SECURE NETWORK

Every organisation, irrespective of size, industry, and infrastructure requires a combination of software solutions, architecture, processes and policies to protect its network from sophisticated cybercriminals and their ever-evolving techniques. Additionally, organisational networks are becoming increasingly complex and are continually subjected to new vulnerabilities that cybercriminals can and will exploit. In order to address these threats and vulnerabilities, it is vital to implement protective measures to secure your network.

WHY INFOTRUST?

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

NETWORK DETECTION AND RESPONSE

56% of breaches are taking months or longer to discover

71% of O365 users suffer malicious account take overs

Networks and the way we work have fundamentally changed. Organisational data is increasingly moving to the cloud and most organisations have adopted a hybrid work model. In fact, more than 70% of employees around the world are now remote. Cybercriminals have also pivoted their tactics, compromising unsuspecting users to get their credentials so they can exfiltrate sensitive data in the cloud. Compromised credentials are becoming a bigger threat to many organisations and require a different approach to security. InfoTrust offers a Network Detection and Response (NDR) solution to provide complete coverage over your cloud network. This solution tracks suspected attacks as they pivot between cloud and on-prem, and detects malicious intent by analysing how your hosts, accounts, and workloads are being used. This helps reduce the risk of a breach in your cloud and hybrid networks.

SD-WAN AND SECURE ACCESS SERVICE EDGE (SASE)

25% of users will manage their WAN through software within 2 years

80% of enterprises will have adopted SASE/SSE architecture by 2025

The increasing need to secure traffic from different locations whilst supporting flexible remote connectivity has given rise to Software-Defined Wide Area Networking (SD-WAN) for organisations to simplify operations, gain greater visibility and control, whilst improving the user experience.

The emergence of Secure Access Service Edge (SASE) has also come about which consolidates multiple point products including Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Zero Trust Network Access (ZTNA), Firewall as a Service (FWaaS), and SD-WAN, into a single unified service, reducing network security complexity whilst augmenting organisational agility.

+61 2 9221 5555

www.InfoTrust.com.au

InfoTrust
Protection from Cybercrime

OUR INDIVIDUAL SERVICES

- PROACTIVE CUSTOMER SUPPORT
- REGULAR CONFIGURATION REVIEWS
- CYBERSECURITY MATURITY ASSESSMENTS
- CISO SERVICES RETAINER

ZERO TRUST NETWORK ACCESS (ZTNA)

51% of workers work from home 2 to 3 days per week

76% of employees want to continue working from home at least part of the time

The attack surface has increased exponentially as a result of hybrid working and cloud transformation. Legacy remote access architectures are now vulnerable to more sophisticated attack techniques like user account compromise as they provide excessive access with no threat or vulnerability detection. Zero Trust Network Access (ZTNA) technology facilitates improvements in security, manageability, and scalability i.e. direct-to-app connectivity versus backhauling traffic to data centres. ZTNA paves the way for securing user access in an evolving world where work is now an activity, not a place.

DETECT, INVESTIGATE, & RESPOND. SECURE YOUR EXPANDED NETWORK PERIMETER

+61 2 9221 5555

www.InfoTrust.com.au

InfoTrust
Protection from Cybercrime