

THREE KEY QUESTIONS TO SECURE YOUR MICROSOFT OFFICE 365 DEPLOYMENT


TABLE OF CONTENTS



EXECUTIVE SUMMARY




CLOUD-BASED PRODUCTIVITY BRINGS NEW RISKS




QUESTION 1

ARE THE PEOPLE ACCESSING
CORPORATE DATA THROUGH
OFFICE 365 MY EMPLOYEES?



QUESTION 2

WHAT INFORMATION IS IN
OFFICE 365, AND HOW EASILY
CAN IT BE SHARED?



QUESTION 3

IS MY EMAIL PROTECTED
FROM DELIVERY OF
MALWARE?



CONCLUSION



EXECUTIVE SUMMARY

Microsoft Office 365 is already dominant in the marketplace and is poised to surpass 75% market share this year. The cloud-based productivity suite interacts with a vast amount of corporate data including email (Outlook Online), individual file storage (OneDrive), and even financials (Excel Online). Its built-in security tools are helpful but inadequate, and organizations would do well to ask a few questions before they deploy Office 365:

- *Are the people accessing data through Office 365 my employees?* Stolen credentials are a major source of data loss, and privileged users have traditionally been trusted across the network after logging in once. A simple username and password are not adequate.
- *What information can be shared from Office 365, and with whom?* Like most cloud solutions, the default setting in Office 365 is unlimited sharing of files and other data internally and externally. Organizations must be strategic about how to prevent data loss.
- *Is my email protected from delivery of malware?* More than 90% of malware is still delivered by email, and email threats have become more sophisticated. Organizations must consider whether Microsoft's email security is adequate, or whether the Office 365 environment should be protected with a secure email gateway (SEG).

The best solution is an integrated approach that eliminates silos and brings all elements of security together. The Fortinet Security Fabric is a consistently highly rated solution that brings the whole security infrastructure under a single pane of glass.

CLOUD-BASED PRODUCTIVITY BRINGS NEW RISKS

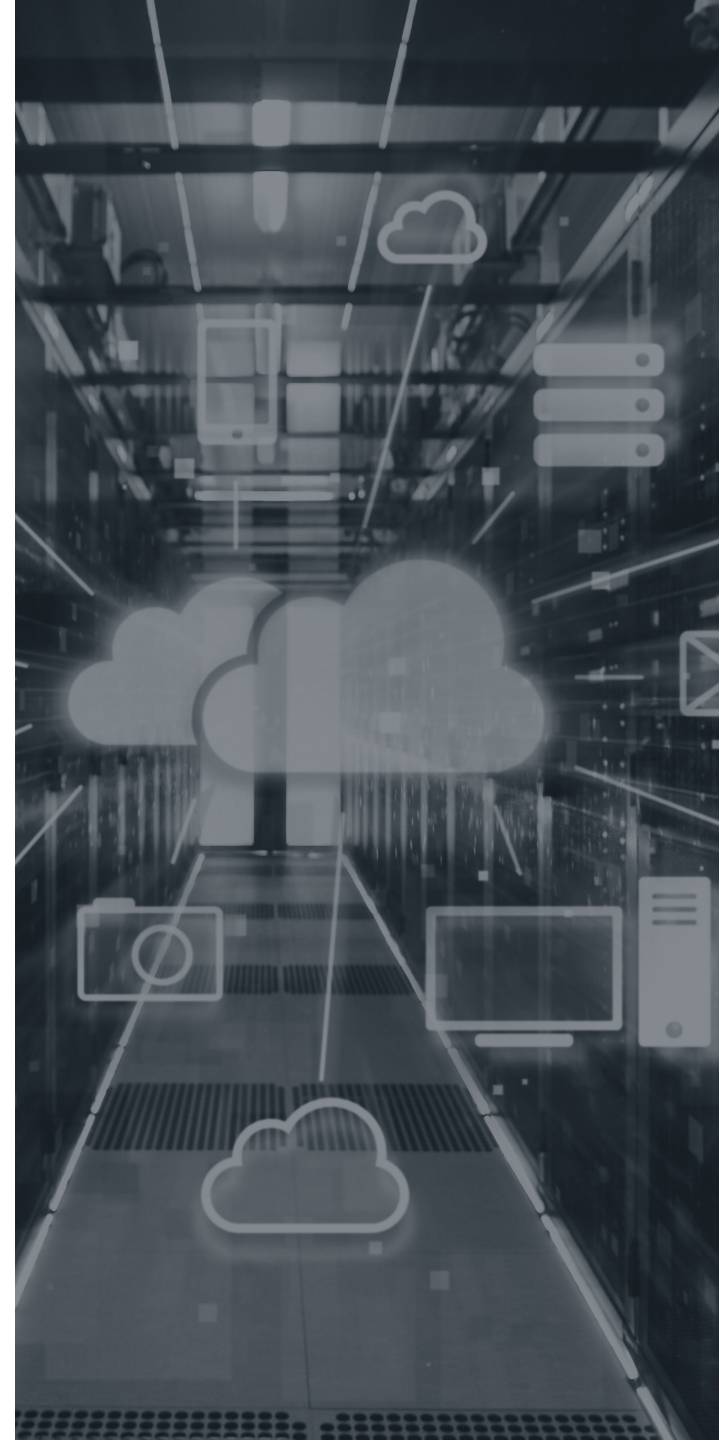
Microsoft Office 365 is a powerful, cloud-based business productivity solution. According to Osterman Research, adoption of Office 365 has reached 62.4% of organizations in January 2018 and is projected to reach 78.1% by early 2019.¹

Customers of cloud services in general, and Office 365 in particular, typically shift workloads to the cloud for its predictable cost and elastic capacity and to reduce staff time spent on mundane infrastructure management. This can promote cost savings and enable the organization to place more focus on its core business priorities. However, the use of Office 365 and its cloud-based productivity tools, email infrastructure, and data storage also introduces considerable risks. These include:

- Impersonation of privileged users by cyber criminals, resulting in data theft and other risks
- Internal and external sharing of corporate information via Office 365
- Delivery of malware via email in the Outlook Online component of Office 365

Certainly, there are important foundational security controls built in to Office 365 and included with the most common E3 license. And for an extra charge, Microsoft offers additional protection capabilities in the E5 and other license mechanisms. But are these offerings enough? Following are three security-related questions you should ask when deploying Office 365:

¹ ["Supplementing the Limitations in Office 365,"](#) Osterman Research, March 2018.



QUESTION 1: ARE THE PEOPLE ACCESSING CORPORATE DATA THROUGH OFFICE 365 MY EMPLOYEES?

According to research by Verizon, the use of stolen credentials was the number one action leading to breaches in 2017.² Privileged users present an especially high risk, as they have access to more data and generally are trusted across the network once they log in. A username and password are no longer sufficient; rather, a multipronged approach is critical.

Of course, the process should start with the integration, or federation, of external clouds with the organizational directory service to ensure a single source of truth for who gets access. Beyond that, users ideally should be verified through both strong multifactor authentication and activity logging.³ Multifactor authentication requires a second step to verify identity—a hard or soft token, for example. Activity logging uses machine learning to analyze past login

activity of specific users and detect anomalies such as differences in time of day and type of data accessed.

At a minimum, consider using the baseline two-step authentication found in Office 365. However, given the challenge of managing identity and access on the network and in each cloud, many organizations utilize more robust identity and access management solutions that work across environments

as well as provide stronger (and often easier) methods of multifactor authentication. Increasingly organizations are taking advantage of Identity and Access Management as a Service (IDaaS), with authentication as the most important function.

² “[2018 Data Breach Investigations Report](#),” Verizon, April 10, 2018.

³ Gartner, [Clouds Are Secure: Are You Using Them Securely?](#), January 31, 2018.

**The foundation for
the well-managed
use of external
clouds of all types is
identity governance
and administration.**

Gartner, [Clouds Are Secure: Are You Using Them Securely?](#), January, 31 2018.

**GARTNER
RECOMMENDATION**

QUESTION 2: WHAT INFORMATION IS IN OFFICE 365, AND HOW EASILY CAN IT BE SHARED?

As Gartner reports, most SaaS applications make it quite easy for individuals to inappropriately share data internally—and even externally—with little or no authentication required for access. Unfortunately, several of the most popular SaaS applications default to allowing all users to share all data with anyone in the world.⁴

Information Rights Management in Office 365 is actually a rather good start, with data loss prevention (DLP) policy templates and reports in the Security and Compliance Center. This protects your Office 365 environment; however, your data lives not only in the Microsoft suite but also in your on-premises network and across other clouds. In order to protect all this data, we need to know where it is and identify its type. This is also necessary for

compliance with standards and regulations on some types of data.

According to the Fortinet Threat Landscape Report, the average organization utilizes an average of 37 cloud applications.⁵ It quickly becomes apparent why a single mechanism to identify and protect data in multiple cloud applications is valuable. And it's a bonus when it is integrated with data controls on-premises for consistent enforcement and consolidated reporting.

As Gartner notes, CASBs provide a consistent and convenient point of control over user activity and user data in a growing set of SaaS and other cloud-based applications.⁶

⁴ Gartner, [Clouds Are Secure: Are You Using Them Securely?](#), January 31, 2018.

⁵ [“Threat Landscape Report Q1 2018,”](#) Fortinet, April 2018.

⁶ Gartner, [Magic Quadrant for CASB](#), November 30, 2017.

CASBs have become an essential element of any cloud security strategy, helping organizations govern the use of cloud and protect sensitive data in the cloud.

Gartner, [Clouds Are Secure: Are You Using Them Securely?](#), January, 31 2018.

QUESTION 3: IS MY EMAIL PROTECTED FROM DELIVERY OF MALWARE?

With the maturity of cyber crime and its supporting infrastructure, threat volume and velocity continue to accelerate. In the first quarter of 2018, FortiGuard Labs reported 15,671 new malware variants,⁷ making more advanced security technologies like sandboxing and outbreak protection services a requirement. And email remains the dominant delivery method for malware. In 2017, 92.4% of malware—including 49% of malware successfully installed—came via email.⁸

New email attack classes like business email compromise cost businesses an estimated \$675 million in 2017, and the increasing use of embedded rather than attachment-based malware makes it harder to stop. Clearly, protecting email in the Office 365 cloud is of paramount importance.

Many organizations begin by trying out the built-in protections that come with Exchange Online in Office 365. And, in fact, many continue to use

them to handle garden-variety spam and known malware. However, nearly half (40% to 50% depending on the analyst firm cited) choose third-party security components to provide added protection, and often to integrate with other security controls.

Indeed, Gartner notes that most multiproduct vendors in this market, distracted by other products in a broader portfolio, had allowed development of their secure email

gateways (SEGs) to wane. As the threat landscape shifted, they were caught flat-footed and scrambled to iterate their products. In contrast, vendors that continued to invest in their SEG products all along were able to use this as a competitive advantage.⁹

⁷ [“Threat Landscape Report Q1 2018,”](#) Fortinet, April 2018.

⁸ [“2018 Data Breach Investigations Report,”](#) Verizon, April 10, 2018.

⁹ Gartner, [Market Guide for Secure Email Gateways](#), May 7, 2017.

**Supplement gaps
(if replacement is
not an option) in
the advanced threat
defense capabilities of
an incumbent SEG by
adding a specialized
product that is tailored
for this purpose.**

Gartner, [Market Guide for Secure Email Gateways](#), May 7, 2017.

**GARTNER
RECOMMENDATION**

CONCLUSION

With more than three out of four organizations moving to Office 365 by early 2019, securing this powerful, cloud-based business system is critical. While there are many baseline security controls included in the standard Microsoft E3 license that should be properly utilized, organizations should strongly consider added measures, such as those in the E5 license or independently proven security components from expert third parties.

Of note, Fortinet offers additional recommended controls:

- Identity and Access Management, including software-based multi-factor authentication, with the FortiAuthenticator and/or FortiToken product lines.
- Data and Threat Protection for Office 365 and other popular SaaS applications from the FortiCASB offering, as well as FortiGate and FortiMail.
- Advanced Threat Defense, including

capabilities recommended in Gartner's SEG Market Guide from the FortiMail family.

While there are other vendors offering similar components, individually or all three, only Fortinet delivers:

- Independently and consistently top-rated threat protection for on-premises and multi-cloud environments—including Office 365 components such as Exchange Online and OneDrive.

- A common user interface and administrative experience across components.
- A free, no-obligation Email Risk Assessment to audit the effectiveness of security on the delivery channel for 92.4% of malware.