The reality is a cyberattack is reported every 8 minutes in Australia, and in 2021 our Kaspersky products detected 380,000 new malicious files every single day. All organisations – including NFPs – are at risk.

Not-for-profit organisations are prime targets for cyberattacks thanks to the large amount of personal and financial information you hold on your clients, supporters and employees. This is attractive bait for cybercriminals, but poses a serious risk for your organisation's reputation.

According to our research, in over 75% of data breach incidences last year the victims were neither able to identify the attackers nor find out how they were compromised. This can motivate cybercriminals to delve into the field of data theft and illegal trading, and we actually predict there will be more databases, internal communications and personal details stolen from Australian organisations and traded on the black market this year.

There is therefore greater need to protect every laptop, every mobile device and every server within your organisation to safeguard your sensitive data. But crucially you don't want this endpoint protection to affect performance, or productivity.

How can Kaspersky help?

Our Kaspersky Endpoint Security for Business reduces your exposure to cyberattacks by protecting you against threats, detecting and patching vulnerabilities, and encrypting data whilst helping boost productivity – all without impacting on performance.

For those looking for extra value, Kaspersky Endpoint Security Cloud enables remote encryption that keeps your data safe even if a device gets lost or stolen. It allows employees to work securely on any device whether that is at home, the office or in the field, while you can manage your security from anywhere, and at any time, via our cloud-based console.

This can be a good solution for those with tighter budgets, as it can scale up or down to suit your requirements, and with a monthly billing model you always know exactly how much the service costs.

For those looking to step it up a level, Kaspersky Endpoint Detection and Response Optimum is built for smaller cybersecurity teams with limited resources who want to upgrade their incident response capabilities. It gives you deep visibility into threats, so you'll be able to see the threat, understand how it occurred it, reveal its full scope and avoid further damage with a rapid automated response.

Why Kaspersky?

At Kaspersky, our mission is simple – building a safer world. Our technologies protect over 400 million users worldwide and we help 240,000 corporate clients protect what matters most to them.

We detect and neutralise threats regardless of their origin or purpose to protect our users, and any data sent to Kaspersky is robustly protected and is not attributed to a specific individual.

We are actively involved with governments and law enforcement agencies in the fight against cybercrime, and we are fully committed to the trustworthy development of our technologies and solutions. Through our Global Transparency Initiative we engage the security community, our customers and other stakeholders in validating and verifying the trustworthiness of our products, internal processes and business operations.