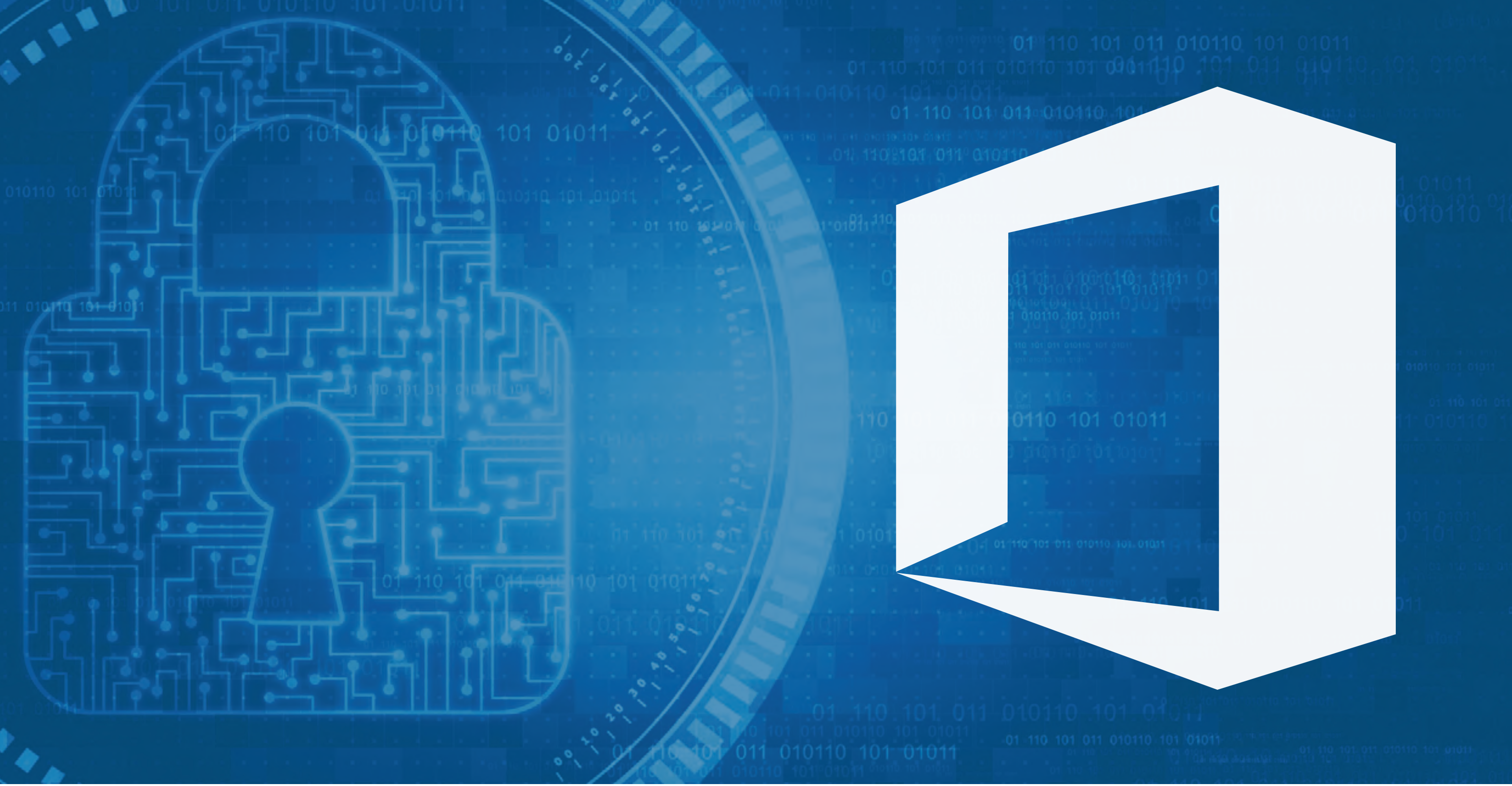


InfoTrust

A Guide To Securing **Microsoft Office 365**

Introduction

The number of businesses migrating to Microsoft Office 365 is soaring. It is responsible for helping a huge volume of organisations transition to the cloud and, according to its fourth quarter of 2018 results, it now has a staggering 31.4 million subscribers. Its popularity is due to the many benefits it offers, primarily mobility and collaboration. Office 365 is cloud-based, supplying a great variety of tools and applications that are easy for employees to access anywhere and anytime. Organisations using Office 365 have access to the latest versions of the likes of Excel, Word and Outlook as well as productivity platforms such as OneDrive, Yammer and SharePoint.

In spite of the vast amount of users and undeniable business benefits offered by Office 365, it's vital to not forget about security. The product provides the physical security of Microsoft's data centers along with intrusion prevention, and 24/7 resources to keep hackers out of their servers. With these measures in place, it can filter many large-scale, spam-like attacks and identify bulk malicious senders. As it does offer some level of protection, it is better than a lot of other cloud-based email providers. However, thought needs to be given to how well Microsoft prevents more sophisticated email-based attacks. If an email gets through their filters and into your inbox, it doesn't matter how secure their data center is. Businesses can easily make the mistake that Office 365 is an email security and compliance product. In fact, although there are some built-in email threat protection features, more often than not these are not sufficient to provide the protection organisations needs.

InfoTrust

Email has long been a primary channel for cyber criminals to use to gain access to business networks. The type of threats have grown along with the sophistication and now include the likes of business email compromise, ransomware and social engineering. The volume of these attacks is on the rise too, with **80% of organisations** having to deal with an email-based cyber attack in the last year. The financial implications of a cyber attack on businesses can be enormous, with the average data breach incident now costing companies an average of **$3.8 million**. As such, organisations need to maintain a high level of trust and confidence in their security measures. A simple MX record lookup will tell hackers that a company is using Office 365. This then gives them all the information they need to target their attack accordingly.

Organisations that are used to having robust email security are adopting complimentary email security to work alongside Office 365. This approach allows businesses to ensure that their security solution keeps up with the ever-changing nature of email security threats. Additional security should be layered with the existing features offered by Microsoft. The extra protection works to fill the gaps where Office 365's security falls short. In fact, many organisations migrate their users in stages to reflect their hybrid on-premise and cloud environment. Taking a phased approach enables companies to build up their expertise with cloud-based environments and to ensure they have secure employee usage before rolling out enterprise-wide.

In this guide, we'll cover the main areas of vulnerability that are not covered by Microsoft Office 365's native tools and measures that can be taken to overcome these. These best practices will ensure that whether you have, or are thinking of migrating to Microsoft Office 365, you are well equipped to meets your businesses security, compliance and governance requirements.

96%

of organisations have fallen victim to a BEC attack

Inbound Security

As we've already touched on, email is a primary route of attack for cyber criminals and actually accounts for over 95% of the world's security breaches. Migrating to Office 365 brings considerable benefits to an organisation, but it also opens up the possibility for cyber-attacks. The native security tools that come along with the Microsoft package will ensure your company isn't at risk from the likes of spam, known viruses and malware. However, the more sophisticated attacks such as business email compromise and spear phishing rely on identity deception, which is beyond the capabilities of native tools. Identity deception is such an effective method for hackers that it is used in nearly all of the more advanced attacks and this will only continue to rise. To mitigate the risk and stop these attacks, security needs to focus on determining sender trust and message authenticity, which is far too advanced for Exchange Online Protection.

In contrary to other approaches that try to predict bad behavior or detect malicious content, Agari Enterprise Protect integrates machine learning models to detect and block the most sophisticated email attacks. Machine learning and artificial intelligence enable the software to map communications to known correspondents and in doing so to detect behavioural anomalies. Understanding the trust relationships is key to revealing deception. Agari's vast network of support, deciphering over 2 trillion emails each year, allows its machine learning models to stay ahead of the attackers' sophisticated methods.

Archiving technology can reduce an organisation’s legal risk by

62%

Archiving & e-Discovery

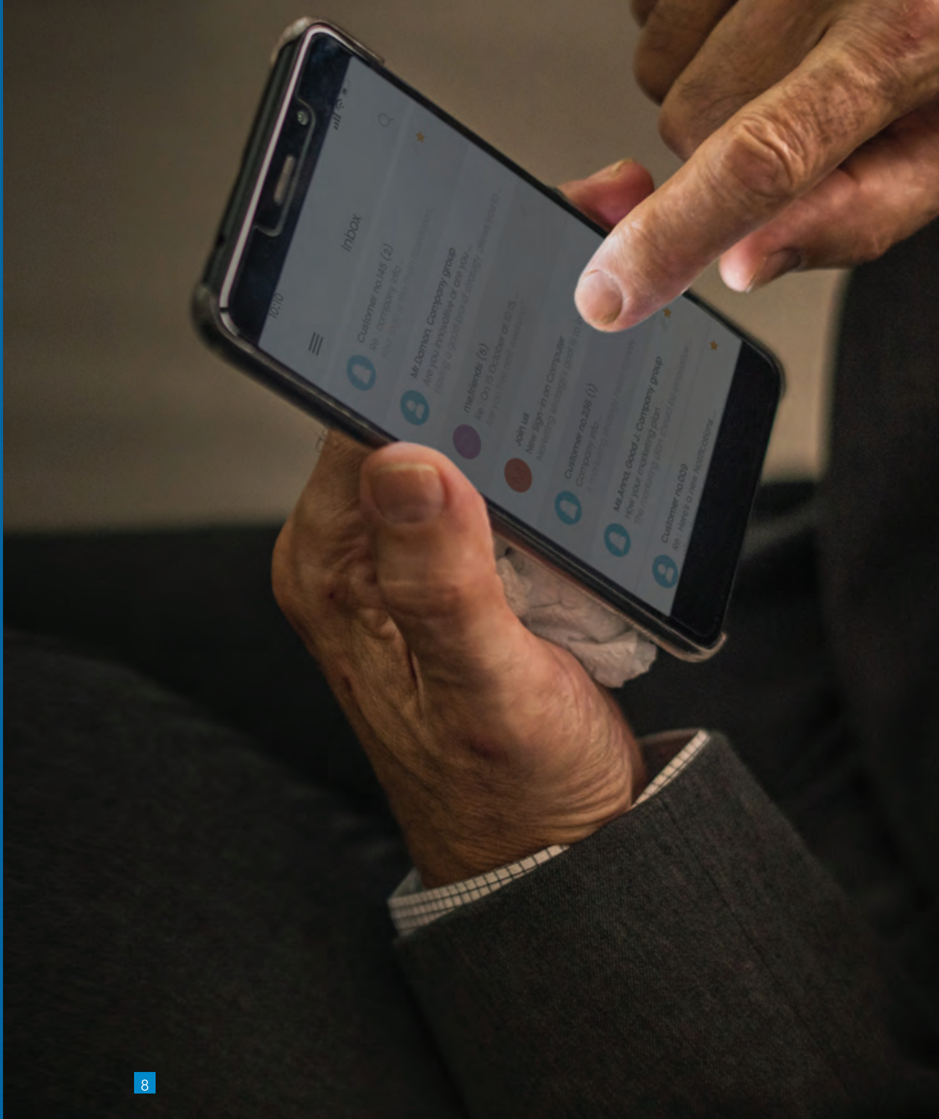
It's possible for businesses to find themselves involved in disputes of one form or another at any time and, in fact, it is a regular occurrence. Disputes can include anything from commencing proceedings for ownership of intellectual property, defending claims for unpaid invoices or responding to subpoenas for documents. As such, it is vital for organisations to implement a secure and reliable email and document archiving system. While Microsoft Office 365 offers the possibility to archive mailboxes in a bid to help retention management, it doesn't prevent users from deleting messages from within these mailboxes. To prevent the deletion of messages, the mailboxes require an in-place hold to be set up. Enabling this feature requires human intervention or scripts, which can fail without the organisation being made aware. Office 365 doesn't hold an immutable second copy of emails and documents, which means data loss is often irreversible. This represents a serious risk in relation to messages on litigation hold and users of Office 365 should carefully consider the limitations of the product and how they can mitigate the loss of vital documents. Meanwhile, the search functionalities of Office 365 are limited which can make discovery of vital documents a lengthy task. Unfortunately, time often isn't on your side when facing litigation, your organisation needs to be able to find relevant documents quickly and easily. It's vital for businesses to implement a secure archiving system prior to finding themselves in a dispute, this will enable them to preserve data, control litigation costs and mitigate future risk.

Veritas Enterprise Vault.cloud can both help ensure a smooth migration to Office 365 and document retention and compliance for its ongoing use. Veritas EV.cloud captures email as journaled records, allows you to quickly find information through iterative searches, and creates a positive archiving user experience. Archived information is kept in a single repository with unlimited storage that is protected against unauthorised or accidental deletion. What's more, organisations are able to implement automated retention policies that ensure regulatory compliance.

The average cost to an organisation for unplanned downtime is

$111,000

per hour



Email Continuity

Email continuity is a vital consideration for organisations, and it needs to be considered for both the migration to and use of Microsoft Office 365. Email is an essential form of communication for the majority of businesses. Any loss of connectivity will affect users productivity. The result is that any loss, albeit even temporary, of access can have serious financial implications. In addition to this, email acts as the single largest repository of corporate memory and information. While Microsoft Office 365 offers amazing resources for productivity and collaboration, archiving email continuity requires additional third-party solutions.

To ensure email continuity in Office 365, you need robust security, dedicated support and the ability to access mail even when servers are down. Veritas EV.Cloud offers all of this and includes an add-on feature that allows users to send and receive emails during server outages. EV.Cloud can be configured as a secondary gateway to ensure continuity during a Microsoft server outage. During the outage, your security provider will route the mail to EV.Cloud allowing users to send and receive mail. When the outage ends the continuity service automatically flushes all of the messages to the mail server to resume normal delivery.

Account takeover based attacks increased by

126%

in 2018

Account Takeover Risk

Targeted email attacks resulting in account takeovers are a huge risk to businesses and one that, yet again, is on the rise. The reason for this is that they are so effective, which only motivates attackers further. What's more, the cloud-based nature means that accounts can be accessed from anywhere, which again adds to the threat level. Microsoft Office 365 has become so commonplace that it has become part of many of our internal business identities. As such, we inherently trust emails that appear to come from this source, we assume they are legitimate. Unfortunately, this is not always the case. Office 365 has become a common target for highly personalised and compelling attacks. Attackers attempt to steal login credentials which then give them access to launch internal attacks. All hackers need is a username and password to gain the power to take over all of your accounts. Once all of your corporate data resides in the cloud, the attack is even more valuable to them. Microsoft's product isn't sufficient to protect your organisation. A large part of this is due to the fact that hackers test their attacks against the default security system. By the time of their actual attack, they have confidence that they will be able to get in.

Okta is the leading cloud identity management service that enables easy integration of multi-factor authentication. What this means is that users need to verify their claimed identity, so, even if hackers get hold of an account password, they can't immediately gain access to your company. Standard authentication strategies haven't evolved in many years, whereas Okta's identity approach offers a secure solution that is cloud-focused and ideal for Office 365 users with instant integration. Okta's multi-factor identification includes one-time passwords, physical tokens and even biometrics. On top of this identity is centralised so that multiple passwords aren't necessary, single sign-ons allow passwords to be as strong as possible. The attack surface is reduced by the implementation of lifecycle management and visibility of who has access to what at any given time. Okta provides full reporting and identifies any unusual behavior in real-time. The result is that your data is protected no matter where or how it is accessed.

74%

of organisations use SaaS-based services

Data Backup

Many organisations that implement Microsoft Office 365 don't realise where Microsoft's responsibilities regarding backup and recovery end, and where theirs begin. Although Microsoft provides off-site infrastructure, it is not responsible for protecting data against the likes of human error, deletion and malware. It is the business' responsibility to protect data that is stored in the Microsoft cloud. Short-term and item-level recovery is possible, but you are not able to perform defined time recovery of lost data. Even if data is retrievable, the process is long and complicated, and each application varies. This means that, without additional security, data that is either accidentally or maliciously deleted or corrupted isn't guaranteed to be recoverable. Data loss and protection should be a major consideration for any organisation considering migrating to the cloud. Organisations need to ensure they follow business best practice guidelines for automated backup and recovery. Failing to backup cloud data could put your business at significant exposure.

Veritas SaaS Backup is a cloud-host, comprehensive and cost-effective solution designed specifically to protect data in companies using cloud-based software such as Microsoft Office 365. The simple integration process links your Microsoft Office 365 online account with Veritas SasS Backup, giving you access anytime, anywhere and from any device. The service boasts an astonishing 99.9% uptime, backs up up to six times a day and instantly restores. As it is based on the cloud, it offers unlimited storage and no time is required for installing, deploying or upgrading.

Microsoft Office 365 Migration Health Check

Microsoft Office 365 Health Check

Companies who are migrating or have migrated to Office 365 are turning email into part of a much larger ecosystem. Securing Office 365 requires more than the simple protection of inbound messages. Organisations need to detect compromised accounts, ensure their data across email SharePoint, OneDrive and other productivity apps is discoverable, highly available and complies with regulations. Any security solution that is integrated must incorporate all the parts of the Office 365 environment alongside your broader Enterprise architecture. This is done by creating a multi-layered approach to security where third-party solutions are implemented to add to the existing security in place, natively available from Microsoft.

If your business is about to migrate to Microsoft Office 365 or already has, it's vital to establish the right security measures in place. Go to InfoTrust.com.au/o365 to find out more and request a free Office 365 health check. Alternatively, contact us directly via the details on the next page.

InfoTrust

☎ +61 2 9221 5555

✉ info@infotrust.com.au

www.infotrust.com.au

Visit
infotrust.com.au/o365
to find out more