SECURE ENDPOINT

Endpoint security is arguably a direct descendant of the first forms of computer protection in the early days of IT, when simple AV solutions were deemed to be enough. With technology advances and changing requirements to how organisations operate through cloud and mobility, the challenge of endpoint security has become more complex and requires a more comprehensive strategy.

WHY INFOTRUST?

- BEST-OF-BREED SOLUTIONS
- SPECIALISTS IN CYBERSECURITY
- EXPERTS IN ENDPOINT SECURITY
- CUSTOMER OUTCOME DRIVEN
- ELEVATE SECURITY MATURITY

NEXT GENERATION ANTI-VIRUS

80% of compromised endpoints were characterised as zero day threats for which legacy signature-based solutions were ineffective

60% of attacks are missed by legacy anti-virus/anti-malware solutions on average

The endpoint security threat landscape has changed. Long gone are the days where security and IT professionals were concerned about malware and signature-based attacks. Cybercriminals have evolved their tactics to bypass traditional anti-virus solutions to compromise endpoints. The rise of these file-less attacks means that on average traditional anti-virus solutions miss up to 60% of attacks. Next Generation Anti-Virus technology leans on machine learning, cloud scanning, automated remediation and forensics to provide a more proactive and system-centric approach.

ENDPOINT DETECTION AND RESPONSE

64% of organisations have had at least one endpoint compromised in the last year

40% of attacks on the endpoint are malware-free

As cybercriminals evolve their tactics, prevention on the endpoint is not enough. With the workplace becoming more agile, attackers have exploited endpoint security solutions that haven't been able to keep up. Once an attacker has access to an environment the average dwell time before detection is 90 days. Being able to detect threats and respond accordingly is paramount to keeping your organisation secure. EDR solutions brings immediate visibility to what is happening, enabling security teams to accelerate their threat response.

INCIDENT RESPONSE SERVICES

162 Hours to detect and respond to data breaches

1 in 3 organisations have been hit by a data breach in the last 12 months

Unfortunately, even with all the best preventative measures in the world the likelihood of your organisation experiencing a data breach at some point is significantly high. How a business responds to a threat will determine the related business impact and having a clear Incident Response (IR) plan in place will navigate a business to recovery. Implementing a response plan will give you peace of mind that you can confidently limit damage, recover your data and get your business back up and running as quickly as possible.

+61 2 9221 5555

www.InfoTrust.com.au

InfoTrust
Protection from Cybercrime

OUR INDIVIDUAL SERVICES

- ENDPOINT SOLUTION IMPLEMENTATION
- INCIDENT RESPONSE SERVICES
- PENETRATION TESTING
- VULNERABILITY SCANNING

VULNERABILITY MANAGEMENT

75% of organisations cite unpatched and outdated software as their greatest security risk

50% of managed cloud apps were targeted by credential attacks

Vulnerabilities in apps and operating systems being used within your organisation provide cybercriminals the opportunity to compromise your infrastructure. Attackers are constantly on the lookout for network weaknesses and if your business has a point of vulnerability, they'll find it. Although most organisations undertake vulnerability scans, legacy scanners can be slow and burdensome, reports can be difficult to digest and action, and scans based on networks alone can have blind spots. A Next Gen solution should enable you to see not only your security gaps but the gaps that your adversary is targeting delivering information straight to the hands of your security analysts, in real-time.

THREAT INTELLIGENCE

80% of companies report zero-day attacks are to blame for compromised endpoints

287 Days to identify a data breach on average

Businesses need to be empowered to make decisions on their cyber security strategy and take action against potential threats. Understanding the threat landscape and possible attack vectors as they evolve means you can be better prepared for future threats. Threat intelligence is a critical part of an IT security strategy; however, it involves a range of information from simple indicators to in-depth profiles. By having an instant analysis of threats that may reach your endpoints, your security team is able to effectively implement predictive security.

THREAT HUNTING

82% increase in ransowmare related data leaks in 2021 compared to the previous year

3.5 MILLION cybersecurity job openings worldwide by 2021

Endpoint security has come a long way with the evolution of Next-Gen solutions; however cybercriminals are still finding ways to outsmart this technology and quickly pivot to use other successful techniques. An additional layer of oversight and analysis provided by threat hunting capabilities is needed to ensure threats aren't missed and that your organisation doesn't fall victim to the next mega breach. Managed threat hunting adds an extra level of assurance by offering a team of dedicated, expert threat hunters to work on your behalf.

ENDPOINT IS THE LAST LINE OF DEFENCE

+61 2 9221 5555

www.InfoTrust.com.au

InfoTrust
Protection from Cybercrime