FORTINET

Security for Microsoft 365: 3 Critical Strategies to Consider

Table of Contents

Executive Overview

With over 258 million paying users, Microsoft 365 holds the enviable position as leader in terms of customer and user subscriptions versus Google Workspace.[1] The cloud-based productivity suite interacts with a vast amount of corporate data within email, in files located in individual OneDrive storage, in spreadsheets, in presentation files, and so on. Its built-in security tools are helpful but inadequate—and organizations would do well to ask a few questions before they deploy Microsoft 365:

- **How well is Microsoft 365 protecting my organization from email-based threats such as phishing, malware, impersonation, and business email compromise (BEC) attacks?** SE Labs found that, even with Microsoft 365 Defender enabled, Microsoft 365 had a total accuracy rating of less than 30% when it came to spam, phishing, and malware-infected emails. Because email remains a top threat vector for malicious content, organizations must consider whether Microsoft's email security is adequate for their needs.[2]
- **Are the people accessing Microsoft 365 my employees and are they using devices that are compliant with our security policies?** Access control and endpoint protection should be part of any Microsoft 365 deployment. 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.
- **Does my Microsoft 365 deployment include sensitive data, and who is accessing it?** Data loss prevention is a key attribute of any attempt to secure Microsoft 365. Like most cloud solutions, the default setting in Microsoft 365 is unlimited sharing of files and other data internally and externally. Organizations must take a strategic approach to preventing data loss.

This eBook will answer these questions and provide key strategies for securing organizations using Microsoft 365.

Cloud-based Productivity Brings New Risks

Microsoft 365 is a powerful, cloud-based business productivity solution. However, the use of Microsoft 365 and its cloud-based productivity and collaboration tools, email infrastructure, and other components can expose organizations to security risks.

Customers of cloud services in general, and Microsoft 365 in particular, typically shift workloads to the cloud for predictable costs and elastic capacity, as well as 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 Microsoft 365 and its cloud-based productivity tools, email infrastructure, and data storage can simultaneously introduce cyber risks. These may include:

- Impersonation of privileged users by cyber criminals, resulting in data theft
- Internal and external sharing of corporate information via Microsoft 365
- Delivery of email-borne threats, including content-based, malware-based, and link-based attacks

While there are many foundational security controls built into Microsoft 365 and included with the most common E3 license and expanded controls in the E5 license, organizations will need to evaluate these controls to determine how effectively they mitigate risks and align with the organization's overall security and compliance needs.

Strategy I: Email Security

How well is Microsoft 365 protecting my organization from email-based threats such as phishing, malware, impersonation, and business email compromise (BEC) attacks?

According to Gartner, 71% of companies were using cloud or hybrid cloud email services in 2020.[3,4] Meanwhile, research shows that email remains a primary threat vector. Verizon's 2020 Data Breach Investigations Report revealed 22% of breaches were caused by "social actions" where the intent was to play on user or employee behavior. With 96% of these social actions delivered via email and 90% of those being classified as phishing, IT and IT security teams must take a hard look at their email security solutions and validate their effectiveness against the full spectrum of email-based threats.[5]

Though Microsoft offers various security options to harden Microsoft 365, independent tests show Microsoft 365 Exchange Online Protection (EOP) and Advanced Threat Protection (now called Microsoft 365 Defender) perform poorly compared to other vendor solutions. In fact, testing by SE Labs showed that Microsoft 365 native security tools scored a total accuracy rating of 29% (EOP) and 28% (Defender), which earned Microsoft 365 a "C" rating. By comparison, Fortinet's Total Accuracy Rating was 90%.[6]

Executive Summary				
Product	Protection Accuracy Rating	Legitimate Accuracy Rating	Total Accuracy Rating	Total Accuracy Rating (%)
Fortinet FortiMail	2,525	640	3,165	90%
Google G Suite Business	825	535	1,360	39%
Microsoft Office 365	463	550	1,013	29%
Microsoft Office 365 Advanced Threat Protection	426	550	976	28%

Figure 1: SE Labs found Microsoft EOP and Defender both trailed all other venders in accurate threat detection.

Fortinet
Recommendation

Perform testing of Microsoft 365 native email security tools to identify gaps, performance issues, and potential risks the tools do not address. For organizations that may not have the ability to perform a side-by-side comparison, Fortinet offers a free Email Risk Assessment.

Strategy II: Identity and Access Management

Are the people accessing Microsoft 365 my employees and are they using devices that are compliant with our security policies?

"Criminals are clearly in love with credentials, and why not since they make their jobs much easier?"[7] Credential theft remains a primary objective for threat actors because it provides cyber criminals the ability to access environments under the guise of a legitimate user. Of the breaches caused by social actions, 62% resulted in the theft of credentials, while the favorite malware for threat actors are password dumpers.[8] All of this makes the use of usernames and passwords for identity and access administration grossly inadequate to address these risks. Instead, a multipronged approach becomes critical.

This process should start with the integration 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 multi-factor authentication (MFA) and activity logging. MFA requires a second step (e.g., a soft or hard token) to verify identity. Activity logging uses machine learning to analyze past logins of specific users and detect anomalies such as differences in time of day and types of data accessed.

Securely and effectively managing identity authentication and authorization for all systems and applications across both on-premises and cloud environments is crucial to minimize security breaches.

At a minimum, consider using the baseline two-step authentication found in Microsoft 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 MFA. Increasingly, organizations are taking advantage of Identity and Access Management-as-a-Service (IDaaS), with authentication as the most important function. Device management is also a key function of access control—is the device used to access sensitive data up to date, secured, and compliant?

Fortinet
Recommendation

Deploy sound identity and access protections based on strong multi-factor authentication and tokenization best practices.

Strategy III: Application and Data Security

Does my Microsoft 365 deployment include sensitive data, and who is accessing it?

According to Blissfully, midsized organizations use on average 185 Software-as-a-Service (SaaS) applications across their organizations, while SaaS applications churned at a staggering 58% over two years. Meanwhile, enterprises use on average 288 SaaS applications with 60% churn over the same period.[9] Recognizing the dynamic nature of SaaS application usage in organizations, 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.

Information Rights Management in Microsoft 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 Microsoft 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.

That's where cloud access security brokers (CASBs) come in. As Gartner notes, "CASBs provide a central location for policy and governance concurrently across multiple cloud services and granular visibility into and control over user activities and sensitive data from both inside and outside the enterprise perimeter, including cloud-to-cloud access."[10]

Cloud access security broker (CASB) products provide critical protection of employees, corporate environments, and data when using SaaS applications, especially in a post-COVID-19 world.

An effective CASB solution can provide:

- **Visibility:** Understand both sanctioned and unsanctioned SaaS application usage.
- **Data Security:** Extend data-centric security policies to the cloud and protect valuable data and intellectual property assets.
- **Threat Protection:** Identify and address risky activity and data at risk.
- **Compliance:** Ensure SaaS usage aligns with corporate compliance policy requirements.

Companies that use CASB solutions also experienced additional business value, such as improved collaboration and enhanced employee productivity, faster time-to-market due to the ability to launch new products more quickly, and stronger business growth.[11] All of these benefits mean that it is critical for organizations utilizing Microsoft 365 to consider CASB solutions in the broader context of their organization's overall SaaS usage and application security strategy.

Fortinet
Recommendation

Implement cloud access security broker (CASB) services to address critical application and data security risks associated with the broader use of SaaS applications across the organization, including Microsoft 365.

Conclusion

With over 258 million paid users of Microsoft 365, it is imperative that organizations understand the potential risks and limitations of Microsoft 365's native security capabilities.[12] While there are many baseline security controls in the standard E3 license and expanded controls in the E5 license, organizations should strongly consider independently validated and proven security components from expert third parties like Fortinet.

[1] "Microsoft FY20 Third Quarter Earnings Conference Call - Michael Spencer, Satya Nadella, Amy Hood," Microsoft, April 29, 2020.

[2] "Email Security Services Protection," SE Labs, January-March 2020.

[3] Gartner, "Market Guide for Email Security," authors Mark Harris, Peter Firstbrook, Ravisha Chugh, published September 8, 2020.

[4] "2020 Businesses@Work Report," Okta, 2020.

[5] "2020 Data Breach Investigations Report," Verizon, May 2020.

[6] "Email Security Services Protection," SE Labs, January-March 2020.

[7] "2020 Data Breach Investigations Report," Verizon, May 2020.

[8] Ibid.

[9] "The 3 Biggest SaaS Trends in 2020," The Blissfully Report, Blissfully, March 10, 2020.

[10] Gartner: "Magic Quadrant for Cloud Access Security Brokers," authors Craig Lawson and Steve Riley, October 28, 2020.

[11] "Cloud Adoption and Risk Report," McAfee, June 2019.

[12] "Microsoft FY20 Third Quarter Earnings Conference Call - Michael Spencer, Satya Nadella, Amy Hood," Microsoft, April 29, 2020.

www.fortinet.com

873173-A-0-EN

February 17, 2021 11:42 PM

ebook-microsoft-365-873173-A