SOLUTION BRIEF

Securing Microsoft 365 with Fortinet Security Fabric

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 365, key Security Fabric elements include email security with FortiMail, FortiCASB to monitor Microsoft 365 usage, data, and configurations, as well as tools for multi-factor authentication, zero-trust network access, and endpoint security. The Fortinet Secure SD-WAN solution delivers a fast and secure connection to Microsoft 365 and other cloud-based applications while adhering to Microsoft 365 networking principles and guidelines.

The Fortinet Security Fabric offers unprecedented visibility and protection for your infrastructure, both on-prem, and in the cloud as well securing users and devices.. 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).

Add Extra Protection for Exchange Online

Email is the delivery vehicle for 92.4% of all malware, and 49% of successfully installed malware.[1] Beyond malware, email can lead users to phishing sites, expose them to scams, and can be used to extract sensitive information from your network. Microsoft offers security packages for M365 such as Exchange Online Protection and Advanced Threat Protection. But even when fully implemented and properly configured, Microsoft's security solutions accurately detect less than 30% of malicious emails. To protect your users, customers, and your business, it is critical to deploy email security tools. FortiMail and FortiCASB enhance Microsoft 365's native security 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 application programming interfaces (APIs) for intelligence sharing across the Fortinet Security Fabric about multistage attacks that begin with an email

Lead with FortiMail for Integrated Protection

Providing 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 applications for just that purpose. This allows Fortinet FortiCASB to complement the in-built 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 and 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

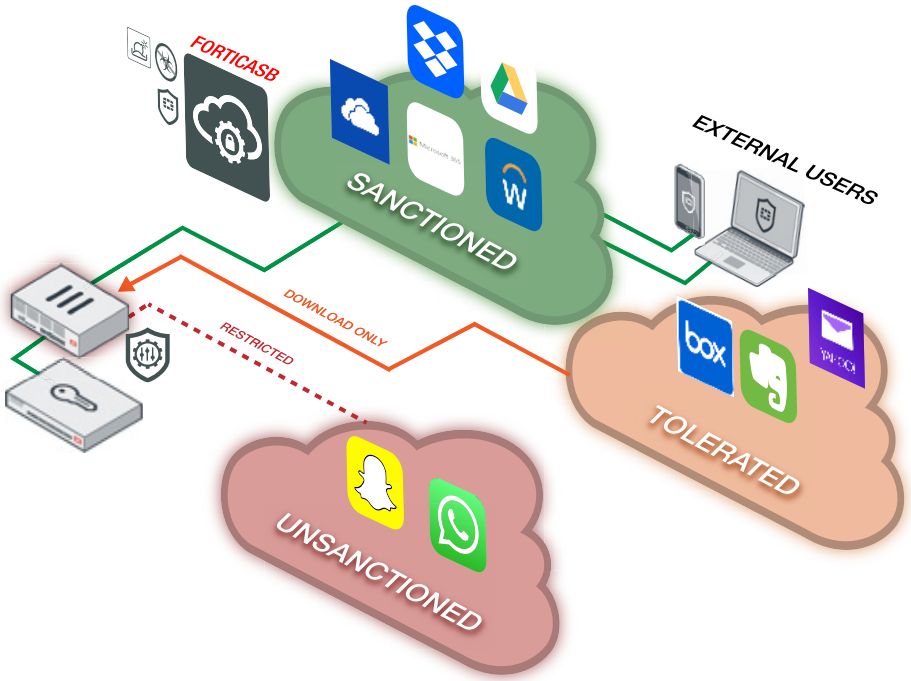


Figure 1: FortiCASB integrates with Microsoft 365 and extends security and SaaS clouds.

Ensure Strong Identity and Access Management

Of course, it does not take malware for cyber criminals to enter Microsoft 365, nor employee error for sensitive data to leave it. As of 2020, top cyber criminal techniques resulting in breaches still include 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 Microsoft 365 that enable single sign-on, federation, vand 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

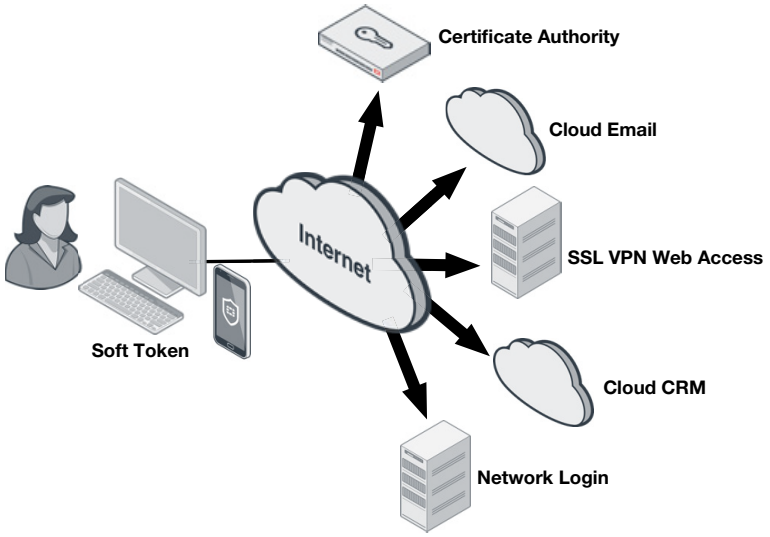
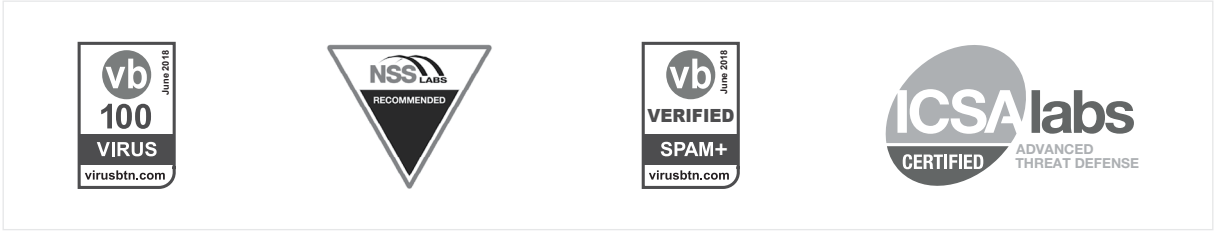


Figure 2: FortiToken helps protective sensitive data on and off network across clouds of all types.

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 Microsoft 365.

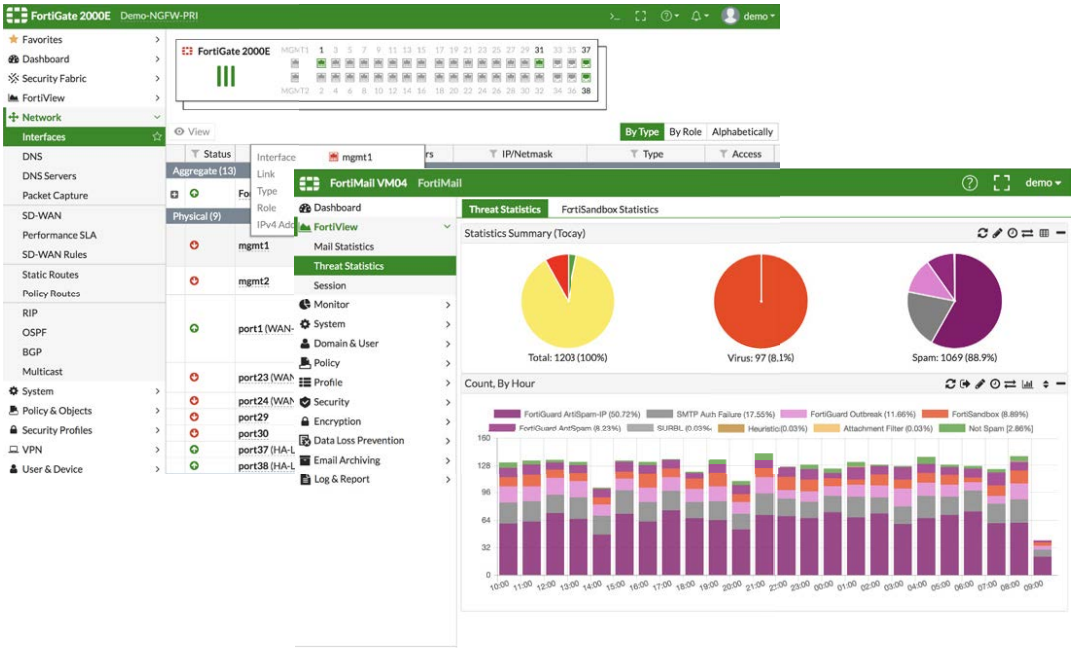


Figure 3: Fortinet offers a common user interface across security components for microsoft 365.

[1] "2020 Data Breach Investigations Report," Verizon, June 2020.

September 4, 2020 12:11 AM

759500-0-0-EN

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