

SECURE CLOUD ACCESS



As organisations reap the benefits of moving their business systems to the cloud, they continue to face an evolving set of cyber security threats. Cloud applications allow for flexibility, agile working and increase productivity within your workforce, but also provide new challenges for data loss prevention.

How do you enable your organisation to continue this enhanced productivity and still ensure data governance within the cloud?

WHY INFOTRUST?

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



SECURE OFFICE 365

OVER 155 MILLION global business users of Office 365

39% of brand spoofed phishing attacks utilise the Microsoft name

In spite of the vast number of users and undeniable business benefits of Office 365, it's vital to not forget about security. Adopting the "good enough" security controls natively included has been the default choice for many. But this can leave your organisation open to unnecessary risk. InfoTrust can help your business augment its Office 365 defences for data breaches, targeted and account takeover attacks, data loss, and continuity.



CLOUD ACCESS SECURITY BROKER

OVER 50% of managed cloud apps were targeted by credential attacks

49% of companies believe their employees are unable to deal with the vast number of security alerts

Every organisation uses cloud apps to meet its business needs. Unfortunately, many are used under the radar without any security controls in place. Cloud services are a vital resource for organisations, which makes safeguarding data across all cloud platforms a critical requirement. A Cloud Access Security Broker enables businesses to gain visibility of all cloud services being used, identify risky applications, prevent the use of unsanctioned apps and data leakage.




SECURE WEB GATEWAY

22 WEBSITE VISITS a week per organisation are marked as risky or malicious

4,800 WEBSITES on average experience a form jacking each month

Increasing web use, rapid cloud adoption, and greater numbers of mobile and remote users expose your network to risk. Advanced threats can hide in plain sight on legitimate websites or in pop-up ads. Relying on your employees to know when not to click on potential threats is not enough, a layered security approach is necessary. A Next Gen Secure Web Gateway delivers a broad set of advanced capabilities including anti-virus scanning, sandboxing, web isolation, data loss prevention, and email security.

 +61 2 9221 5555

 www.InfoTrust.com.au



InfoTrust
Protection from Cybercrime

OUR INDIVIDUAL SERVICES

- CLOUD SECURITY IMPLEMENTATION
- SECURITY MATURITY ASSESSMENT
- WEB APPLICATION TESTING
- DATA GOVERNANCE ASSESSMENT



DATA LOSS PREVENTION

1
OUT OF
7

employees have deliberately exfiltrated data when they were about to leave the organisation

73%

of organisations blame immature security practices for cloud incidents

Traditionally, data loss has taken place via email, web or endpoint but as the IT infrastructure of businesses has evolved over the past decade to include more cloud-based applications, companies have needed to re-evaluate their data governance policies and cyber security strategy. By utilising a DLP technology organisations can control flow of data from their network, endpoints and cloud applications from a single dashboard. DLP solutions can also uncover data loss blind spots in sanctioned and unsanctioned cloud apps.



CLOUD AUTHENTICATION

64%

of businesses believe unauthorised access is to blame for cloud security incidents

43%

of companies aren't currently using multi-factor authentication

The increase and ease at which criminals are able to steal credentials through phishing means that all applications should be secured. The traditional method of single-factor authentication is no longer enough. Identity and Access Management technology enables you to empower your users to work more productively and securely by centralising cloud authentication and identity with single sign-on and multi-factor authentication.



SECURITY ACCESS SERVICE EDGE (SASE)

20%

of enterprises will adopt SWG, CASB, ZTNA and branch FWaaS by 2023

40%

of enterprises will develop strategies to adopt SASE by 2024

Cloud services, security and networking have quickly converged together, creating a new model where security and networking are delivered as software services alongside cloud-based applications. As a result, a simplified cloud-based environment has emerged, with a much more improved user-experience with a reduction in cost. This emerging security and network framework is called Secure Access Service Edge (SASE). SASE addresses the changing security landscape by protecting users, applications, and data outside of the traditional data center and in the cloud.

GAIN THE BENEFITS, SECURE YOUR USERS & DATA IN THE CLOUD



+61 2 9221 5555



www.InfoTrust.com.au



InfoTrust
Protection from Cybercrime