SOLUTION BRIEF

Securing Microsoft 365: Advanced Security and the Fortinet Security Fabric

Executive Summary

Over 258 million people use the Microsoft 365 productivity and collaboration suite today.[1] However, while there are many important foundational and premium security controls built into Microsoft 365, IT and security teams will need to evaluate these native controls to determine how effectively they mitigate risk and align to their organization's overall security and compliance needs.

Fortinet security solutions including email security, SaaS application security, malware protection, and identity and access management products—all part of the Fortinet Security Fabric—provide comprehensive protection for organizations using Microsoft 365. This solution brief provides an overview of Fortinet solutions to provide robust protection for employees, applications, and data when using Microsoft 365.

Close Security Gaps With the Fortinet Security Fabric

Fortinet provides a wide range of integrated capabilities as part of the Fortinet Security Fabric to address security gaps and risk posed to Microsoft 365 users. Key Security Fabric elements for Microsoft 365 users include:

- FortiMail to deliver email security
- FortiCASB to monitor Microsoft 365 usage, data, and configurations
- FortiSandbox for advanced malware and malicious link detection
- FortiAuthenticator and FortiToken for access management and multi-factor authentication (MFA)

Enhance Email Security Protections

Email remains a primary threat vector for bad actors. According to Verizon, 22% of breaches were caused by "social actions," with 96% of these social actions delivered via email. Of those, 90% were classified as phishing.[2] At the same time, email was involved in 54% of malware delivery either through attachments or links to content.[3] Unfortunately, Microsoft 365 Exchange Online Protection and Microsoft 365 Defender tools do not effectively protect email from threats. According to SE Labs, Microsoft 365 Defender scored a low 28% Total Accuracy Rating in testing across email threats and spam.[4]

FortiMail for Email Security

To protect users, customers, and business, it is critical to deploy email security tools. FortiMail enhances email security for Microsoft 365 users with:

- Comprehensive threat protection against the full spectrum of email-borne threats
- Top-rated FortiGuard Labs security services, including antispam, antivirus, sandboxing, content disarm and reconstruction, click protection, impersonation analysis, and more
- Open application programming interfaces (APIs) for intelligence sharing across the Fortinet Security Fabric
- Email data loss prevention (DLP) to protect against egress of sensitive information and data
- Integration with FortiGate, FortiAnalyzer, and FortiSIEM for a single view of security

Secure SaaS Applications, Usage, and Data

Providing comprehensive protection for cloud solutions is a challenge, with Software-as-a-Service (SaaS) vendors such as Microsoft controlling not just the infrastructure but also the application layer.

FortiCASB for SaaS Protection

Fortunately, it is now common practice for major cloud providers to provide API-based access to their SaaS offerings. This allows Fortinet FortiCASB to complement the built-in visibility of the Microsoft 365 Admin Center, security tools to assess and report on users, behaviors, and data associated with Microsoft 365 and other SaaS applications. More importantly, it also enables advanced FortiCASB functions to extend security policies and intelligence to data centers.

Specifically, Microsoft 365 customers are able to:

- Inspect content in transit or at rest for threats with the threat intelligence of FortiGuard Labs AV and sandbox services
- Monitor and ensure appropriate user behavior and entitlements
- Identify and control authorized use of a wide range of sensitive data types, as defined by industry regulations or corporate policy
- Discover and similarly control other cloud applications and infrastructure
- Integrate with FortiGate, FortiAnalyzer, and FortiSIEM for a single view of security on-premises and in the cloud

Protect Against Malware and Malicious Links

Productivity tools such as Microsoft 365 touch a tremendous amount of sensitive corporate information and data. Utilizing artificial intelligence (AI) and advanced machine learning (ML), FortiSandbox provides advanced protection against known and unknown malicious threats and URLs. Without interruption from successful cyberattacks, employee productivity is safeguarded. FortiSandbox integrates with the Fortinet Security Fabric to address the rapidly evolving and more targeted threats including ransomware, crypto-malware, and zero-day threats.

Specifically, it delivers real-time actionable intelligence through the automation of zero-day advanced malware detection and response. FortiSandbox delivers:

- Effective defense against advanced targeted attacks through a cohesive and extensible architecture
- Detection of both known and unknown threats
- Results of inspections in minutes
- Protection of network-based traffic and email zero-touch breach protection via integration with Fortinet and non-Fortinet solutions

Deploy Strong Identity and Access Management

It does not always require the use of malware to give cyber criminals unauthorized access to Microsoft 365, nor employee error for sensitive data to leave it. Credential theft remains a primary objective for threat actors today because it provides bad actors the ability to access the environment under the guise of a legitimate user. In fact, of the breaches caused by social actions, 62% resulted in the theft of credentials while the top malware of choice for threat actors are password dumpers.

Fortinet offers FortiToken and FortiAuthenticator identity and access management (IAM) products to mitigate these issues. These are commonly used in conjunction with Active Directory (AD) services of Microsoft 365 that enable single sign-on and federation. Fortinet IAM solutions take security to the next level with:

- MFA by hard or soft tokens
- Integration with secure directories like AD
- Push notifications for one-tap approval on mobile devices
- Self-erase, brute-force protection
- Central authentication service access to on-premises and cloud-based resources

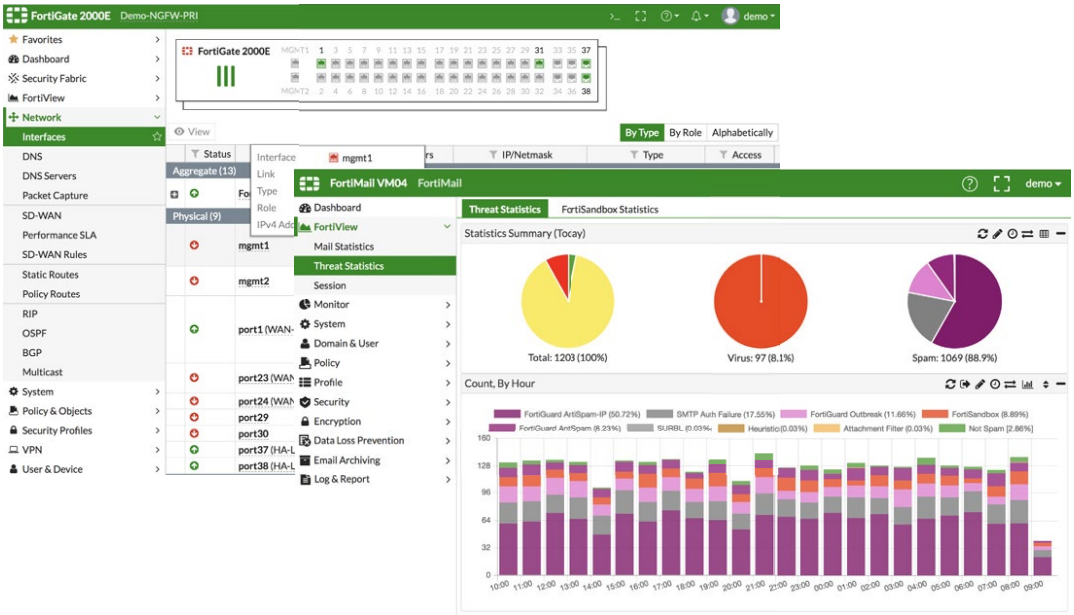

Figure 1: Fortinet offers a common user interface across security components for Microsoft 365.

Fortinet Is the Ideal Partner for Microsoft 365 Security

The security industry offers quite a few choices, especially for products like email security, IAM, and cloud access security broker (CASB).

There are three primary areas that set Fortinet apart:

1. Only Fortinet delivers a consistent set of security controls across on-premises networks, email, and major cloud services. These include anti-malware and sandbox services to identify traditional and advanced threats, data loss prevention capabilities to secure sensitive information, and MFA.
2. Our traditional and advanced threat protection capabilities have earned the most independent certifications and top ratings in the industry. Validated by Virus Bulletin, ICSA Labs, SE Labs, AV-Comparatives, and more, Fortinet solutions provide the most rigorously tested security available, natively and via open API across security infrastructures.
3. With a consistent user interface and administrative experience across all components, Fortinet reduces the time spent deploying, configuring, monitoring, and managing security for Microsoft 365.

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

[2] "2020 Data Breach Investigations Report," Verizon, June 2020.

[3] Ibid.

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

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

FORTINET®

www.fortinet.com

Copyright © 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

February 12, 2021 2:55 AM

759500-A-0-EN

sb-FA-securing-M365-with-fortinet-security-fabric-942020