WHY DO BUSINESSES NEED DEFENCE IN DEPTH CYBERSECURITY?

The threat landscape is constantly evolving, at a pace that most organisations are struggling to keep up with. Cyber attackers are utilising ever-more sophisticated tactics and targeted attacks to bypass security controls.

ONE CONCEPT THAT WE OFTEN HEAR IN THE INDUSTRY TO TACKLE THESE CHALLENGES IS

DEFENCE IN DEPTH

BUT WHY IS IT IMPORTANT FOR ORGANISATIONS?

2/3

Australian businesses suffered a ransomware attack in 2020

30%

Chance your business will experience a data breach in the next 2 years

60%

Of malware is now cloud delivered

+612 9221 5555 info@infotrust.com.au www.InfoTrust.com.au

InfoTrust

PHISHING, CLOUD-BASED MALWARE, ZERO DAY EXPLOITS

These are just some of the strategies that cybercriminals use today to conduct their nefarious activities. One or even two layers of security controls these days just won't cut it.

THE BENEFITS OF DEFENCE IN DEPTH

MULTIPLE LAYERS OF SECURITY

Deter a potential attacker but also improve the ability to detect and respond to attacks too.

REMOVES SINGLE FAILURE POINT

Remove the opportunity for a single point of failure occurring in your systems.

ANALYSIS AND REMEDIATION

Forensic analysis capability to understand indicators of compromises, and how they can be stopped.

InfoTrust
Protection from Cybercrime

Whilst defence in depth is the advisable approach for businesses to take, it can be difficult for security and IT teams to manage on their own. This is where a trusted cybersecurity partner can help to create and manage a defence in depth strategy for your business, keeping you protected from cybercrime.

To find out more contact our team of security consultants today.

+61 2 9221 5555 info@infotrust.com.au www.InfoTrust.com.au