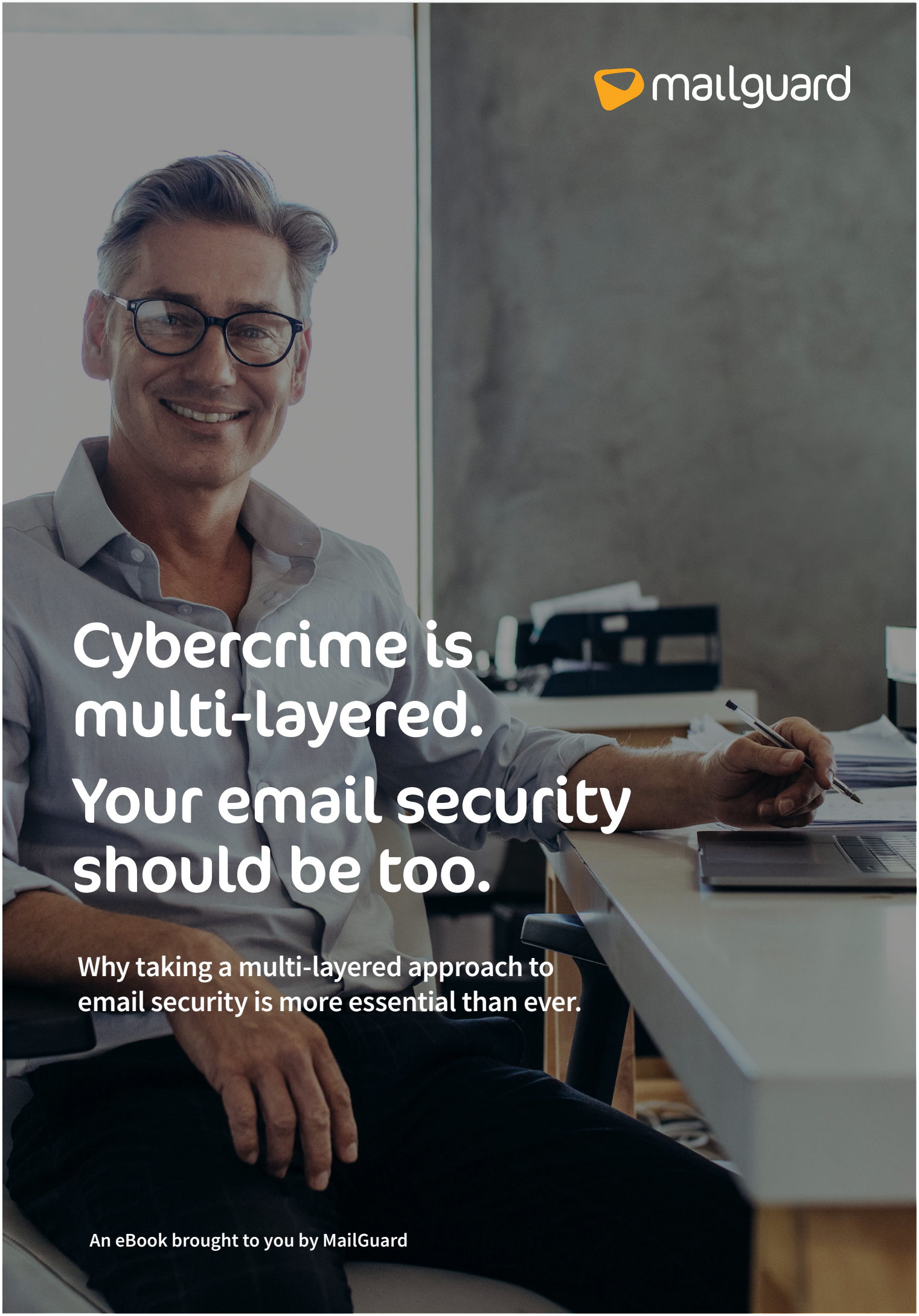

mailguard
Cybercrime is multi-layered.
Your email security should be too.
Why taking a multi-layered approach to email security is more essential than ever.
An eBook brought to you by MailGuard

When it comes to your business' security, email can be a key vector for cybercriminal attacks. Sophisticated phishing, spear phishing and business email compromise [BEC] scams all appear legitimate to the casual user and often still get through basic filters. These attacks are becoming increasingly sophisticated and complex - whether your employees are using their business or personal email, they can unwittingly put your business at risk.

Even though a solution like Microsoft 365 is equipped with Microsoft's enterprise-level cloud security, it's impossible to provide 100% protection against an ever-evolving threat landscape, particularly one that exploits human vulnerabilities. No single solution can.

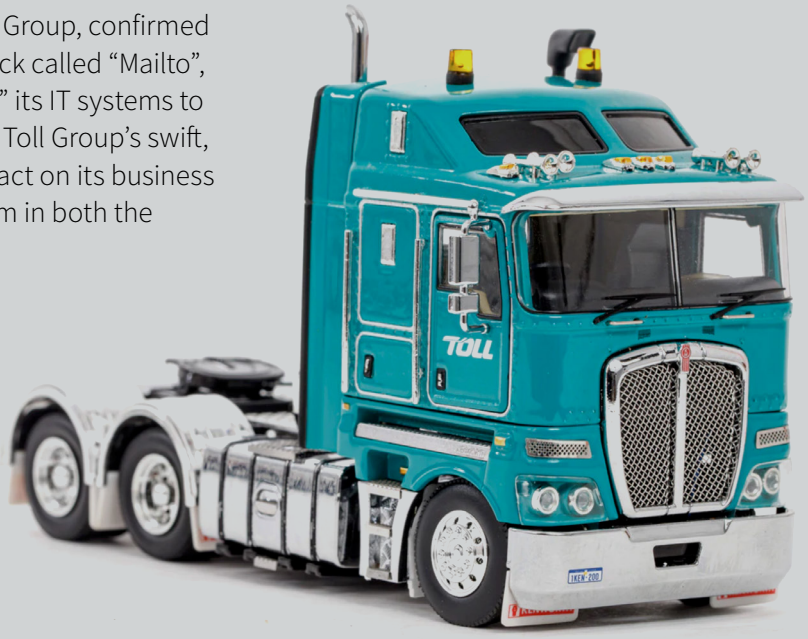
In this eBook, we explain the importance of taking a multi-layered approach to email security to ensure your business is completely protected.

90% of cyber-attacks start from email. [1]

One cyber-attack is reported every 10 minutes. [2]

Toll Group suffers a “Mailto” ransomware attack

Recently, the large-scale logistics business, Toll Group, confirmed it was the victim of a targeted ransomware attack called “Mailto”, which led it to “immediately isolate and disable” its IT systems to stop the ransomware from spreading.[3] Despite Toll Group’s swift, responsible and transparent reactions, the impact on its business has been significant, and it has received criticism in both the mainstream press and on social media.



Toll Group is a sophisticated, connected, global organisation that is likely to have invested heavily in its security, with a team of dedicated Infosec professionals and partners in place to mitigate threats. If a targeted ransomware attack like this can disrupt a large organisation like Toll Group, it can happen to anyone.

Why a single security solution is no longer sufficient

When it comes to business security, the phrase ‘you are only as strong as your weakest link,’ is truer now than ever before.

As Microsoft’s CEO, Satya Nadella, said, “…the issue with security is, you can’t just secure one room in the house. You have to have end-to-end security. Starting with identity, to devices, to applications to information and data, as well as your infrastructure. It needs to be one chain.”[4]

There are many reasons why a single security solution is no longer enough to protect you in this new era of cybersecurity threats. Here are the most significant for today’s connected organisations.

Cloud-based services are a target

A majority of businesses are now moving their business data and email systems to the cloud, especially as workforces become more remote amid the COVID-19 pandemic. According to the Oracle and KPMG Cloud Threat Report 2019, the number of organisations with more than half of their data in the cloud will increase by a factor of 3.5 between 2018 and 2020. Plus, 70% of businesses now say the majority of their cloud-based data is sensitive in nature.[5]

Moving to the cloud offers a huge range of benefits for modern businesses when it comes to productivity, cost savings and employee engagement. However, the rapid move to cloud services makes many businesses a far softer target for cybercriminals. According to Oracle and KPMG, this is due to several factors, including internal confusion around new security models, a lack of visibility into cloud security, and poor password management.[6]

Welcome to a whole new world of attacks

The nature of email-based cybersecurity threats is changing constantly, making it increasingly difficult for businesses and individuals to keep up.

Sophisticated hackers are now using social engineering techniques, which means emails can be heavily personalised and may not contain overtly malicious content, allowing them to slip through traditional filters.

While traditional email filters work well to catch malicious emails, sophisticated phishing, spear phishing and BEC scams often appear legitimate, and can still get through.

> "Cloud adoption has expanded the core-to-edge threat model. An increasingly mobile workforce accessing both on-premises and cloud-delivered applications and data dramatically complicates how cybersecurity professionals must think about their risk and exposure."
>
> **Oracle and KPMG Cloud Threat Report 2019**[7]

Many breaches are still going undetected

Given the complexity of modern cybercrime, detection remains a problem.

According to a recent Telstra report, 19% of Australian respondents estimated that more than half of the data breaches impacting their company went undetected altogether in the past year.

This is despite 74% of Australian businesses believing they have strong systems in place to verify when an incident has occurred.[8]

Cybercrime is profitable - expect it to grow in ferocity

The volume and complexity of email-borne cyber-attacks is increasing year on year – to the extent that 61% of IT leaders now think a negative impact is inevitable.[9]

The Australian Competition and Consumer Commission's (ACCC) Targeting Scams 2019 report identified Australians lost over $634 million to scams in 2019. While the true cost of cybercrime to the Australian economy is difficult to quantify, it is estimated to reach a staggering $29 billion annually.

The steps that you put in place to defend your business today may not be enough for tomorrow. As such, it's important to continually challenge your readiness, and adapt to new innovations – just as cybercriminals are.

Your employees may be your biggest source of risk

More employees are now working remotely and on an array of devices – which means providing consistent email security is becoming increasingly difficult. Employees remain a key security risk, as their behaviour can't always be predicted, or controlled.

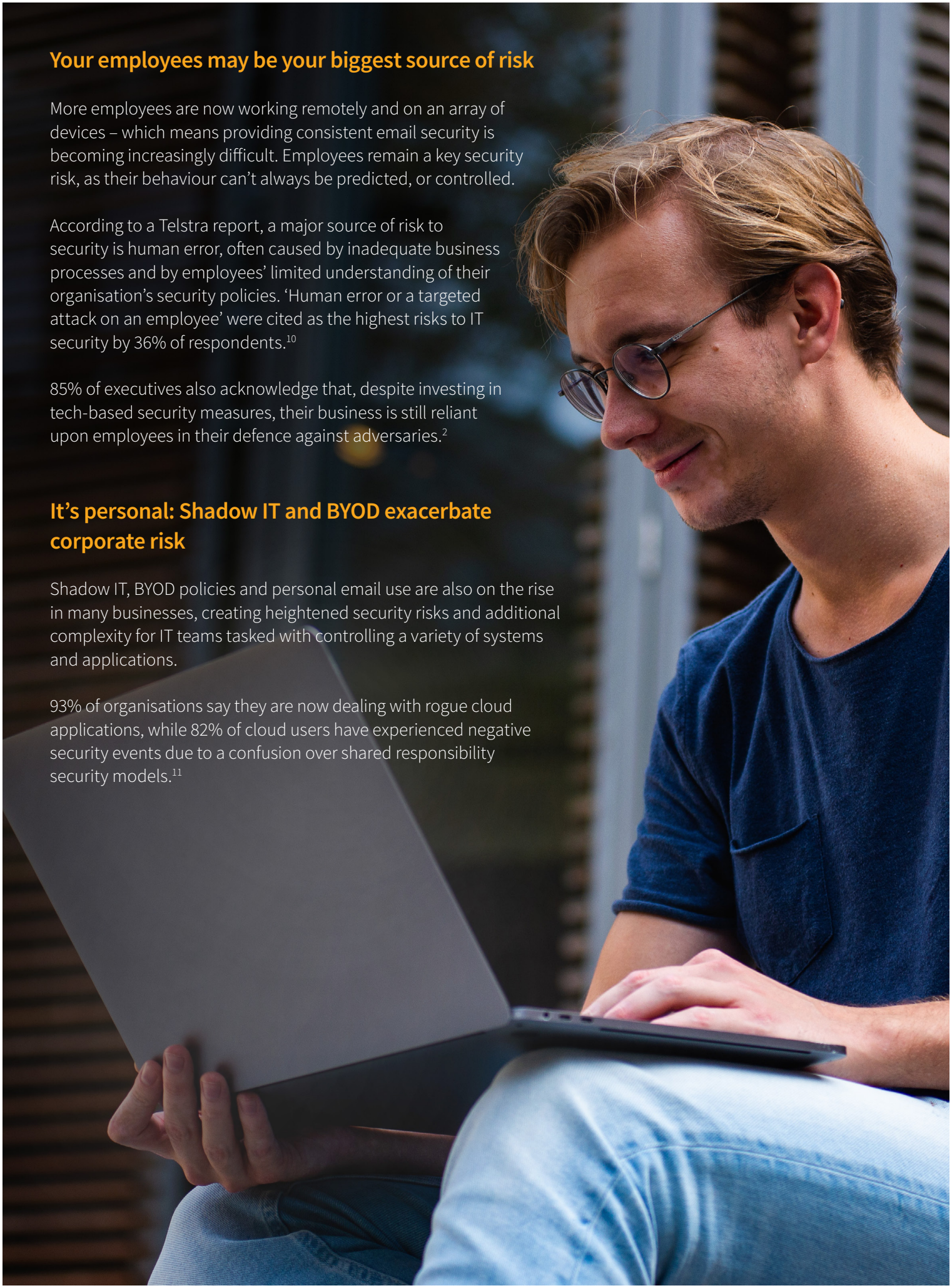
According to a Telstra report, a major source of risk to security is human error, often caused by inadequate business processes and by employees' limited understanding of their organisation's security policies. 'Human error or a targeted attack on an employee' were cited as the highest risks to IT security by 36% of respondents.[10]

85% of executives also acknowledge that, despite investing in tech-based security measures, their business is still reliant upon employees in their defence against adversaries.[2]

It's personal: Shadow IT and BYOD exacerbate corporate risk

Shadow IT, BYOD policies and personal email use are also on the rise in many businesses, creating heightened security risks and additional complexity for IT teams tasked with controlling a variety of systems and applications.

93% of organisations say they are now dealing with rogue cloud applications, while 82% of cloud users have experienced negative security events due to a confusion over shared responsibility security models.[11]



How a multi-layered approach can help

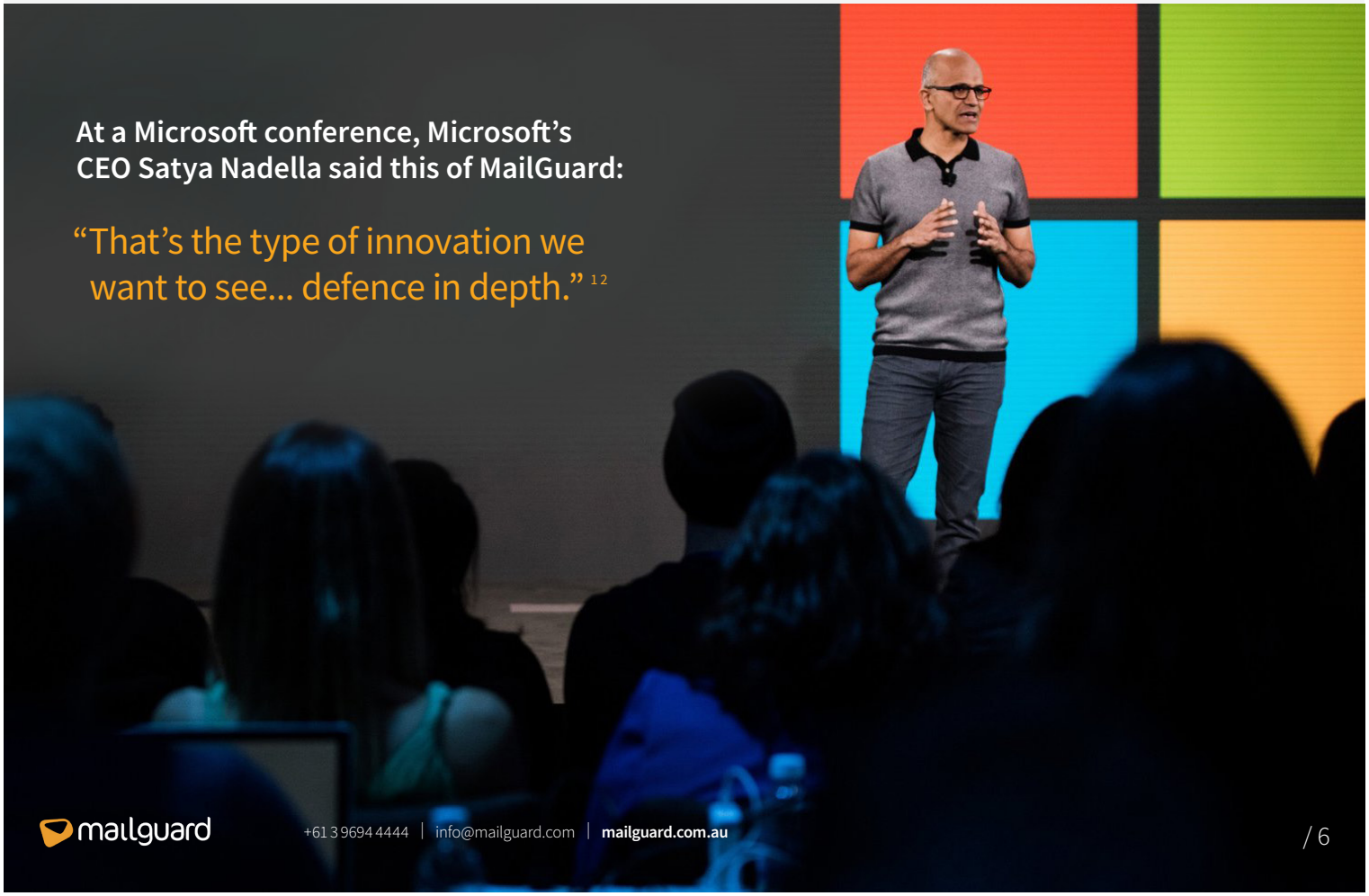
Just one malicious email is all it takes to destroy a business, and Microsoft 365 users are prime targets. While Microsoft 365 is equipped with Microsoft's enterprise-grade security, it's impossible to provide 100% protection against all email attacks, especially ones that exploit human fallibility. No single solution can.

Cybercriminals iterate on their attacks to avoid detection by traditional email security including Microsoft 365. Known exploits are likely to be intercepted, so cybercriminals continually test small changes in their approach to unlock weaknesses in vendor algorithms – sending each variation to mailboxes protected by traditional vendors to see what gets through. In one such example intercepted by MailGuard, cybercriminals attempted more than 160 iterations of the same attack within a 3-hour window.

That's why, to stay protected it's important to take a multi-layered approach. This ensures that your inboxes are protected against as many variants of an email threat as possible. One of the most effective ways to quickly and easily boost your email security is by pairing Microsoft 365 with MailGuard.

MailGuard makes life safer and easier for email users, providing defence-in-depth protection for your business.

Getting started with MailGuard is quick and easy. Your organisation can update its email security today with a free 14-day evaluation.



Why choose MailGuard for your business?

MailGuard is a cloud-based email security provider offering a simple customer experience with a targeted focus on stopping malicious threats before they ever reach your users.

With 19+ years of specialised email security expertise and IP from MailGuard, no software to install, immediate security updates and a team of real people available to help you on the phone 24/7, your business will always have the most current protection and support against emerging threats.

Does your business rely on Microsoft 365? As a Gold Microsoft partner, **MailGuard works effortlessly alongside Microsoft 365** - acting as an additional layer of security to give your business defence in depth.

Our Hybrid AI threat detection engines are always learning and adapting to threats as they begin circulating - so while other businesses are learning the hard way that their security is inadequate, you can rest assured knowing your business is protected.

Jasco Consulting boosts their clients' data security with MailGuard and Microsoft 365

Jasco Consulting is a trusted Microsoft partner that provides information security solutions to manage clients' risks. So it was concerning when clients using Microsoft 365 reported email threats slipping past their existing security filters.

MailGuard was a perfect solution. Jasco Consulting have enjoyed far greater protection, confidence and peace of mind, knowing that their clients' sensitive data and communications are protected by MailGuard.

"We have been selling MailGuard for several years as the best-of-breed email security solution. Choosing the MailGuard solution to recommend to our clients was a no-brainer.

The MailGuard solution is just so simple to deploy and it instantly protects our clients from email threats."

– Service Desk Team Leader, Jasco Consulting

Ready to make the move against email threats?

Take a multi-layered approach to email security right across your business with MailGuard.

To learn more, get in touch here

1. Microsoft, MailGuard, New approach to Microsoft 365 email security keeps patient data secure, Capitol Health case study **2.** ACSC Annual Cyber Threat Report FY19-20: https://www.cyber.gov.au/sites/default/files/2020-09/ACSC-Annual-Cyber-Threat-Report-2019-20.pdf **3.** IT News, February 2020, Toll Group confirms targeted ransomware attack, [online]: https://www.itnews.com.au/news/toll-group-confirms-targeted-ransomware-attack-537494 **4.** MailGuard, 5 key messages on cybersecurity from Microsoft CEO Satya Nadella **5 - 7.** Oracle and KPMG, Cloud Threat Report 2019, online: https://www.oracle.com/au/a/ocom/docs/cloud/cloud-threat-report-2019-executive-summary.pdf **8.** IT Brief, Why cybersecurity remains a top business priority, [online]: https://itbrief.com.au/story/why-cybersecurity-remains-a-top-business-priority **9.** CPO Magazine, How cybersecurity leaders can best navigate the C-suite, [online]: https://www.cpomagazine.com/cyber-security/how-cybersecurity-leaders-can-best-navigate-the-c-suite/ **10.** IT Brief, Why cybersecurity remains a top business priority, [online]: https://itbrief.com.au/story/why-cybersecurity-remains-a-top-business-priority **11.** Oracle and KPMG, Cloud Threat Report 2019, online: https://www.oracle.com/au/a/ocom/docs/cloud/cloud-threat-report-2019-executive-summary.pdf **12.** MailGuard, 5 key messages on cybersecurity from Microsoft CEO Satya Nadella