EXECUTIVE SUMMARY

The Fortinet Security Fabric provides broad, integrated, and automated protection across the organization—on-premises, across multiple clouds, and out to users and devices. For those using Microsoft Office 365, key Security Fabric elements include a cloud access security broker (CASB) to extend on-network data security policies and enforcement to the cloud, consistently top-rated email security to protect cloud-based email, and multi-factor authentication to prevent unauthorized access to your cloud-based productivity suite and storage. Further, with a common user experience across security components, organizations are able to manage this added security with less effort.

The Fortinet Security Fabric offers unprecedented visibility and protection from on-premises infrastructure, to IoT devices, to multiple clouds. Its integrated detection of advanced threats, automated response, and continuous trust assessment consistently receives top ratings from third-party reviewers. Built on the foundation of the flagship FortiGate Next-Generation Firewall (NGFW), traditionally deployed on-premises, it is critical for today’s digital business to extend the insight and security of the Fortinet Security Fabric into cloud services like Microsoft Office 365.

LEVERAGE CASB FOR INTEGRATED PROTECTION

Providing such comprehensive protection for cloud solutions is a challenge, with Software-as-a-Service (SaaS) vendors like Microsoft controlling not just the infrastructure but also the application layer. Fortunately, it is now common practice for major cloud providers to provide API-based access to their offerings to CASBs for just that purpose. This allows Fortinet FortiCASB to complement the in-built visibility of the Office 365 Admin Center, with additional options to assess and report on users, behaviors, and data stored in clouds like Office 365. More importantly, it also enables advanced FortiCASB functions to extend security policies and intelligence currently in use in other parts of the network—on-premises and across multiple clouds.

Specifically, Office 365 customers using OneDrive 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

FORTICASB INTEGRATES WITH OFFICE 365 AND EXTENDS SECURITY INTO SaaS CLOUDS.

- 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

Add Extra Protection for Exchange Online

Email is the delivery vehicle for 92.4% of all malware, and 49% of successfully installed malware. Hence, ensuring that your organization’s email in Exchange Online is free of phishing, ransomware, business email compromise, and other threats is critical. At the same time, email can just as easily be used to improperly expose sensitive data. That’s where FortiMail Cloud complements FortiCASB and the basic capabilities of Exchange Online Protection with:

- Top-rated FortiGuard Labs security services including antispam, antivirus, sandboxing, content disarm and reconstruction, click protection, impersonation analysis, and more
- Consistent data loss prevention technologies also available in FortiGate and FortiCASB
- Robust, yet easy to use, identity-based email encryption technologies
- Integration with FortiGate, FortiAnalyzer, and FortiSIEM for a single view of security
- Open APIs for intelligence sharing across the Fortinet Security Fabric about multistage attacks that begin with an email
ENSURE STRONG IDENTITY AND ACCESS MANAGEMENT

Of course, it does not take malware for cyber criminals to enter Office 365, nor employee error for sensitive data to leave it. According to Verizon, the top cyber-criminal technique resulting in breaches is the use of stolen credentials. That’s why Fortinet offers FortiToken (and optionally FortiAuthenticator) Identity and Access Management (IAM) products.

Commonly used in conjunction with the Active Directory (AD) services of Office 365 that enable single sign-on, federation, and more, Fortinet IAM solutions take security to the next level:

- Multi-factor authentication by hard or soft tokens, including email, SMS, and mobile 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

FORTITOKEN HELPS PROTECT SENSITIVE DATA ON AND OFF NETWORK, ACROSS CLOUDS OF ALL TYPES.

WHY FORTINET?

There are plenty of third-party vendors to choose from, especially across multiple components like CASB, Email Security, and Identity and Access Management. There are three primary things that set Fortinet apart from the rest:

1. Only Fortinet delivers a consistent set of security controls across your on-premises network, email, and major cloud services. These include antimalware and sandbox services to identify traditional and advanced threats, data loss prevention capabilities to secure sensitive information, and multi-factor authentication.

2. Those traditional and advanced threat protection capabilities have earned the most independent certifications and top ratings in the industry. Validated by Virus Bulletin, ICSA Labs, AV-Comparatives, NSS Labs, and more, Fortinet solutions provide the most rigorously tested security available, natively and via open API across your security infrastructure.

3. With a consistent user interface and administrative experience across all components, Fortinet reduces the time spent deploying, configuring, monitoring, and managing security for Office 365.

Copyright © 2018 Fortinet, Inc. All rights reserved. FortiGate®, FortiCare®, 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.