PRISMA

WHEN PROXIES AREN'T ENOUGH

# Three Pillars of Security in Office 365 Deployments

# TABLE OF CONTENTS

INTRODUCTION

# The Importance of Connectivity and Security for Office 365

If your organization is like most, you have migrated or are planning to migrate to Microsoft Office 365. You're in good company: Office 365 now supports more than 180 million commercial users, gaining more than 4 million new users each month.[1]

This rapid adoption is creating a paradigm shift in the way organizations think about security. In the cloud, data no longer sits in one place. The cloud enables users to use, edit, and share data easily. How do you control access and protect data when neither the application nor the user is on your network?

Office 365
**now supports more than**
180 million commercial users,
**gaining more than**
4 million new users
**each month.**

When it comes to Office 365 deployment, some providers specialize in just one aspect, such as connectivity. While connectivity is important, you must also make sure your deployment is secure. You need to be able to protect your users and data from threats just as much as you need to provide a seamless, productive user experience.

This e-book will help you navigate the requirements for properly deploying Office 365 as well as provide guidance on how to choose a solution that delivers both the connectivity and security you need.

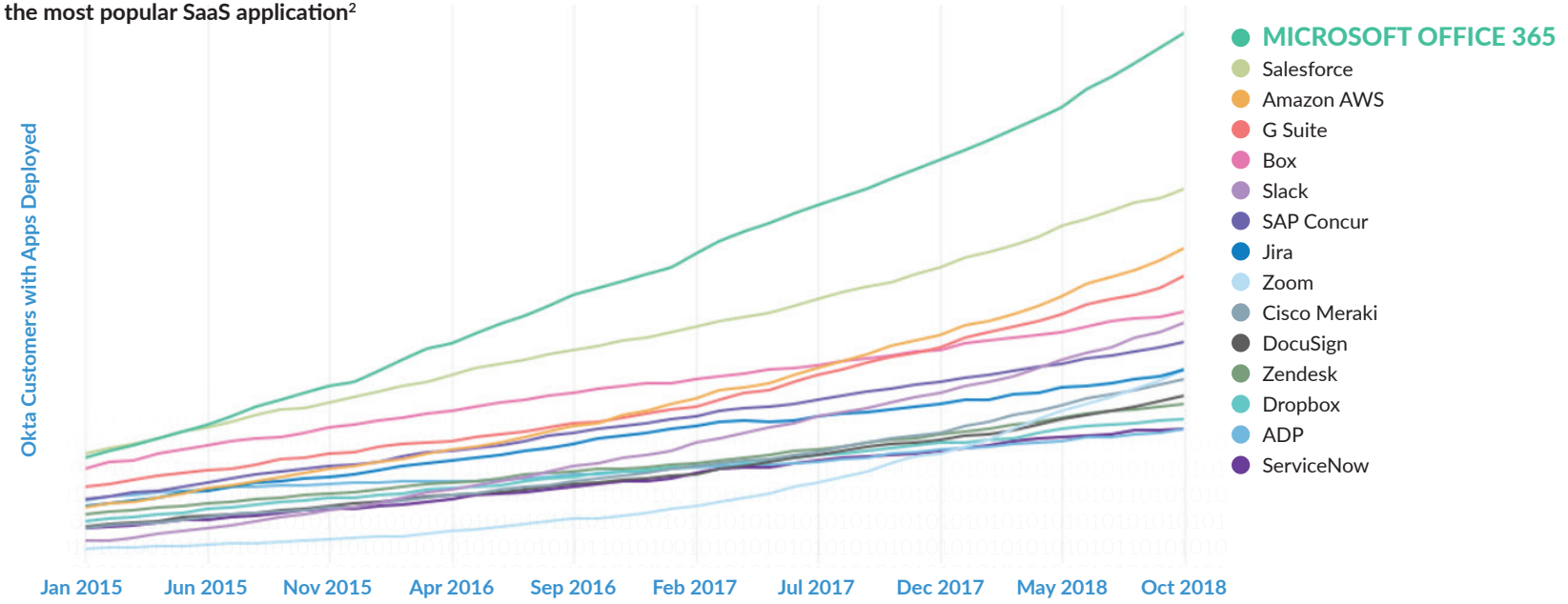
1. Tony Redmond, "Office 365 Reaches 180 Million Monthly Active Users," Office365ITPros.com, April 25, 2019.

# A Look at Office 365 Adoption

Because organizations are moving their workloads to the cloud, Office 365 adoption is growing rapidly. Today, it is the most widely used cloud service in terms of monthly average users.

## Most Popular Apps (Number of Customers)

**FIGURE 1**
**Office 365 is the most popular SaaS application[2]**




This comes as no surprise when you look at the applications within Office 365 and the functionality they offer:

- Word processing: Microsoft Word
- Spreadsheets: Excel
- Email: Exchange Online
- File sharing: SharePoint
- Messaging: Yammer
- Online conferencing: Skype
- File storage: OneDrive

According to Palo Alto Networks research,[3] Office 365 also uses a lot of bandwidth, accounting for 59% of the data transferred in enterprise applications. With the large amount of data in Office 365, it can be a lucrative target for cybercriminals. While Microsoft does its share to protect users, analyzing more than 6.5 trillion signals every day to identify emerging threats,[4] enterprises must seek out additional security to ensure they fully understand which users have access to their data.

2. "Businesses @ Work 2019," Okta, last accessed September 11, 2019.
3. "The Current State of SaaS: Usage and Risk Perspective," Palo Alto Networks, June 28, 2019.
4. "Microsoft by the Numbers," Microsoft, last accessed September 11, 2019.

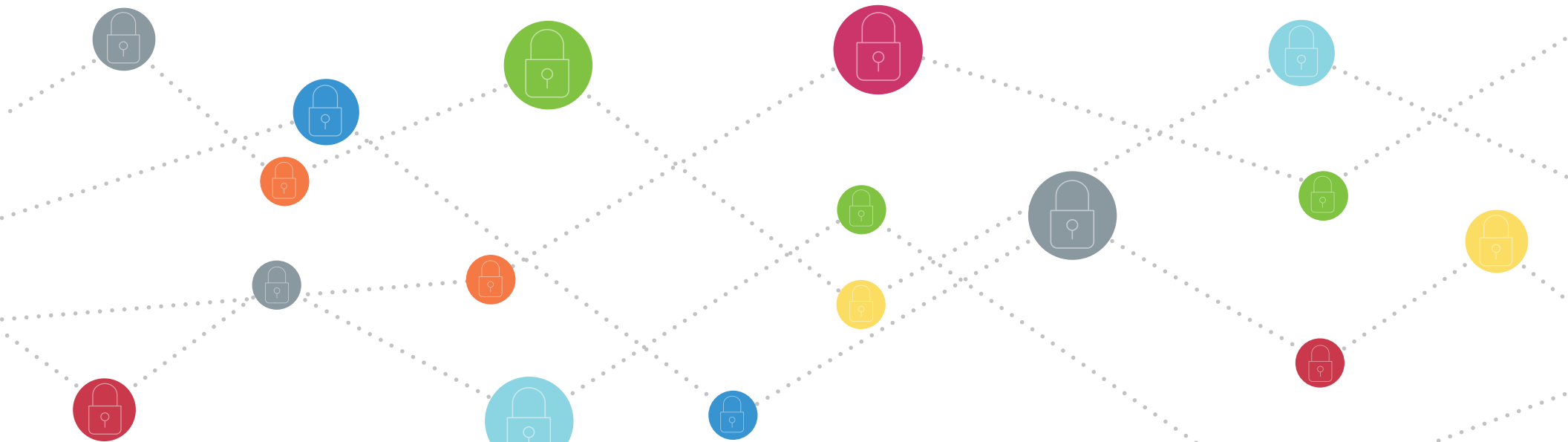
# Connectivity Is Important, but It Is Not Enough

Connectivity plays a crucial role in the Office 365 user experience. You need to have fast access to applications no matter where you are in the world.

However, Office 365 solutions that focus on connectivity typically don't provide the needed level of security. Products based on proxies are often not able to rewrite all of the connections to Office 365 applications. In fact, this is why the recommended proxy configuration disables inspections normally present for other applications.

Proxies are also notoriously difficult to interoperate. When an organization implements a cloud access security broker (CASB) proxy for SaaS applications and a secure web gateway for internet access, problems arise around how the proxies are supposed to interact with one another.

The net is that security is not always available when using Office 365 with a proxy, regardless of whether it's top of mind for the organization.



# Security is the Foundation of a Successful Office 365 Deployment


FIGURE 2
**Most common Office 365 security risks**

To properly protect your organization and its assets, you must be able to inspect user access and behavior, data, and potential threats in order to answer these questions:

- Who has access to your Office 365 instance?
- Which applications are they using?
- What type of content is in Office 365?
- How is it being used?
- Is content being shared properly?
- What's being downloaded or stored?

Adequately addressing those questions minimizes the chances of a data breach. Your customers should be confident your organization is making the right security decisions in order to protect their private information. It is extraordinarily difficult to regain consumer confidence once that trust is lost—and if you don't, the cost is high.

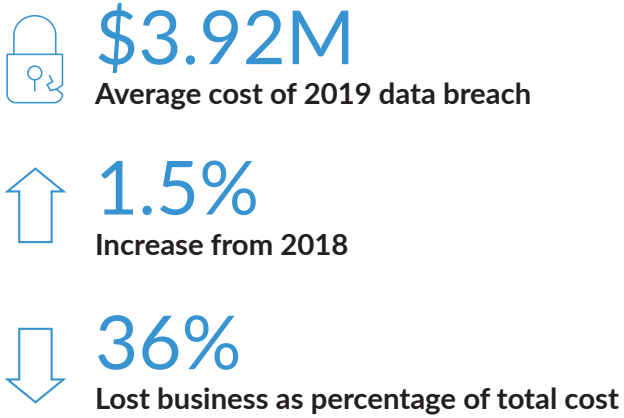



FIGURE 3
**2019 Cost of a Data Breach, Ponemon Institute**

The bottom line is that uncontrolled SaaS usage, exposure of sensitive data, and propagation of malware can all lead to negative brand reputation. Let's look at what can be done about it. >>>

# Key Security Requirements for Office 365

As you migrate to Office 365 or seek to secure your current deployment, look for solutions that offer connectivity and comprehensive security, ones that gives you visibility into users, applications, and threats across all SaaS applications.

**Visibility and Access Control**
To understand and control who is accessing apps and data.

**Data Loss Protection**
To secure content in motion and at rest.

**Threat Prevention**
To prevent bad actors from stealing or corrupting data.

FIGURE 4
**Key capabilities for Office 365 security**

Such a solution should extend cloud-native security controls to:

- Offer data protection for your other SaaS apps.
- Give you in-line visibility and granular app control.
- Deliver sophisticated data leak prevention capabilities.
- Protect against threats across network, cloud, and endpoints.
- Defend against zero-day malware.

**THE BOTTOM LINE:** You need no-compromise protection against cyberattacks, with consistent enforcement of policy at every location. The solutions should deliver comprehensive, automated protection that stops known and unknown malware, exploits, credential theft, command and control, and many other attack vectors across all ports and protocols.

Let's take a closer look at the specific capabilities you should consider. > > >

# SECURITY REQUIREMENT #1
# Control Access

Just because Office 365 is internet accessible that doesn't mean everyone on the internet should have access to your particular deployment. Allowing attempts to authenticate to your Office 365 environment creates a large attack surface and raises the risk of access using stolen credentials. Instead, you can reduce the risk of unauthorized activity by controlling access to your specific Office 365 instance using a gateway only your users access.

The implementation of such a gateway also establishes a way to enforce other types of granular protections, including the ability to enforce controls based on the use of managed or unmanaged devices as well as compensating controls that allow access to extended users with unmanaged devices, such as contractors.

Office 365 has both consumer and enterprise account types, but what does that mean for your company? Which are authorized and which are unauthorized? Who has access to which apps? For example, your users log in to their personal accounts from work to access and share their documents. Doing so creates risk, such as data loss or even the unintentional download of an infected document.

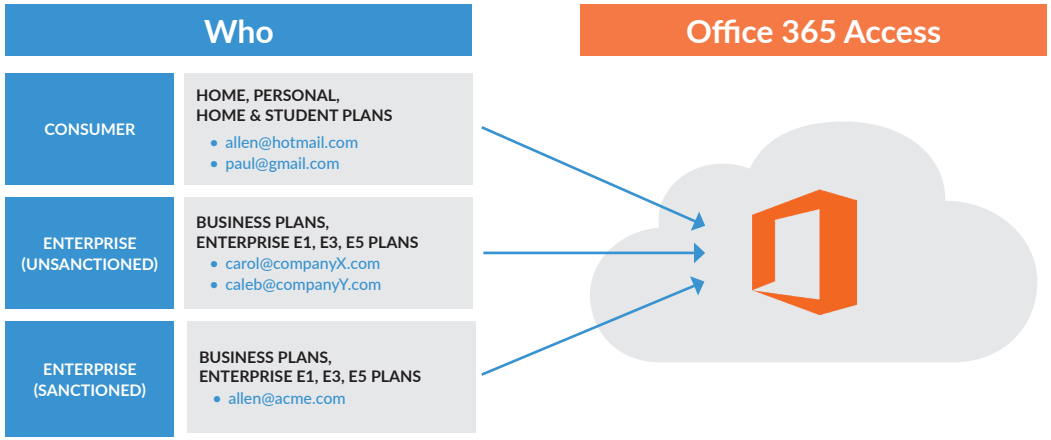



FIGURE 5
**Multiple users + one Office 365 policy = limited visibility or control**

Unrestricted access to Office 365 is risky. By controlling access, you'll be able to better protect sensitive data stored within these apps. For example, you could:

- Block access to consumer Office 365 accounts.
- Allow access to your own enterprise account but block access to other enterprise and consumer accounts.
- Allow access to sanctioned enterprise accounts and block all other unsanctioned enterprise and consumer accounts.
- Lock down access to shared files and folders.

## When evaluating solutions, ensure they do the following:

- ✓ Identify Office 365 traffic and enforce security policies.
- ✓ Control access to Office 365.
- ✓ Use multi-factor authentication (MFA) for additional identity assurance.
- ✓ Stop in-process credential phishing by blocking users from sending corporate credentials to unknown sites.
- ✓ Prevent credential leakage.
- ✓ Offer user activity visibility with Office 365.
- ✓ Identify non-enterprise accounts, such as personal OneDrive accounts.
- ✓ Mitigate the risk of inappropriate sharing and public links.

# SECURITY REQUIREMENT #2
# Protect Data

The private data that fuels enterprise can easily be shared or stored within Office 365. For example, files can be shared inadvertently to a public folder or intentionally copied onto a personal OneDrive account. Without a comprehensive approach to securing Office 365, you won't know if these files contain the types of sensitive data shown in Figure 6.

**FIGURE 6**
**Types of sensitive data**

| CONFIDENTIAL DATA | PAYMENT INFORMATION | PERSONALLY IDENTIFIABLE INFORMATION | REGULATED DATA |
|---|---|---|---|
| Company financial records, intellectual property, source code | Credit card numbers, bank account information, debit card numbers | Social Security numbers, phone numbers, street addresses, dates of birth, tax IDs | Health information, for example, including diagnoses, prescriptions and medical records |

Protecting data requires visibility into applications and users to determine which applications are being used by whom and how—and defining policies for behavior such as downloading, uploading, sharing, and accessing from personal accounts. Without visibility, protecting data, users, and apps becomes a nearly impossible task, severely impacting the security posture of the organization.

Even when data is properly stored within Office 365, the organization must maintain controls to ensure the data isn't inadvertently or maliciously moved to the wrong places. That's where data loss prevention (DLP) controls can help. For example, DLP controls provide the means to discover, classify, monitor, and protect data as well as authenticate users and control who has access to which applications and data, and when. DLP clearly defines and enforces role-based data access and usage policies while ensuring that data is being stored, accessed, and used in a way that complies with data protection regulations and data privacy laws.

## When evaluating solutions, ensure they do the following:

Offer in-line enforcement of policies to control access to sanctioned applications, provide security, and block access to unsanctioned applications.

Maintain bidirectional control over the unauthorized transfer of files, intellectual property, Social Security and credit card numbers, and custom data patterns.

Provide granular control of Office 365 based on the application user; for example, allow user to download a file but not upload to OneDrive.

Address CASB requirements for risk discovery, deep visibility, and data protection as well as hook into other apps for a consistent security posture.

# SECURITY REQUIREMENT #3
# Stop Threats

Given the popularity of Office 365, the opportunities for attacks have expanded. For example, users will log in to their personal accounts, and they might either inadvertently or intentionally share confidential information, download malware, or click links to phishing sites. These are just some of the many ways threats can arise.

According to industry research, the average organization experiences 256 anomalous events resulting in 2.7 threats each month within Office 365.[5] That is one of the reasons why Gartner estimates that by 2020, 50% of Office 365 deployments will rely on third-party tools to fill gaps in security and compliance as well as maintain consistent security policies.[6]

## Types of Threats

Threats can be external or internal, for example:

**MALWARE** that was downloaded and stored either inadvertently or intentionally.


**STOLEN ACCOUNT CREDENTIALS** used to access sensitive data.

**INSIDER THREATS,** such as disgruntled employees, taking data when they leave the company.

**PRIVILEGED USER THREATS,** a type of insider threat where users have and abuse excessive permissions.

**DOCUMENT-BASED ATTACKS** in which adversaries include macros or OLE2 embedded link objects or exploit flaws in Flash and Microsoft Equation Editor to run malicious code.

## When evaluating solutions, ensure they do the following:

- ✓ Use in-line malware prevention to apply payload-based signatures based on cloud-delivered threat intelligence.
- ✓ Block command-and-control (C2) activity, data exfiltration, and delivery of secondary malware payloads.
- ✓ Block suspicious or malformed Domain Name System (DNS) queries and sinkhole DNS queries from infected hosts to sever communications back to the attacker.
- ✓ Automatically block web-based attacks, including phishing links in emails, phishing sites, and pages that carry exploit kits.
- ✓ Prevent attacks that use the stolen credentials of privileged users.
- ✓ Stop malicious insider attacks, whether by infected device or destructive employee.

5. "Office 365 Security Use Case #4: Detect Compromised Accounts and Insider/Privileged User Threats."
6. Steve Riley and Neil MacDonald, "How to Enhance the Security of Office 365," Gartner, November 17, 2015.

# How Prisma by Palo Alto Networks Can Help

To deploy Office 365 properly, you need an architecture designed for networking and security from the start. Prisma™ by Palo Alto Networks is cloud-based security infrastructure that helps you securely access Office 365 as well as all of your other applications in the public cloud, SaaS, internet, internal data center, and other locations. With over 100+ Prisma locations around the world, users automatically connect to Prisma for secure access to Office 365, localized into the language the user expects.

Prisma enforces protection to make sure only authorized users have access to your Office 365 applications. Once connected, Prisma provides in-line protections to stop threats and prevent the movement of data as well as API protections for deep visibility within Office 365, data protection, and governance.

With Prisma, you can protect your Office 365 deployments with in-line and API security for true multi-mode CASB with next-generation security. Over time, as your needs grow, expand your deployment to cover other enterprise applications in the public or private cloud with consistent security for all users in all locations.

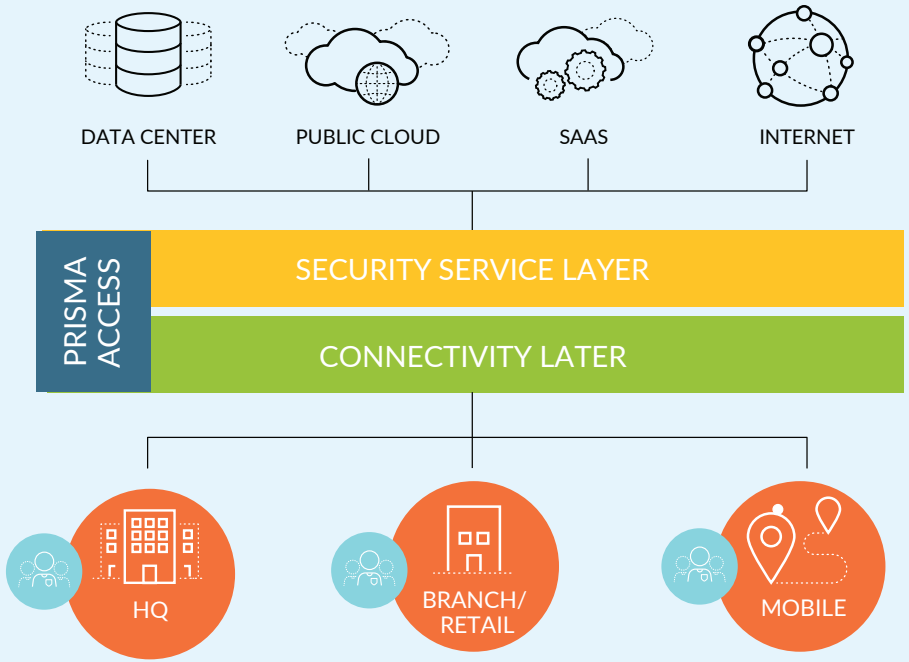



FIGURE 7
**Prisma architecture**

# Conclusion, Next Steps, and Resources

Office 365 is here to stay. The question is: are you doing enough to secure your deployment and protect your users and data when connecting, accessing applications, and sharing files? Prisma by Palo Alto Networks provides secure access to Office 365—and other SaaS apps—for all users, irrespective of their location: headquarters, regional branch offices, or on the go.

## Next Steps

See how Prisma can provide both connectivity and security to your Office 365 users. Request a demo today or watch the webinar.

## About Prisma by Palo Alto Networks

Governed access plus pervasive protection for data, applications, hosts, containers, and serverless—this is the proper foundation for the journey to the cloud. With a comprehensive cloud security suite, Prisma helps our customers secure every step of their journey.

Prisma provides unprecedented visibility into assets and risks, consistently securing access, data, applications, and modern workloads, regardless of location. The suite helps customers deploy and adapt quickly with speed and agility as well as control operational costs and reduce complexity with a radically simple architecture.

**Prisma is the most complete cloud security suite for today and tomorrow.**

PRISMA™
BY PALO ALTO NETWORKS