GUIDE TO SECURING MICROSOFT OFFICE 365 FOR THE ENTERPRISE

A Platform Approach to SaaS Security

Over the past several years, Microsoft® Office 365® – the cloud-based version of Microsoft's collaboration suite – has emerged as the company's cloud juggernaut, with 120 million commercial users at last count. Not content to stop there, the software giant's stated goal is to move two-thirds of its current Office business customers to the cloud by mid-2019.[1]

The potential downside of the ubiquity of the Office suite – and the skyrocketing adoption of Office 365, in particular – is that it's now a highly valuable target for cybercriminals. This makes securing your enterprise's use of Office 365 more critical than ever. Although Microsoft's security tools and capabilities are a great place to start, many enterprises moving to Office 365 are finding they need more control and even greater visibility and protection across all their cloud applications.

[1] "Microsoft Office 365 now has 120 million business users," Mary Jo Foley, ZDNet, October 26, 2017.

Thinking Beyond the Security Built Into Office 365

What fuels the collaboration, productivity, communications and creativity companies gain from using Office 365? Data – your corporate data, to be exact – which will be created, shared and stored in the cloud within Office 365 applications, such as OneDrive® and SharePoint®. In fact, some reports indicate as much as half of all corporate data is already stored in the cloud.

To secure Office 365 applications, Microsoft provides built-in policies, controls and systems. These capabilities are designed to support the security responsibilities for providers of SaaS as defined by the industry-standard shared security model, including physical security, host infrastructure, network controls and application-level controls. In that same model, businesses are responsible for data classification and accountability. Both the SaaS provider – in this case, Microsoft – and your company share responsibilities for identity and access management as well as client and endpoint protection.

For its part, Microsoft offers native Office 365 security controls, including:

- Management of user identities, credentials and access rights.
- Data compliance, including archiving, e-discovery and auditing.
- Rights management through Microsoft Azure® to protect Office documents.
- Malware detection for automatic protection against spam and malware.

To meet your company's shared security responsibilities as well as simplify and enhance security for the Office 365 applications and data your company relies on, a third-party product may be the best choice. Many enterprises choose third-party products to serve security use cases that require:

- Protection for other cloud applications beyond Office 365, enabling the same level of security for all the enterprise's sanctioned applications, such as Box, Salesforce®, Slack®, ServiceNow®, Google® G Suite™, JIVE® and others.
- Granular application control and inline visibility across all user and data activity in the cloud.
- Sophisticated data loss prevention, or DLP, capabilities that give enterprises visibility and control over sensitive data in cloud applications to prevent accidental and malicious data loss.
- Advanced threat protection across network, cloud and endpoints to block known and unknown malware.
- Greater protection against zero-day malware with discovery and prevention of highly evasive, unknown exploits and malware.

> *"Through 2020, at least 99% of cloud security failures will be the customer's fault."*
>
> – Source: Gartner, "Magic Quadrant for Cloud Access Security Brokers," November 30, 2017

Turning to a Cloud Access Security Broker

It would be extremely challenging for organizations to attempt to solve all requirements for securing Office 365 with their existing security tools, particularly those already deployed to secure on-premise environments.

Instead, an increasing number of companies are deploying a cloud access security broker, or CASB, which delivers visibility and control over the usage of cloud applications as well as compliance and protection for cloud-based data. Unlike other security tools your enterprise may use, CASBs offer cloud-specific capabilities that address security gaps in your organization's use of cloud services.

It's important to know that CASBs can be deployed in two different modes, depending upon your organization's requirements:

- **Inline approach**. With an inline approach, a CASB can use either forward or reverse proxy. With forward proxy, the CASB forwards cloud traffic to an appliance or service that can provide application visibility and control capabilities. Forward-proxy capabilities are not limited to traditional proxies, such as secure web gateways. Powerful next-generation application control capabilities can be enforced using a next-generation firewall appliance or services. Companies that already have an NGFW deployed as an internet gateway for on-premise or remote users can avoid the additional management overhead and complexity of using a traditional proxy offered by most CASB vendors. For a reverse proxy, a CASB can use single sign-on, or sometimes DNS, to reroute users to an inline CASB service to enforce policies.
- **API-based approach.** Quickly becoming the preferred method of implementing a CASB, the API-based approach provides visibility into all the company's data within the cloud application or service while complementing security services "in between" the cloud traffic. This out-of-band approach supports granular inspection of all data at rest in the cloud application as well as ongoing monitoring of user activity and administrative configurations. This deployment mode preserves the user experience for the cloud application because it's non-intrusive and does not interfere with or depend on the data path to the cloud application. In addition to applying policies for any future violations, an API-based CASB is the only way to inspect existing data stored in the cloud as well as remediate any DLP violations and threats.

> *"By 2020, 60% of large enterprises will use a CASB to govern cloud services, up from less than 10% today."*
>
> – Source: Gartner, "Magic Quadrant for Cloud Access Security Brokers," November 30, 2017

For enterprises with more advanced security needs and use cases, a third-party CASB can complement native security controls from Microsoft.

Taking a Platform Approach to Securing Office 365

To protect SaaS application usage, including Office 365, Palo Alto Networks® takes a platform approach. The Palo Alto Networks Security Operating Platform is a suite of products and services that prevents successful cyberattacks by harnessing analytics to automate routine tasks and enforcement. It delivers the industry's most advanced security and compliance capabilities across multi-cloud environments to prevent data loss and business disruption.

Palo Alto Networks offers both inline and API-based protection technologies that work together to minimize the wide range of cloud risks that can cause breaches. Focused on the broad ecosystem of cloud applications, Palo Alto Networks supports Microsoft cloud offerings as well as many other popular cloud applications and services.

With the Security Operating Platform, you can secure your Office 365 environment and other SaaS applications using:

- **An inline approach** with Palo Alto Networks next-generation firewalls on-premise to secure inline traffic with deep visibility, segmentation, secure access and threat prevention, and GlobalProtect™ cloud service to extend protection to remote users. This approach combines user, content and application inspection features within the next-generation firewall to enable CASB functions. The inspection technology maps users to applications to deliver granular control over cloud application usage regardless of location or device. Other features include application-specific function control, URL and content filtering, policies based on application risk, DLP, user-based policies, and prevention of known and unknown malware. GlobalProtect cloud service extends the protection of the Security Operating Platform to your mobile workforce to prevent the exfiltration of sensitive data across all applications.
- **An API approach** with Aperture™ SaaS security service to connect directly to SaaS applications for data classification, DLP and threat detection. Aperture delivers complete visibility and granular enforcement across all user, folder and file activity within sanctioned SaaS applications, providing detailed analysis and analytics on usage without requiring any hardware, software or network changes. It allows granular, context-aware policy control within SaaS applications to drive enforcement and quarantine users and data should a violation occur.

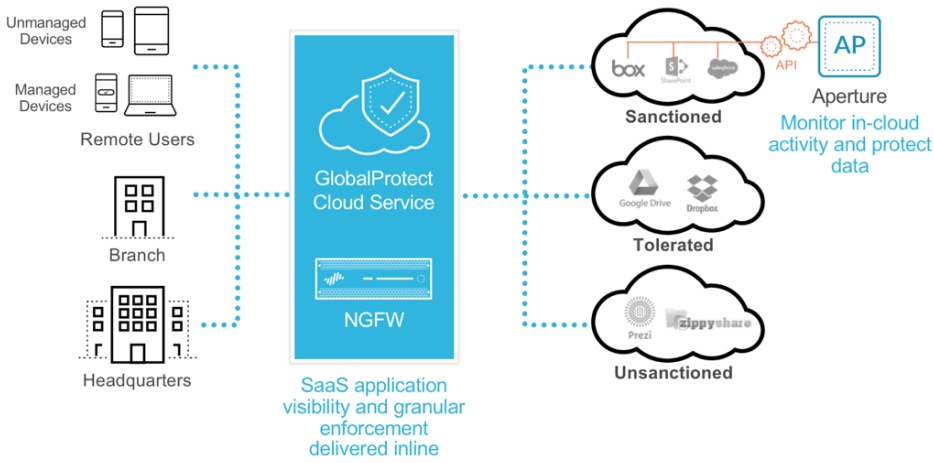

Figure 1: A platform approach to securing Office 365

Meeting the Top Three Requirements for Securing Office 365

A platform approach to securing Office 365 and other cloud applications gives you the visibility, data protection, threat protection and control you need to protect your company as well as your data in the cloud. Palo Alto Networks delivers all three of the top requirements for securing Office 365 and other cloud applications.

Requirement 1: Gain Visibility Into Cloud Application Usage, Including Office

Leverage App-ID for cloud application visibility: Palo Alto Networks next-generation firewalls are built from the ground up to provide unparalleled visibility and granular control of all applications, including details on application usage across the network. Cloud applications constitute one of many categories supported through an extensive library of App-IDs that provides instant classification and fine-grained policy controls. Palo Alto Networks and Microsoft collaborate to enable App-ID™ technology to provide superior identification of Office 365 application usage, including the ability to detect usage and the direction of transfer – that is, upload versus download – even in encrypted flows. By decrypting and inspecting files within those flows, Palo Alto Networks can analyze threats through WildFire® cloud-based threat analysis service and immediately share new threat intelligence with all customers.

Palo Alto Networks WildFire *stops known and unknown threats from spreading through sanctioned SaaS applications, preventing a new insertion point for malware.*

Generate detailed cloud application reports: With regular reporting of cloud application usage, you gain continuous understanding of your organization's exposure and the ability to keep policies up to date with the latest applications being used within your organization. With PAN-OS®, you can mark individual applications as either sanctioned or unsanctioned for better visibility and reporting as well as generate a detailed cloud application report on demand. Paired with User-ID™ technology, it provides details of who is using which applications and in what quantity. With this deep visibility, you can define cloud application usage policies for employees, customers and business partners as well as determine policies and migrations needed to move end users to sanctioned applications.

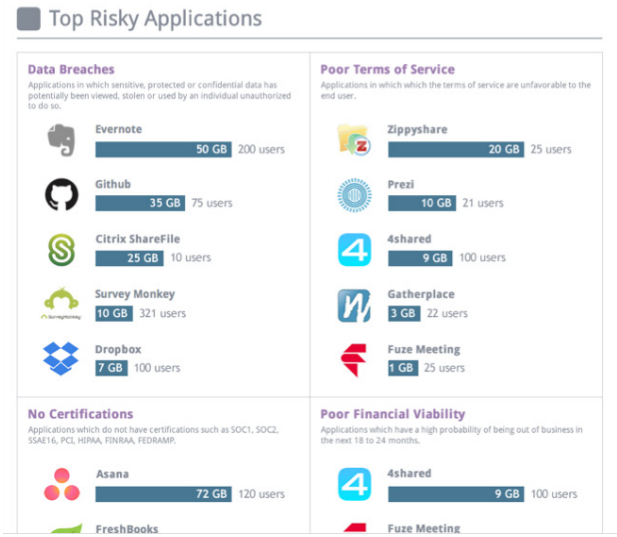

Figure 2: Example of a SaaS Application Usage Report

Get real-time visibility with interactive dashboards: Dashboards provide real-time visibility of sanctioned and unsanctioned cloud application usage, users and content based on User-ID, App-ID and ContentID™ technology.

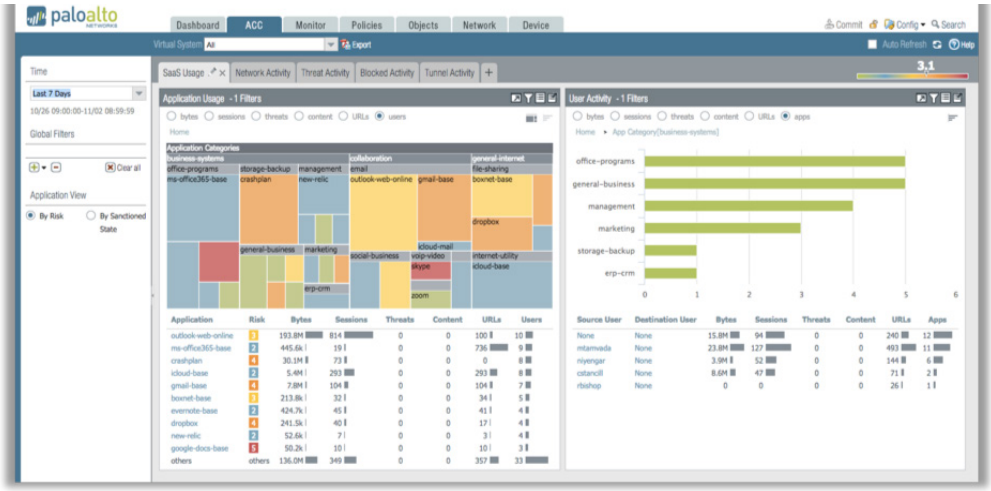

Figure 3: A dashboard showing application usage and user activity

Requirement 2: Use the Next-Generation Firewall to Control Usage and Migrate Users

Block unsanctioned applications: Block unsanctioned applications, such as those often infected with malware, hosted in dangerous geographic regions with poor security and governance controls, or with limited or no end-user license agreements or service-level agreements.

Exercise granular control of tolerated applications: For the many applications that fall somewhere between enterprise-sanctioned and unsanctioned, use a more granular and measured approach to control their usage. For example, tolerated applications may be those that third-party vendors, such as marketing contractors or legal firms, use to share documents with your company.

Migrate users from tolerated to enterprise-sanctioned applications: Standardizing on an enterprise-sanctioned application, such as Office 365, creates an opportunity to move users from tolerated applications to sanctioned ones to improve security, visibility and governance. You can implement a policy to allow only downloading of data from the tolerated application with no upload rights so users can migrate their data to Office 365 over a period of time. Once the data has been migrated, you can move tolerated applications to unsanctioned, allowing you to block them.

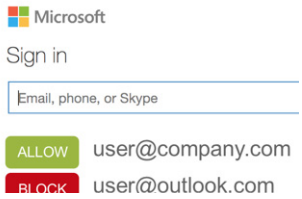

Figure 4: Example of blocking unsanctioned applications after migration to Office 365

Requirement 3: Improve Protection for Office 365

Secure Office 365 against data loss: Cloud applications are becoming the first insertion points for malware and the last exfiltration points for data loss. Using Aperture, you can connect via API directly to Office 365 and other cloud applications to provide data classification, including machine learning of data, sharing and permission visibility, activity analysis and alerts, and threat detection. This yields unparalleled visibility, enabling organizations to inspect content for data-risk violations and control access to shared data via contextual policy controls.

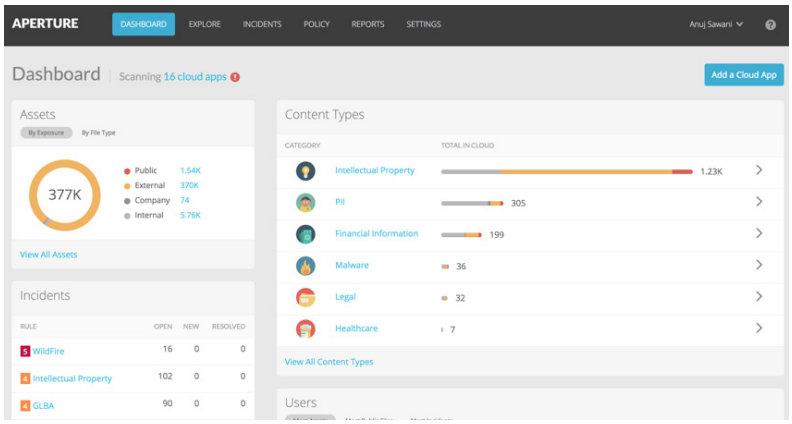

Figure 5: Data classification results in Aperture

Protect against malware: Integration of WildFire with Aperture as an API-based CASB uniquely provides advanced threat prevention to block known malware as well as identify and block unknown malware. This prevents threats from spreading through sanctioned applications and prevents an insertion point for malware. When Aperture discovers new malware, it shares intelligence with the rest of the Security Operating Platform and across customers. WildFire integration with Aperture keeps threats from infiltrating Office 365 applications and prevents end users in any location from being infected.

Securing Your Environment

The Palo Alto Networks Security Operating Platform helps secure your Microsoft environment from the network to the cloud to the endpoint. Employing some of the most comprehensive Microsoft security capabilities in the industry, the Security Operating Platform supports the physical security of Microsoft operating systems and applications through App-ID; private cloud security with the VM-Series for Hyper-V®; public cloud threat prevention in Azure; Office 365 security with CASB functions via inline next-generation firewalls and via API using Aperture SaaS security service; and finally, Microsoft endpoints with GlobalProtect network security and Traps™ advanced endpoint protection.

To learn more about securing Microsoft Office 365 and other SaaS applications, visit http://go.paloaltonetworks.com/office365.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

guide-to-securing-microsoft-office-365-for-the-enterprise-wp-060518