Executive Summary:

A Guide to Protecting Microsoft Office 365 from Security Threats

by Mark Bowker, ESG Senior analyst

August 2018

It's no secret that cybersecurity permeates the mindsets and priorities of key business executives all the way up to the CEO level. At the same time, IT has to manage a balanced corporate security posture that provides a frictionless approach to protecting employees and the business in the midst of device proliferation, cloud consumption initiatives, and changes in where work is getting done.

Beyond Microsoft Office 365 Basics

Microsoft Office 365 (O365) triggers security concerns and potential new opportunities. O365 adoption has triggered companies to think of how they can replicate their cloud strategy and security posture across multiple clouds and an entire suite of business applications they need to support and protect.

74%
of organisations are already using software-as-a-service in some capacity

In 2013, 61% of SaaS users delivered no more than 20% of their applications via SaaS. Today,

63%
report that SaaS currently accounts for more than one out of five of their business applications.

More than one-third
of all organisations surveyed in 2017 said that they currently used cloud-based email (39%) and/or office productivity software (37%)

Microsoft is aggressively migrating companies to O365—inclusive of Exchange email, OneDrive (file sharing and storage), and SharePoint/Sites/Teams/Groups/Yammer (collaboration)—and also transforming the way IT services (inclusive of security) are delivered. As a result, businesses are finding themselves investigating ways to embrace and protect O365 along with a plethora of other cloud-based applications and data.

Threats Can Strike Any Time, Any Place…

As companies migrate to Microsoft O365 and other cloud applications, they are not always aware of potential threats, policies with limited effectiveness, and vulnerabilities resulting from accidental configuration. Business are still responsible for monitoring and controlling how applications are used, content is monitored, and data is secured. As a result, they may find themselves at risk without fully understanding where they are truly vulnerable.

To secure this range of cloud applications—some sanctioned and supported by the IT organisation, and other shadow IT constituents bending the rules based on application preference without the knowledge or support of IT—some organisations have initially recognised the need for cloud access security broker (CASB) solutions to provide user behavior analytics (UBA) to determine anomalous user patterns, data protection status, threat detection/prevention strength, and breadth of overall security coverage across a variety of cloud applications (O365 and beyond). In fact, 57% of respondents identified 0365 as one of the (top five) applications most in need of the user access and data loss prevention controls and policies that CASB products provide.

Email continues to be a top attack vector for malicious attacks and data breaches.

66%
of malware is installed via malicious email attachments.

90%
of incidences and breaches included a phishing element.

21%
of ransomware involved social actions, such as phishing.

43%
of all breaches included social tactics.

93%
of social attacks were phishing related.

28%
of phishing attacks were targeted.

There is also a rise in file-less malware (i.e., weaponised content) and, according to the 2018 Verizon data breach incident report (VDBIR), 68% of breaches took months or longer to discover.

… and Vulnerabilities Can be Left Exposed

A security breach is not merely inconvenient. It can be costly, stressful, and even damaging. Businesses must consider how to provide visibility, control, access governance, data security, and threat protection for Office 365 along with other SaaS apps and infrastructure services. Too often, businesses embrace O365 without considering all the security implications across the organisation or the potential external vulnerabilities. Adoption of Office 365 moves key information outside of corporate control and creates risk to intellectual property and compliance-sensitive information.

As a result, IT organisations, security teams, and business executives are currently dealing with the following concerns:

- Multiple new security requirements have arisen with the shift to cloud consumption models that potentially put confidential data at risk.
- Lack of visibility, monitoring, and control across all applications and data.
- Fragmented vendor base promises built-in security and overlapping bolt-on toolsets.
- IT organisations and business units are moving quickly to adopt many cloud applications (not just O365).
- Regulatory compliance risk is increasing, especially with the adoption of new regulations such as GDPR.
- Organisations don't have enough qualified IT security experts on staff.

Common considerations include:

- Guard against new and emerging multi-vector attacks (web, email, endpoint, and collaboration apps).
- Protect SaaS applications, inclusive of O365 and other business SaaS apps.
- Gain control of content: tracking, access, email, sharing…across all business applications.
- Keep key information under corporate control for consistency and visibility.

Goals to Guide Safe O365 Migration

ESG has witnessed some common goals that have helped organisations to address the known and unknown challenges that they face as they scale O365 implementations and prepare for further O365 migrations:

- Secure accounts for sanctioned and unsanctioned applications.
- Create a cohesive strategy to secure the movement to cloud.
- Embrace high-efficacy threat protection.
- Maintain compliance and protect sensitive information within O365, existing business applications, and existing data across on-premises and cloud consumption models.
- Reduce security operational costs with a solution that supports Office 365, other cloud apps, and hybrid cloud environments.
- Improve security processes by using solutions that embrace automation and integration across all business applications to help reduce administrative overhead.
- Consider the value of artificial intelligence (AI)- driven user and entity behavioral analytics (UEBA), automated data classification, and automated policy responses.
- Consider the value of advanced machine learning and threat isolation technologies to address sophisticated and evolving malicious threats.

Protect Information and Protect against Advanced Threats in Email and Apps in Office 365 and Beyond

Security, Compliance, and Threat Protection for Office 365 with CloudSOC CASB and Email Security

Symantec is helping businesses achieve their O365 migration goals through a set of security and information compliance controls that protect Office 365.

For more comprehensive information, including the O365 Security Checklist, email us at info@cstl.com

CST Celebrating 22 YEARS DEDICATED TO THE SECURITY OF INFORMATION