SAFELY ENABLE OFFICE 365

Securing Office 365 Is Easier Than You Think

SaaS applications continue to provide a tremendous value to end users with easy setup and collaboration capabilities that are changing the way organizations do business. The concern over the loss of data leaving the corporate network and opening the network to external threats through unknown collaborators has caused many organizations to take a "wait and see" approach to SaaS. Microsoft® Office 365™ changes all that. Now SaaS services come with the application that many consider the most indispensable tool in business today: Microsoft Office. This pushes SaaS security to the forefront of most organizations and means it can no longer be ignored.

Overview

The demand for businesses to be more agile to meet organizations' demands and stay competitive is driving a change in the way applications are developed, deployed and adopted. Applications, workloads, and the data that go with them are becoming more distributed among varying environments, such as physical networks, private clouds, public clouds (hybrid or dedicated), and Software as a Service (SaaS) applications. Each environment brings its own unique agility benefits and security issues. The challenge has become balancing the agility needs of the business with improving the security of the applications and, more importantly, the data as it moves between the various clouds. Gaining visibility and preventing attacks that are attempting to gain access to the data, both from an external location and through a lateral attack, becomes imperative across all of the locations where the applications and data reside, without adding additional complexity or cost.

This is especially true as applications move beyond the organization's control to SaaS applications where there is traditionally no visibility or control. This adds a new risk of sensitive data exposure and, even more concerning, a new vector for threat insertion that is invisible to traditional in-line security services. Applications like Office 365 highlight this risk, where the applications on the device use encrypted connections to the SaaS service, making visibility into the files being exchanged challenging.

Impacts of Office 365

The pervasiveness of shadow IT is a result of the tremendous value these SaaS applications are providing to end users. Risks of data exposure and threat insertion mean these users can't run unchecked.

This has never been more true than with Office 365. While other SaaS applications can be considered optional and more easily prevented, Office is often a mandatory application. Now that it comes with cloud applications automatically, it has the potential to enable SaaS usage by every employee, regardless of the organization's size. This puts a spotlight on the existing challenge of securing SaaS applications that can no longer be ignored.

File Sharing in Office 365

Beyond being a single application, Office 365 is actually a collection of applications that have many different interactions. The chief concern is applications that are capable of file storage and sharing. This is because file sharing applications are the most vulnerable to data exposure and malware insertion.

Since most Office 365 applications, such as Word and Excel, do not hold files themselves, rather they use file sharing applications for storage, securing the file sharing services secures the applications that use them. With that in mind, there are three key applications we need to focus on securing:

- SharePoint® – A collaboration tool for creating internal team websites and sharing content.
- OneDrive® – A file storage and file sharing application that enables users to sync files and later access them from any device.
- Yammer® – Enterprise social networking service used for private communication and file sharing within organizations.

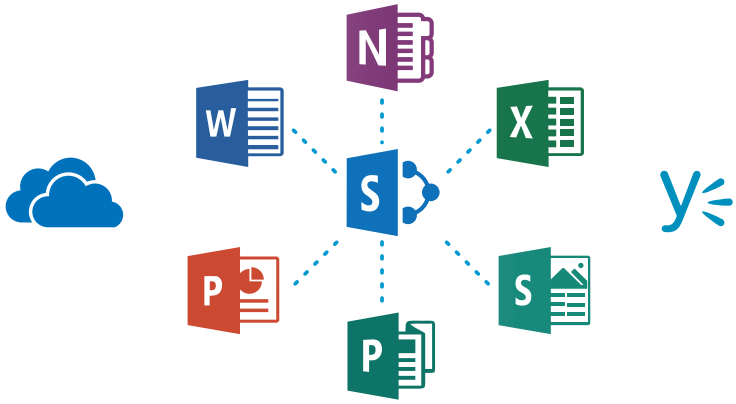

Figure 1: File storage and sharing Applications within Office 365

Note: We have focused on file sharing and storage in this paper because this generally unseen area of vulnerability is often left without proper protections. Email in Office 365 is a slightly different story, however.

Office 365 Provided Security

SaaS vendors, such as Microsoft, realize the concern of moving sensitive data to an environment that is no longer under IT control. Because of the security concerns with moving data to the cloud, many SaaS vendors have focused on ensuring the security of the organization's infrastructure and data. Microsoft, especially, has invested considerable time and resources to ensure Office 365 is secure.

The Microsoft Office 365 Security and Compliance white paper published in January 2016 (https://www.microsoft.com/en-us/download/details.aspx?id=26552) states the ways it accomplishes this, including:

- Port scanning and remediation
- Perimeter vulnerability scanning
- Operating system security patching
- Network-level distributed denial-of-service (DDoS) detection and prevention
- Multifactor authentication for service access
- Auditing all operator/administrator access and actions
- Zero standing permission for administrators in the service
- Just-in-time access and elevation that is granted on an as-needed and only-at-the-time-of-need basis to troubleshoot the service
- Segregation of the employee email environment from the production access environment
- Mandatory background checks for high-privilege access. These checks are a highly scrutinized, manual approval process.

Encryption

To ensure that data cannot be viewed or tampered with, Office 365 also provides data encryption, both at rest and in motion.

Data in Motion

Like most enterprise-grade SaaS applications, Microsoft uses encryption to secure the communication between the SaaS application in the cloud and the clients used by the end user. This introduces a new security challenge as it makes it difficult for security practices designed to look for incoming and outgoing threats to see the files within the encrypted flows. This has the potential to allow threats to spread throughout an organization through an unseen SaaS application.

Data at Rest

Microsoft encrypts the data you store in Office 365 automatically to protect it from unauthorized theft. This is a common practice by enterprise-grade SaaS vendors to ensure the data is safe. Decryption happens automatically through user credentials when the account is accessed.

Breach Prevention

This ultimately leads to the main goal and responsibility for the SaaS vendor, which is to prevent breaches of their infrastructure. Microsoft describes a four-pillar approach to preventing breaches in its Office 365 Security and Compliance white paper:

- **Prevent Breach** – This pillar includes port scanning and remediation, perimeter vulnerability scanning, operating system patches, network-level isolation/breach boundaries, DDoS detection and prevention, just-in-time access, live site penetration testing, and multifactor authentication for service access.
- **Detect Breach** – System and security alerts are harvested and correlated via a massive internal analysis system. The signals analyze alerts that are internal to the system as well as external signals (for example, those coming from organizations' incidents). Based on machine learning, we can quickly incorporate new patterns to trigger alerts, and automatically trigger alerts on anomalies in the system.
- **Respond to Breach** – This pillar is used to mitigate the effects if a component is compromised. A diligent incident response process, standard operating procedures in case of an incident, the ability to deny or stop access to sensitive data, and identification tools to promptly identify involved parties help to ensure that the mitigation is successful.
- **Recover from Breach** – This includes the standard operating procedures to return the service to operations. The pillar covers the ability to change the security principles in the environment, automatically update the affected systems, and audit the state of the deployment to identify any anomalies.

Shared Responsibility

Where Office 365 Security Ends and IT Security begins

Preventing infrastructure breaches is an important goal, and Microsoft is putting significant investment in this area to ensure that Office 365 is a safe place to store your data. Infrastructure breaches are only one part of the issue, and IT must fill the gaps that are not provided by SaaS vendors, such as Office 365. This is where their responsibility ends and the IT team's responsibility begins.

The main security gaps not addressed by SaaS vendors are to:

- Prevent data exposure through improper sharing
- Prevent threat insertion/distribution

Microsoft leaves these responsibilities with the IT team, requiring something else to control their use and prevent a new insertion point for malware. Once legitimate access is granted, new threats emerge.

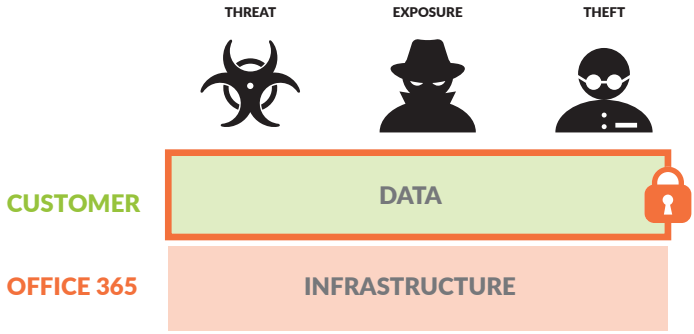

Figure 2: Shared security model

Note: Microsoft provides threat protection for email through a service called Exchange Online Protection (EOP). It is focused on email messages and their attachments destined for the exchange server and does not cover file sharing services, such as OneDrive and Yammer, where the unseen risks exist.

Taking Steps to Securely Enable Office 365

Start by Securing the Cloud

Sharing of data is one of the natural benefits of using SaaS applications. Often the data is not only shared internally but with external collaborators. This means that users outside the organization can now share files with your users through applications, like OneDrive, without the typical checks you would have through email. Even more concerning is that these applications can often use encryption to tunnel through traditional security methods, meaning that malware can enter your network without the existing checks you have put in place. This means that all data within the cloud itself must be cleared of potential threats, at the source, preventing end users from being compromised no matter their location.

The second major concern that needs to be addressed is data loss through intentional or unintentional data being shared externally. Once the data moves into the Office 365 cloud, it is no longer under the organization's control, and visibility is often lost.

To safely enable Office 365 use, IT security must have the tools to manage and secure these risks effectively. Such tools should provide the following:

- Complete visibility across all user, folder and file activity within SaaS applications.
- Detailed analysis and analytics on usage to prevent data risk and compliance violations.
- Granular context-aware policy control to drive enforcement and quarantine of users and data as soon as a violation occurs.
- Real-time threat intelligence on known and unknown threats to prevent new SaaS-based insertion points for malware "in the wild."

These capabilities can only be effectively delivered in a cloud-based platform with the ability to connect to Office 365 directly no matter where the user is located.

Gain Visibility into SaaS Usage

Traditionally organizations have not been able get detailed, SaaS-specific visibility into which applications are being used and by which users. This has been a critical gap for organizations to understand not only their level of exposure but also which applications are being used for business-critical needs.

Detailed reporting of how users are currently using applications is a critical step. To properly control SaaS application usage and limit the impact of shadow IT, you need to have detailed visibility of the applications that are being used, how they are being used, and which users are using them.

Look Deeper to Discover Threats

Because encryption is so commonly used by SaaS applications, preventing threats is especially difficult as the data passes between your network and the SaaS cloud. To ensure threats aren't being exchanged, it's important to be able to decrypt the flows to discover the threat of the payload. This has traditionally been a significant challenge as these applications rely on encryption for secure communication.

Control Access to SaaS Applications

With the visibility from detailed reporting, you have the ability to define granular policy control around critical business usage of SaaS, allowing you to block risky and unnecessary applications while controlling access and usage of those that are business critical.

For example, you may want to limit an application to a particular group, only allowing them to download but not upload data to prevent exposure of sensitive data in unsanctioned applications. It comes down to limiting access to prevent data exposure risk and threat insertion while not disrupting business.

To safely enable applications and protect their data, organizations must be able to accurately identify, categorize and control the applications, including SaaS and web-based applications in use on their network.

The challenge for organizations today is not only the growing diversity of the applications but also the inability to define simple policies to block or allow applications. Sanctioned, enterprise applications are clearly understood because they are provided by IT, and applications that must be blocked can often be easy to define as well. The challenge is that the majority of applications will fall somewhere in between.

- **Enterprise-sanctioned:** Applications that the organization has approved for use and are provided by IT. These apps typically are delivered through a corporate SSO.
- **Unsanctioned:** Applications, including unknown applications that are blocked by the organization, that are not approved for use. These are often considered a risk or simply redundant.
- **Unsanctioned but tolerated:** Applications that are unapproved by IT but not blocked. Their access is strictly controlled by user group or function to reduce exposure or as a means to migrate users away from the application. These applications might be allowed only until the users are migrated to a sanctioned application, for example, since simply cutting off access to them would cause users to lose access to their data and prevent them from migrating it to a sanctioned application.

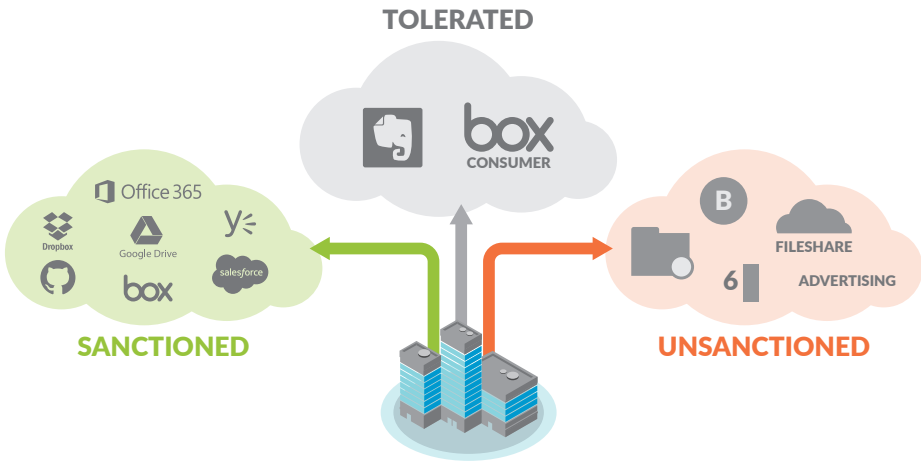

Figure 3: Classifying SaaS applications

Migrate Users to Office 365

A sledgehammer approach of simply blocking applications is not the right approach. Disrupting business-critical applications while blocking risky applications will have significant business impact since users often require these applications to do their daily jobs.

If, as part of your deployment, you want to standardize on Office 365 for file sharing, for example, you need to be able to allow users to migrate their data from the existing applications that are unsanctioned. Simply blocking access will trap the data in the application, preventing users from accessing it or removing it. Instead define a policy that whitelists sanctioned applications, such as Office 365, and allows download-only rights to other applications. This provides an educational opportunity for users, enabling them to remove their data from these applications and migrate it to Office 365. Once a predefined time period, you can change the policy to block access to these applications completing the Office 365 migration.

Move Migrated Applications from Tolerated to Unsanctioned

There are a number of applications that users may have been using that are dangerous or redundant to the newly available Office 365 applications. If these applications are no longer being used for legitimate business needs, or you have migrated users off of them, it's time to block access to them. The way they are blocked is dependent on how restrictive of a policy you want to set. You can either:

- **Whitelist** – Define a policy that only allows specific applications to be accessed. Exceptions can be defined for download-only access, or access from specific groups, but application blocks are implied without express permission.
- **Blacklist** – This is the opposite of whitelisting in that it only blocks specific applications but allows all others. This can be a useful way to regulate application access based on a specific report of user activity, thereby controlling how users access specific risky applications without an overly restrictive policy.

Multi-SaaS Security

Even if vendors, such as Microsoft, provided a full suite of security for Office 365, it is very likely that Office 365 is the only SaaS application supported in your network, long term. Having unified visibility and control across all SaaS applications becomes very important. It's critical to ensure data exposure and threats are not only stopped but that you can also track violations at a user and file level across multiple SaaS applications. Without that unified view, the increasing number of SaaS applications that become sanctioned by IT will make managing them impossible.

How Palo Alto Networks Safely Enables Office 365

Palo Alto Networks® Next-Generation Firewalls were built from the ground up to offer unparalleled visibility and control of all applications, providing details on application usage across the network. Office 365 is one of the many applications that are supported today through an extensive library of App-ID™ instances that provide instant classification and fine-grained controls.

Step 1 – Secure Office 365 from Malware Insertion and Data Loss

SaaS applications are becoming the first insertion point for malware and the last exfiltration point for data loss. Because of this critical point in the infrastructure, the first step should be to secure the cloud applications themselves.

To solve this Palo Alto Networks developed Aperture, a cloud-residing SaaS security service that extends the Next-Generation Security Platform to SaaS applications. Aperture adds the ability to connect directly to SaaS applications, such as Office 365, to provide data classification, sharing/permission visibility, and threat detection within the application. This yields unparalleled visibility, enabling organizations to inspect content for data risk violations and control access to shared data via a contextual policy.

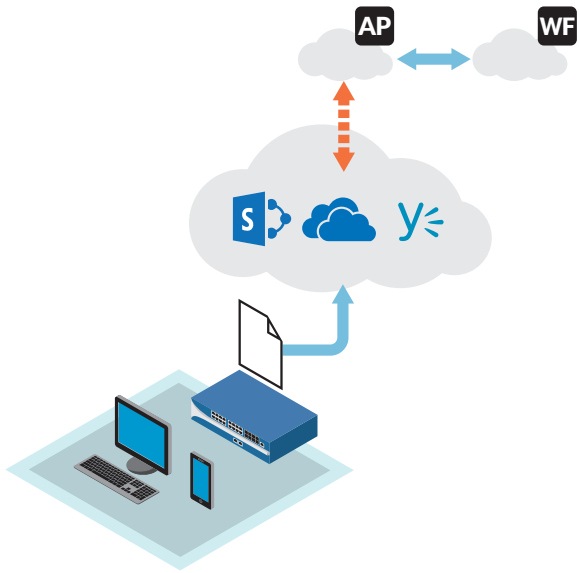

Figure 4: Aperture and WildFire Office 365 Security

Integration of WildFire™ cloud-based malware analysis with Aperture provides advanced threat prevention to block known malware and identify and block unknown malware. This extends WildFire's existing integration to prevent threats from spreading through the sanctioned SaaS applications, preventing a new insertion point for malware. New malware discovered by Aperture is shared with the rest of the next-gen security platform, even if it is not in-line with the SaaS applications. WildFire integration keeps threats out of the Office 365 cloud to prevent end users from being infected no matter their location.

Step 2 – Gain Visibility into SaaS Usage Through Detailed SaaS Reporting

Leverage App-ID for SaaS Visibility

Properly controlling SaaS is impossible without proper visibility of which applications are used in the network and how they are being used. This requires application-level visibility of usage at a granular level.

Palo Alto Networks next-generation firewalls was built from the ground up to provide unparalleled visibility and control of all applications, including details on application usage across the network. SaaS is one of the many application categories that is supported today through an extensive library of App-IDs that provide instant classification and fine-grained controls.

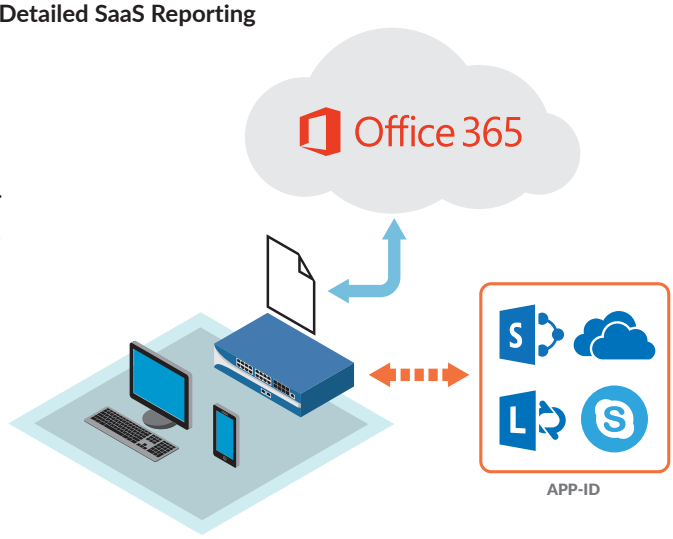

Figure 5: App-ID Office 365 visibility

Palo Alto Networks and Microsoft collaborated to ensure that App-ID provides superior identification of Office 365 application usage. This includes the ability to detect application usage and the direction of transfer (upload versus download) even in encrypted flows. Even more importantly it enables the ability to decrypt Office 365 flows to inspect the files within those flows, allowing detailed analysis of threats through WildFire.

Generate Detailed SaaS Reports in PAN-OS

SaaS visibility and reporting shouldn't be a one-time or infrequent event. Regular reporting of SaaS usage enables a continuous understanding of exposure and the ability to keep policies up to date with the latest SaaS applications that are being used within your organization.

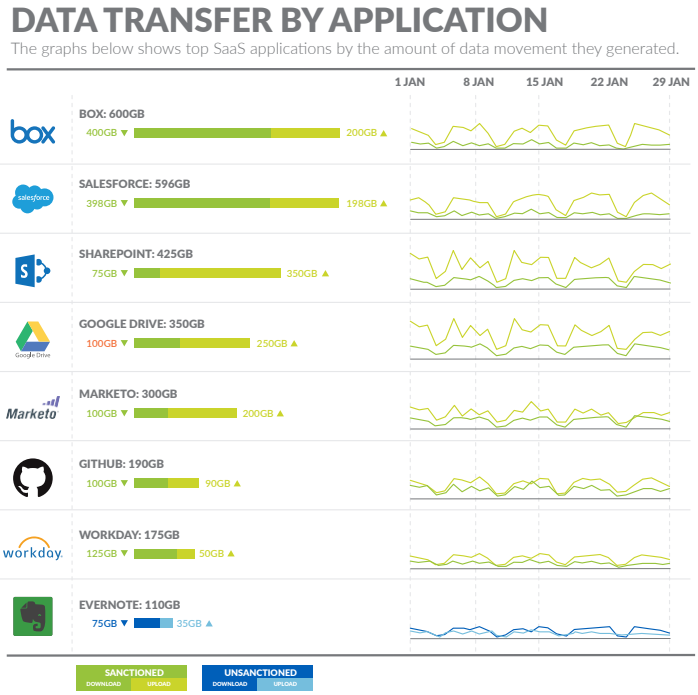

Figure 6: PAN-OS SaaS report

PAN-OS® includes the ability to mark individual SaaS applications as either sanctioned or unsanctioned for better visibility and reporting. This foundation enables a detailed SaaS report that can be generated from PAN-OS or Panorama as needed and, when paired with User-ID™, can provide details of who is using which application and in what quantity. This allows continuous reporting of SaaS usage to become a regular part of IT's security analysis. Even more importantly it provides the key visibility needed to define a SaaS usage policy for employees and a means to determine policies and SaaS migrations that are needed to move end users to sanctioned SaaS applications. It serves as the foundation to a secure Office 365 usage model, and it is included as part of PAN-OS without additional subscriptions or licensing.

Step 3 – Use the Next-Generation Firewall to Control Usage and Migrate Users

Blocking Unsanctioned Applications

Enterprise-sanctioned applications, such as Office 365, are typically allowed without restrictions. Unsanctioned applications, such as SaaS apps often known to be infected with malware, hosted in dangerous geographic regions with poor security and governance controls, or with bad end-user license agreements (EULAs) and service-level agreements (SLAs) are usually blocked outright. Policies to control these applications' usage are straightforward.

Granular Control of Tolerated Applications

It is likely that there are more applications that fall somewhere between enterprise-sanctioned and unsanctioned applications, however. These tolerated applications represent a unique challenge and require a more granular and measured policy to control their usage.

These tolerated applications fall into three main categories:

- **External Partners:** Applications that external partners use that users need access to for sharing and collaboration. These applications are often controlled by a third party or partner who is sharing data with your internal users. Since there is no way to ensure the safety of data in the third party's SaaS application, or the safety of files entering your organization, a few steps need to be taken to ensure its use is safe.
- **Non-Enterprise Applications:** Applications that internal users rely on that are not "enterprise" applications and cannot be made sanctioned.

These tolerated applications require a granular policy to ensure their safe usage without disrupting business. Since these applications do not allow visibility or control in the cloud, their usage should be restricted to ensure the network is secure.

- **Prevent data loss:** Set the next-generation firewall policy to allow only the downloading of files preventing data from leaving your network without visibility or control. File uploads should be restricted to enterprise-sanctioned applications that are secured with Aperture. Exceptions can be set based on users or groups via User-ID-based policies.
- **Prevent malware insertion:** Block encrypted connections that could deliver malware into the network invisibly, possibly bypassing existing security.

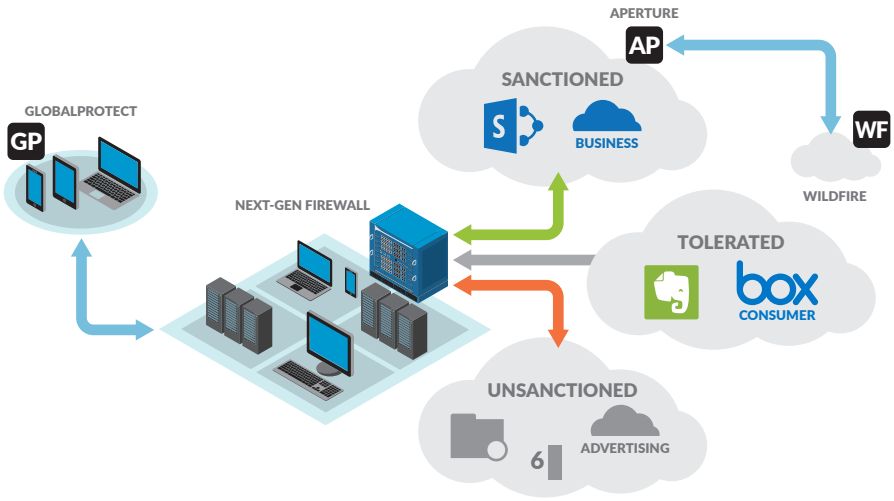

Figure 7: Complete SaaS security

Migrating Users from Tolerated to Enterprise-Sanctioned Applications

Standardizing on an enterprise-sanctioned application, such as Office 365, opens up the opportunity to move users off of tolerated applications, increasing security while providing more capabilities to end users.

Simply cutting off access to these applications often isn't a valid option since corporate data likely already resides in them. Cutting off access only traps the data in the tolerated SaaS applications. Instead a policy should be set to allow only the downloading of data with no upload rights. Have the users move their data to the Office 365 over a period of time. Once the data has been migrated, the application can be moved from tolerated to unsanctioned and blocked.

Part of a Larger Microsoft Security Platform

Office 365 is just the latest Microsoft application secured by Palo Alto Networks, but we have been securing Microsoft deployments for years. We have one of the most comprehensive Microsoft security capabilities in the industry with support for 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™, and Microsoft endpoints with GlobalProtect™ mobile security and Traps™ advanced endpoint protection.

Secure Office 365 deployment is the latest addition to the Microsoft protection capabilities of the Palo Alto Networks Next-Generation Security Platform. App-ID provides the ability to identify Office 365 applications and how they are being used, even if they are encrypted, as well as the ability to decrypt Office 365 flows to inspect even deeper within the files being exchanged to look for threats. Aperture adds the ability to protect data from exposure and threats in the Office 365 cloud itself, stopping them at the source before they have a chance to move to the network or mobile devices.

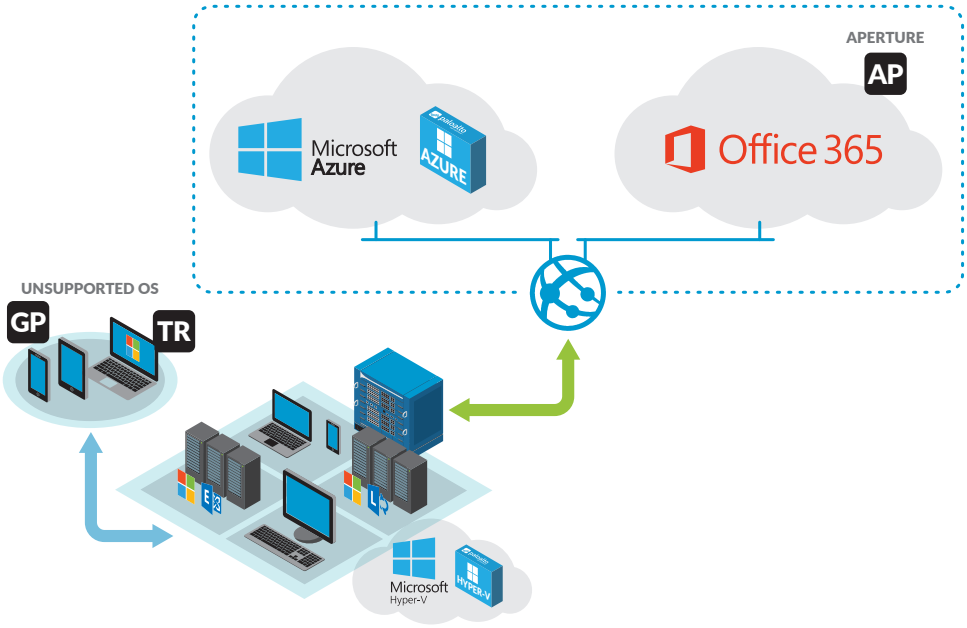

Figure 8: Next-Generation Security Platform Microsoft Security

4401 Great America Parkway
Santa Clara, CA 95054

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

www.paloaltonetworks.com

pan-office365-wp-040516