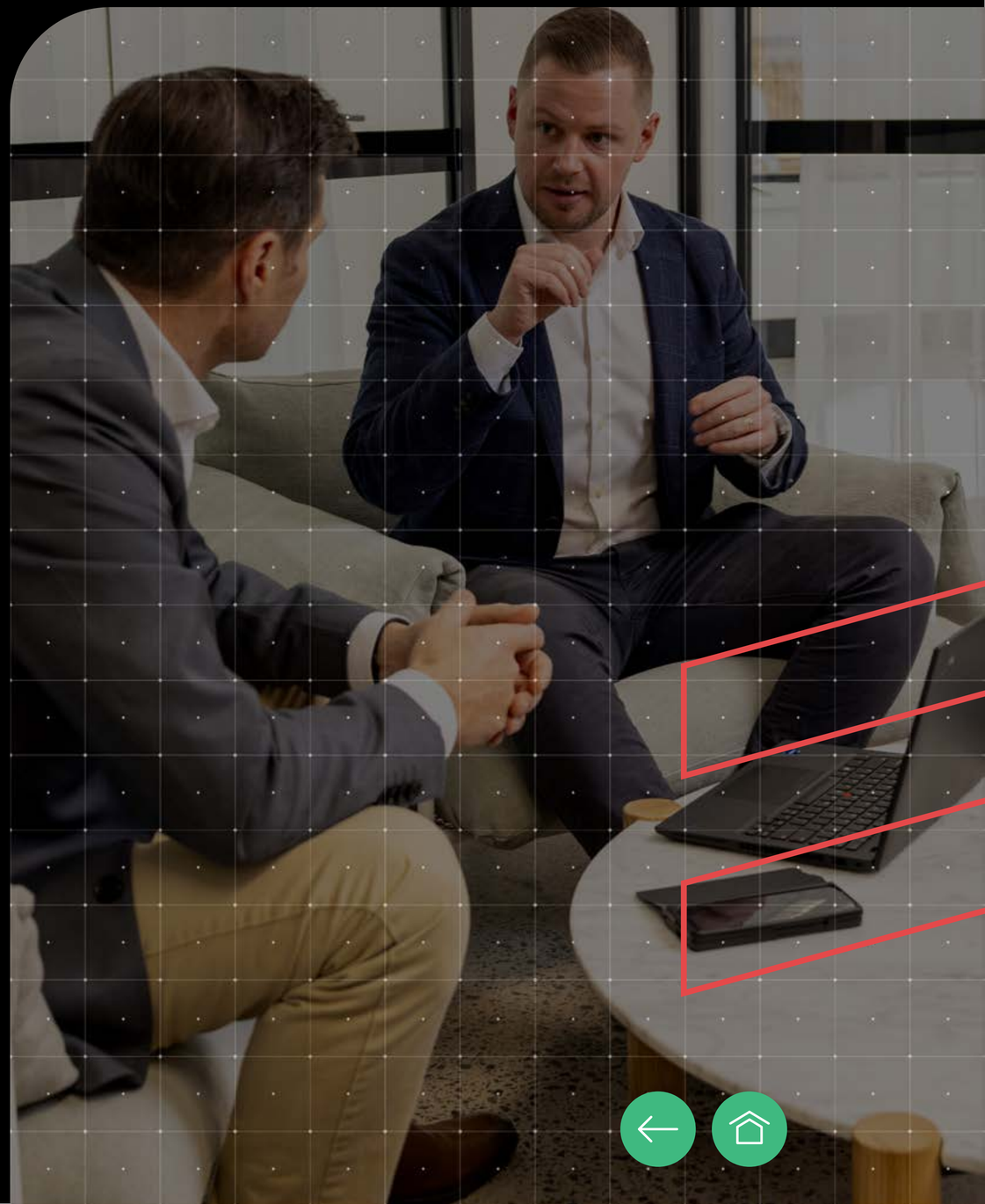
Ready to protect your workspace?

Talk to us about assessing your current Microsoft 365 environment, identifying gaps and mapping a path to comprehensive workspace protection.

1300 800 000

nexon.com.au/cyber

Follow **nexonap**



About Nexon Asia Pacific

Nexon is an award-winning digital and IT services partner for mid-market, enterprise and government organisations across Australia. We offer clients a uniquely broad suite of solutions requiring end-to-end capabilities coupled with specialist expertise in security, cloud and digital solutions. As a certified and accredited local and state government provider, CREST and ISO-certified, Nexon partners with world-class technology vendors to deliver innovative and integrated solutions.

About Check Point

Check Point Software Technologies Ltd. (checkpoint.com) is a leading protector of digital trust, utilising AI-powered cyber security solutions to safeguard over 100,000 organisations globally. Through its Infinity Platform and an open garden ecosystem, Check Point's prevention-first approach delivers industry-leading security efficacy while reducing risk.

Visit: checkpoint.com

References

1 Nexon Asia Pacific, 2025 Cyber Security Report
2 Check Point Research, AI Security Report 2025
3 Check Point, Leader in the 2025 Gartner Magic Quadrant for Email Security, 2025
4 Check Point, Email Security solution overview, accessed 2026 (outcomes vary by environment)
5 Check Point, How Vaco Slashed Support Calls by 20% (While Boosting Email Security), 2024