THE FORTINET SECURITY FABRIC FOR AZURE PROVIDES COMPREHENSIVE PROTECTION FOR MICROSOFT OFFICE 365

EXECUTIVE SUMMARY

Organizations that rely heavily on email for their business operation and see email as a key means of communication throughout the organization are aware of the possibility that email will spread malware and other threats throughout the Internet, as well as the risk the email threat vector imposes to organizations. Office 365 is a very popular email solution employed by organizations and offers a variety of email security functionality for deeper security. The Fortinet Security Fabric for Azure 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 should include a cloud access security broker (CASB) to extend on-network data security policies and enforcement to the cloud, a dedicated email security gateway to protect cloud-based email, and cloud-based sandboxing to prevent zero-day threats. Further, with a common user experience across security components, organizations are able to manage this added security with less effort.

The Fortinet Security Fabric, now available on the Microsoft Azure cloud, offers unprecedented visibility and protection from attacks targeting Office 365 email. Its detection of advanced threats by FortiSandbox, high-speed inspection of email traffic by using FortiMail, and its ability to control Office 365 at the API level using FortiCASB offer unrivaled protection for Office 365 mail systems. Built on the foundation of the flagship FortiGate Next-Generation Firewall (NGFW), which is also available to protect Azure cloud-based systems deployment, it is critical for today’s digital businesses to extend the insight and security of the Fortinet Security Fabric into cloud services like Microsoft Azure and Office 365.

LEVERAGE CASB FOR INTEGRATED PROTECTION

Office 365 provides API-based access to their SaaS application to enable CASBs to interact and support the management of security on SaaS applications. This allows FortiCASB to complement the built-in 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.

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 running over Azure 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

PROTECT FROM ZERO-DAY THREATS

Complement your established FortiMail and FortiGate defenses with the FortiSandbox two-step malware analysis approach. Suspicious and at-risk files are subjected to the first stage of analysis with Fortinet’s award-winning AV engine, FortiGuard global intelligence query*, and code emulation. Second stage analysis is
SOLUTION BRIEF: THE FORTINET SECURITY FABRIC FOR AZURE PROVIDES COMPREHENSIVE PROTECTION FOR MICROSOFT OFFICE 365

Value-Added Fortinet Components

<table>
<thead>
<tr>
<th>Feature</th>
<th>Free Microsoft Component (E3 license)</th>
<th>Value-Added Fortinet Components</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visibility, Control, and Protection</td>
<td>Office 365 Information Rights Management</td>
<td>Fortigate, FortiMail, FortiCASB</td>
</tr>
<tr>
<td>Protect Against Threats</td>
<td>Exchange Online Protection</td>
<td>Fortigate, FortiMail, FortiCASB with FortiSandbox</td>
</tr>
<tr>
<td>Secure Content</td>
<td>Office 365 Admin Center</td>
<td>FortiCASB</td>
</tr>
</tbody>
</table>

WHY FORTINET?

There are plenty of third-party vendors to choose from, especially across multiple components like CASB, email security, and advanced threat detection. 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 anti-malware 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. 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.**

**September 13, 2018 8:52 AM**