FORTINET

SOLUTION BRIEF

Fortinet Secure Productivity for Office 365

Executive Summary

As organizations increasingly transition to using cloud-based applications for productivity and email (e.g., Microsoft Office 365, Google G Suite), their visibility and control over these applications is inherently reduced. The Fortinet Security Fabric enables transparency that protects mail messages from zero-day threats as well as monitoring of the Office 365 API layer. The Security Fabric elements involved here include FortiMail, which natively integrates with Office 365 via a new API connector to provide advanced email security. FortiSandbox-Cloud supports discovery of previously unknown threats via cloud-based email traffic. FortiCASB-SaaS cloud access security broker (CASB) extends on-network data security policies and enforcement to the cloud.

As enterprises increasingly move to the use of Software-as-a-Service (SaaS) offerings in the public cloud for core business productivity functions, security becomes an important question. This includes identity and access management, protection of content against threats, as well as transparency across various public cloud environments. The Fortinet Security Fabric offers unprecedented visibility and protection from on-premises infrastructure to public clouds. Built on the foundation of the FortiGate next-generation firewall (NGFW), the Fortinet Security Fabric offers native API integration and several key solutions that enforce secure productivity when using multi-application SaaS suites like Microsoft Office 365.

Fortinet Secure Productivity Solution Capabilities Include:

- Native integration with Office 365
- Simplified deployment
- Easier procurement from the cloud

The top cyber-criminal action leading to breaches last year was the use of stolen credentials.[1]

Email is the delivery vehicle for 92.4% of all malware, and 49% of successfully installed malware.[2]

Malware is the most expensive attack type for organizations—and the average cost of an attack rose by 11% over the last year.[3]

FortiMail—Integrated Email Security

FortiMail-Cloud inspects incoming and outgoing email to stop threats and prevent data loss. It provides comprehensive coverage, including antispam, antiphishing, anti-malware, data loss prevention (DLP), encryption, and message archiving.

As part of the Fortinet Secure Productivity solution, FortiMail-VM seamlessly integrates with Office 365 through a custom-built API connector. This helps to simplify security operations by eliminating the need for IT staff to manually modify network settings such as DNS and high availability. The solution can be procured from the existing customer cloud accounts (e.g., Office 365 or Azure Cloud) without hassle. It increases security ease of use and advanced threat protection while reducing the burden on limited IT/security resources. Over half of organizations report a problematic shortage of cybersecurity skills—as evidenced by nearly 3 million currently unfilled cybersecurity jobs (a 61% increase from last year).[4]

FortiSandbox—Proactive Advanced Threat Detection

Since both FortiCASB-SaaS and FortiMail leverage the FortiSandbox-Cloud service, it becomes an inherent part of the overall secure productivity solution. Up to 40% of new malware detected is now zero day or previously unknown.[5] And it only takes one threat to slip past security for a data breach to occur. This concern is driving organizations to integrate advanced sandboxing with greater controls and a high degree of automation. As part of the Fortinet Secure Productivity solution, FortiSandbox-Cloud analyzes attached files and URLs for previously unknown threats. It provides multilevel inspection, including static analysis, emulation, and full virtual execution, with granular risk ratings and automatic intelligence updates.

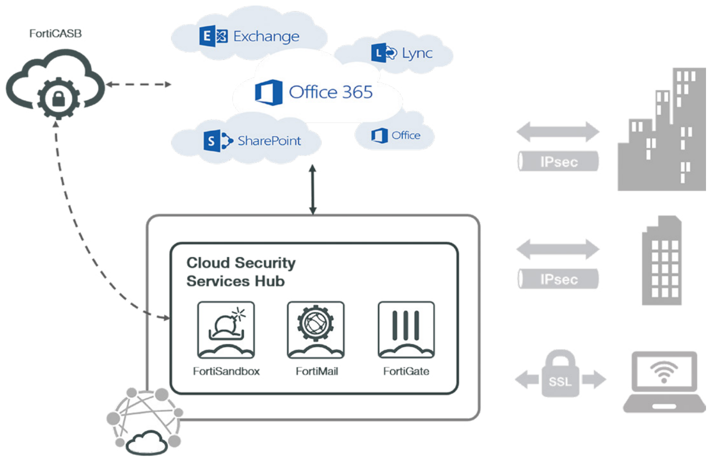

Figure 1: Fortinet Secure Productivity solution.

FortiCASB-SaaS—Integrated SaaS Protection

Providing comprehensive protection for cloud solutions is a particular challenge because SaaS vendors like Microsoft control 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 CASB solutions for just that purpose. In this way, FortiCASB-SaaS complements the built-in visibility of the Office 365 Admin Center with additional options to assess and report on users, behaviors, and data stored in the Office 365 suite of SaaS applications. More importantly, FortiCASB-SaaS also enables advanced functions to integrate security policies and intelligence from other parts of the network.

Add Extra Protection for Exchange Online

It is critical to ensure that an organization's email in Exchange Online is free of phishing, ransomware, business email compromise, and other threats. At the same time, email can just as easily be used to improperly expose sensitive data. This is where FortiMail-VM complements FortiCASB-SaaS 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 DLP technologies also available in FortiGate and FortiCASB-SaaS
- Robust, yet easy to use, identity-based email encryption technologies
- Open APIs for intelligence sharing across the Fortinet Security Fabric about multivector attacks that begin with an email

Why Fortinet for Secure Productivity?

There are plenty of third-party vendors to choose from, especially across multiple components like CASB, email security, and sandboxing. There are three primary things that set Fortinet apart from the competition in these areas:

1. Only Fortinet delivers a consistent set of security controls across on-premises networks, SaaS platforms, and major public cloud services. These include anti-malware and sandboxing services to identify traditional and advanced threats, and DLP capabilities to secure sensitive information.
2. Fortinet 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 an organization's security infrastructure.[6]
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.

[1] "2018 Data Breach Investigations Report," Verizon, April 10, 2018.

[2] Ibid.

[3] Kelly Bissell, et al., "Ninth Annual Cost of Cybercrime Study," Accenture and Ponemon, March 6, 2019.

[4] "Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens," (ISC)², October 2018.

[5] According to internal data from FortiGuard Labs.

[6] "Certifications," Fortinet, accessed March 20, 2019.

FORTINET

www.fortinet.com

April 25, 2019 5:25 AM

377102-A-0-EN

F:\Fortinet\PDF Files\Fortinet - SB 042419\FA\FA-sb-secure-productivity-for-public-cloud