Secure Access for Microsoft Office 365 & SaaS Applications

Implement Robust Compliance for All Users, All Devices, and All Data

This guide illustrates best practices for secure Office 365 and Hybrid IT deployments using full authentication and authorization to reduce account hijacks, malware delivery, and potential data loss.

- ✓ Authorize users with identity-based access control
- ✓ Verify device compliance *before* permitting user access
- ✓ Safeguard data from accidental or malicious user activity

Ensuring Security Compliance for a Hybrid IT Workforce

Advances in IT such as cloud, mobility, and communications have enabled geographically dispersed workforces for nearly all businesses. As companies increasingly leverage remote employees and contractors to meet business goals in highly competitive markets, secure collaboration has become crucial for success. For nearly twenty years, Microsoft's Office has been the defacto standard business productivity suite. Now offered via the cloud, Office 365 provides users up-to-date email, document, filesharing and communications applications regardless of their location.

As of late 2017, Microsoft Office 365 boasted 120+ million active monthly subscribers and is the number one software-as-a-service (SaaS) application worldwide. The growing adoption of the Office 365 cloud service combined with the increased use of mobile devices means companies must ensure that only authorized individuals are allowed access to avoid any kind of security breach. And with the cost of data breaches averaging $4M USD each – not including costs associated with brand reputation, compliance, and customer or end-user notifications – businesses must make certain access to Office 365 is secure or risk regulatory and financial exposure[1].

Secure Access from Pulse Secure ensures that access to Office 365 (or other SaaS applications) is restricted only to authorized users using secured devices. This is critical for healthcare, financial, and public administration industries that are often targets for data breach campaigns – all are subject to stolen credentials, data exporting, and privilege misuse[2]. Indeed, only 30% of global information staff in the healthcare field have been trained on protecting workplace data and even fewer are aware of workplace security policies[3].

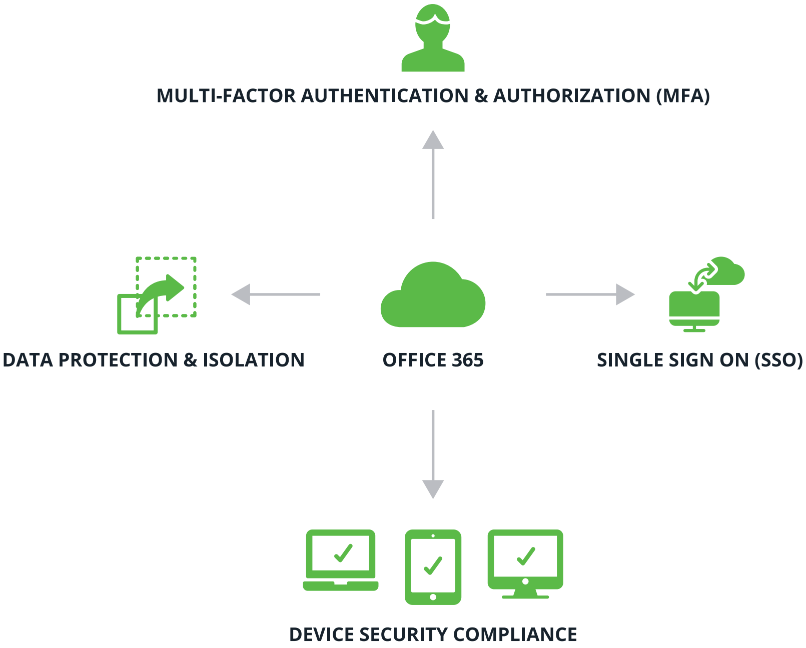
Pulse Connect Secure and Cloud Secure make it easier for customers to transform their trusted and reliable VPN solution into a scalable Secure Access solution. Coupled with Pulse One's broad management capabilities, it adapts to the morphing data center and the different ways today's workers access applications and information. Pulse Secure's Secure Access is designed to simplify how companies establish, maintain, and enforce compliant connectivity in the following ways:

1. Enforce multi-factor authentication (MFA) for access to hybrid IT environments
2. Provide single sign-on (SSO) using an on-premise identity store
3. Ensure security compliance for computers, smartphones and tablets using Host Checker
4. Enable data protection/isolation with on-demand connectivity

[1] IBM Ponemon Institute 2017 Cost of Data Breach Study
[2] Verizon 2017 Data Breach Incident Report
[3] Forrester Research Global Business Technographics Workforce Recontact 2017 Survey

Office 365 Rollout?

How Pulse Secure helps meet compliance standards


MULTI-FACTOR AUTHENTICATION & AUTHORIZATION (MFA)
DATA PROTECTION & ISOLATION
OFFICE 365
SINGLE SIGN ON (SSO)
DEVICE SECURITY COMPLIANCE

Cloud Fast Facts

- Over 70% of businesses deploy Office 365
- 67% of organizations are concerned about data loss and leakage
- Nearly 60% fear employees will do something bad for financial or personal gain — more than hacktivists, criminals, or state-sponsored agents
- Phishing was the #1 threat vector (>50%) for Office 365-based threats with over 200 million phishing emails every month by end of 2017.

(2018 Cloud Security Report, CyberSecurity Insiders; Microsoft Intelligence Report, vol 23; Verizon Mobile Security Index 2018)

This paper discusses best practice use of these capabilities to protect your Office 365 deployment. But it is equally applicable to other cloud or hybrid IT services that may only offer username and password restrictions for access. Accessing such services without a comprehensive authentication and authorization practice can increase the chance of account hijacks, malware delivery, and data leakage -- and risk meeting compliance standards such as HIPAA or PSD2.

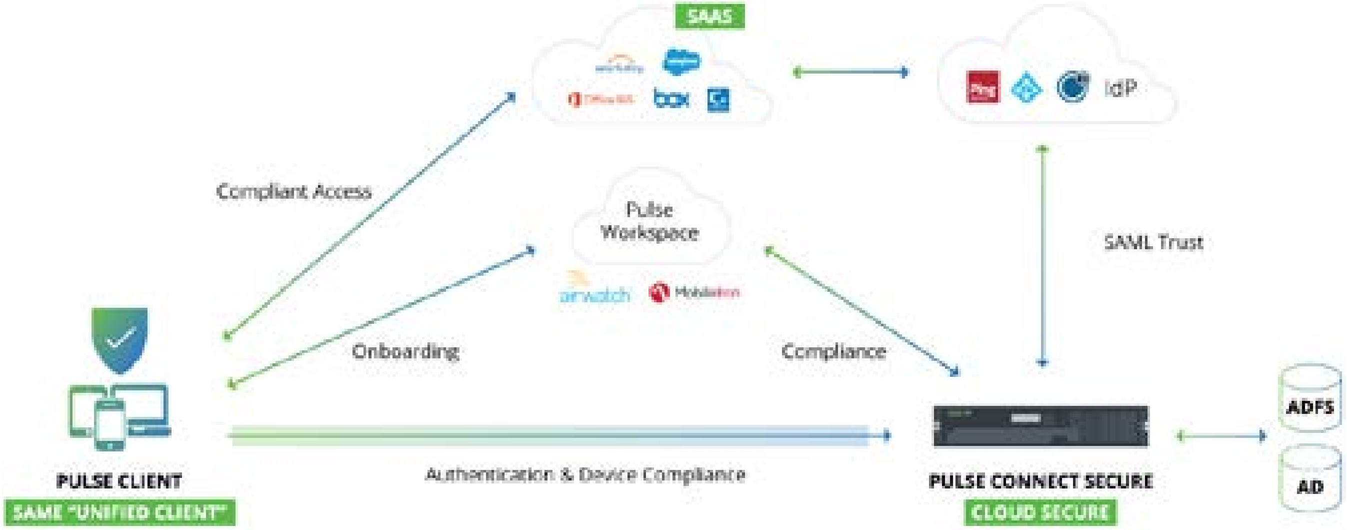


Figure 1 – Pulse Secure's architecture allows seamless secure access to cloud applications like Office 365.

Establish a Secure Multi-Factor Authentication Platform across Hybrid IT

With cybercriminals getting smarter every day, it's critical that only authorized users access Office 365. Simple usernames and passwords are no longer sufficient in a world where phishing attacks are increasing in number and sophistication. Multi-factor authentication (MFA) delivers an additional level of security to combat login attacks.

Pulse Connect Secure meshes seamlessly with Office 365 so that all users are immediately redirected to Pulse Connect Secure, where identities are first validated through MFA, and only then permitted access to Office 365 via Pulse Cloud Secure. From the users' perspective, this is completely friction-free: they can use native applications and quickly log in to their Office 365 account from any location, whether remote or on-campus.

Best Practice Implementation Tips Using Pulse Secure

- Implement tight, identity-based access controls with group-based policies that ensure only authorized users access Office 365 resources
- Provision Host Checker validation of users' computers, smartphones and tablets to ensure devices pass a compliance check before connecting
- Use native Time-based One-Time Passwords (TOTP) such as Google Authenticator to help consolidate authentication infrastructure. Since spear phishing attacks are among the most successful to garner passwords, 2-step verification protects users from account lock-out if passwords are compromised.
- Streamline management, eliminate box-by-box configuration, and ensure compliance visibility and reporting using Pulse One

Reasons to Use

- 93% of businesses indicate that mobile devices present a serious and growing threat
- 53% of Microsoft Office 365 top threats were phishing attacks
- 38% of organizations struggle with compliance
- 27% admitted experiencing an incident that resulted in data loss or system downtime in the past year

(Microsoft Security Intelligence Report, Vol 23; Verizon Mobile Security Index 2018)

Provide Single Sign-on Using On-premise Identity Store

Businesses often want to retain their identity store database, including all user names and passwords, on-premises for security and compliance reasons. Pulse Connect Secure enables the adoption of cloud applications, such as Office 365, by acting as the identity provider without moving the identity store to the cloud as well.

Through SSO, users log in once to Pulse Connect Secure to access multiple cloud services and applications in the data center. This enhances security by reducing the possibility of stolen credentials and streamlines user productivity by eliminating multiple logins. Moreover, your identity database isn't further fragmented and passwords never cross the firewall.

Pulse Secure's at-a-glance Dashboard then makes it easy for administrators to obtain a quick view of the Top 5 SSO applications being accessed, usage trends, and device compliance statistics.

Pulse Connect Secure integrates seamlessly with widely used SAML Identity Providers like Active Directory Federation Services (ADFS), Ping Identity and Okta. Such integrations enable customers to add compliance posture assessments through Pulse Connect Secure to existing deployments.

With businesses seeking to increase productivity through BYOD access 24x7, any downtime – however minimal – can be frustrating. Through integration, Pulse Secure ensures that your employees, partners, and contractors remain fully online and able to access Office 365 or other SaaS applications.

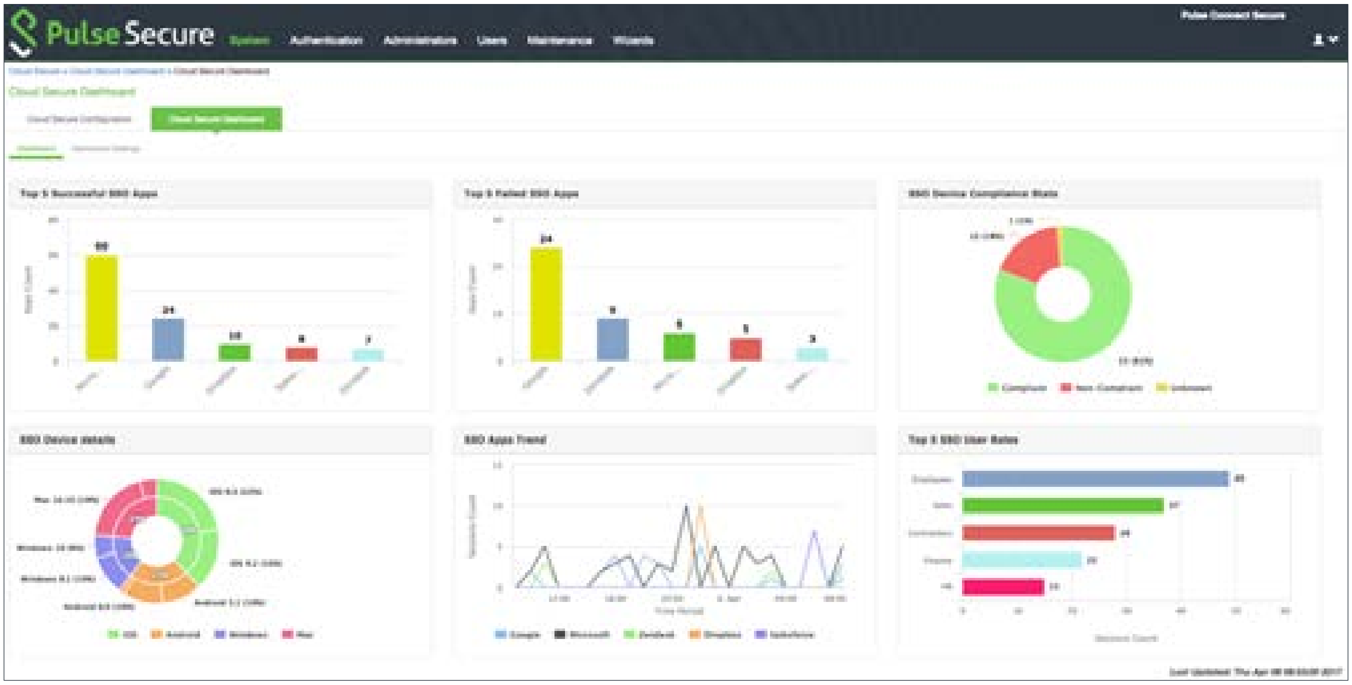


Figure 2 – Cloud Secure Dashboard graphically shows SSO apps usage.

Best Practice Implementation Tips Using Pulse Secure

- Leverage Pulse Connect Secure's integration with ADFS using SAML 2.0 to use your existing identity federation for partners and contractors without any changes
- Use Pulse Connect Secure SAML IdP and SAML SP mode support with no need to re-enter credentials or remember and renew passwords
- Add compliance checks to existing SAML IdPs such as Microsoft Azure AD and Okta to ensure that authenticated users only employ authorized devices

Reasons to Use

- User account attacks up by 300% in 2018
- 55% of businesses fear unauthorized access
- 44% of logins coming from malicious IP addresses

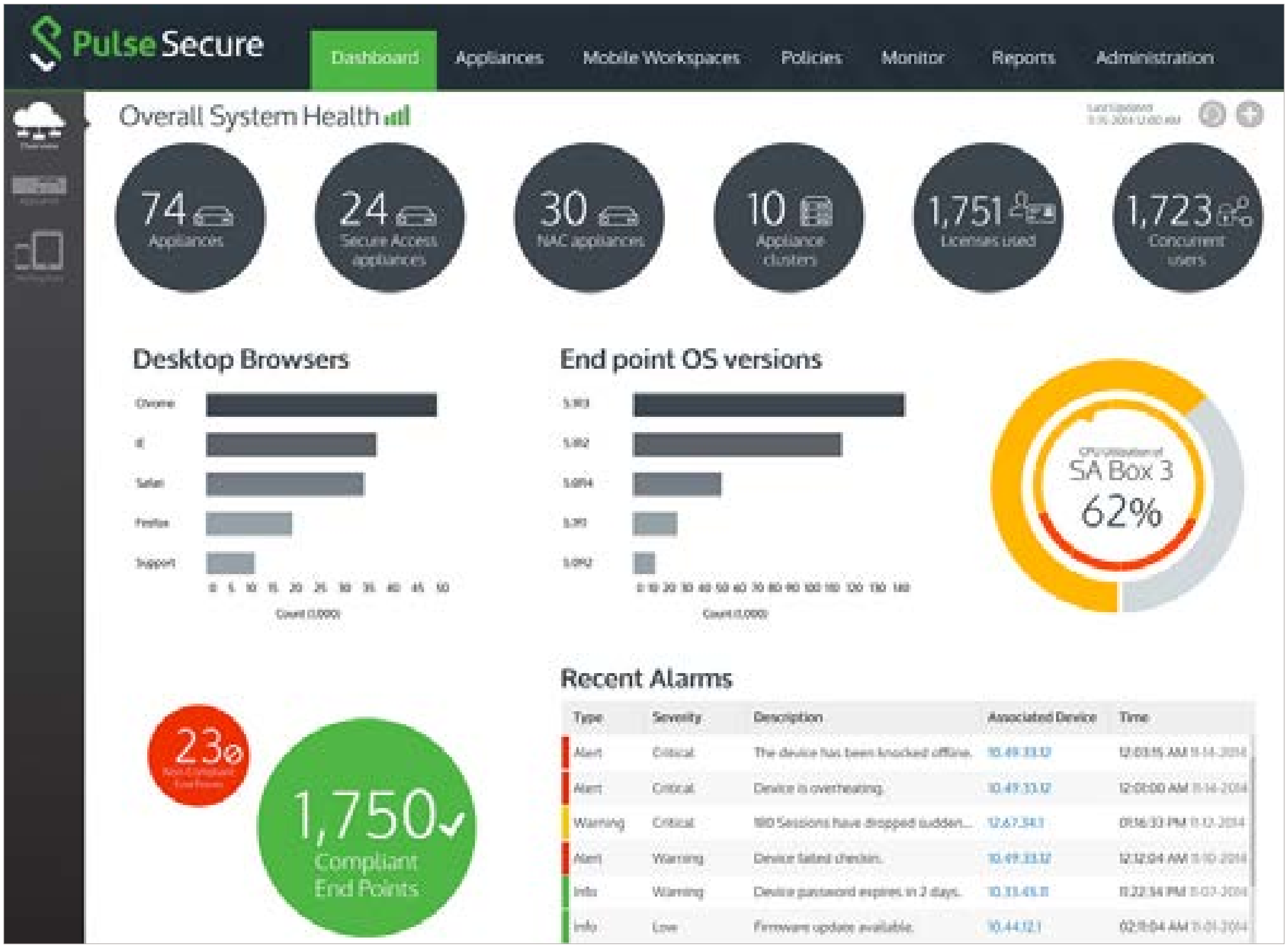
(2018 Cloud Security Report, CyberSecurity Insiders; Microsoft Security Intelligence Report, Vol 23)

Ensure Device Compliance

Device compliance is mandatory with a workforce on the move and accustomed to using the device of their choice. Pulse Connect Secure verifies all devices – laptops, tablets, smartphones, etc. – to ensure that proper policy compliance is in place, such as anti-virus and personal firewall software *before* a user connects to online resources. Only when compliance is validated can workers access data center or SaaS applications such as Office 365. If a device is deemed non-compliant, it can be quarantined – or granted, denied, or given controlled access by administrator-defined policies.

Pulse Connect Secure validates laptops using its rich Host Checking capabilities and integrates with enterprise mobility management (EMM) software to effectively protect and manage mobile devices. This significantly reduces the chance that workers and contractors accessing your network have devices with malware or that have been rooted or jailbroken. Pulse Secure's Pulse One Dashboard makes it easy to see specific compliant or non-compliant devices with at-a-glance visibility and reporting.

Whenever possible, Host Checker automatically remediates noncompliant endpoints by updating software applications that do not comply to corporate security policies.



Recent Alarms

Type	Severity	Description	Associated Device	Time
Alert	Critical	The device has been knocked offline.	10.49.33.12	12:03:15 AM 11-14-2014
Alert	Critical	Device is overheating.	10.49.33.12	12:00:00 AM 11-14-2014
Warning	Critical	100 Sessions have dropped sudden...	12.6.7.34.1	01:16:33 PM 11-12-2014
Alert	Warning	Device failed checkin.	10.49.33.12	12:12:04 AM 11-10-2014
Info	Warning	Device password expires in 2 days.	10.33.45.11	11:22:34 PM 11-07-2014
Info	Low	Firmware update available.	10.44.12.1	02:11:04 AM 11-01-2014

Figure 3 – Gain insights into device health and connection status.

Best Practice Implementation Tips Using Pulse Secure

- Extend compliance checks to mobile devices with EMM integration, including Pulse Workspace, AirWatch, MobileIron and Microsoft Intune
- Enable corporate-owned device access using machine authentication for even stronger security protection
- Protect against malware with Host Checker vulnerability assessment and verification of OS version, patch level, and other policy settings

Reasons to Use

- 54% increase in mobile malware variants
- Only 20% of Android devices are running newest major version
- 2.3% of those are running latest minor release

(Symantec 2018 Internet Security Threat Report)

Protect Data and Provide On-demand Connectivity

The Office 365 user experience must deliver seamless, on-demand connectivity from anywhere on the user's preferred devices. Users routinely access both personal and business applications from multiple devices. In fact, the average employee accesses over five mobile business apps daily[4]. Unfortunately, this opens the door for sensitive, confidential, or proprietary business data being accessed or copied from a business to a personal application on a device.

Pulse Workspace provides per-app, on-demand connectivity for both Android and iOS devices. The industry has long deemed Apple iOS devices to be enterprise class with features such as on-demand, per-app VPN and a secure, easy-to-manage device container. Android, the most popular BYOD device, has strived to reach parity with iOS devices but has lagged behind, creating headaches for security IT practitioners. Pulse Workspace delivers the world's first on-demand, per-app VPN for Android, enabling both Android and iOS users to simply touch an app to connect to the data center or cloud. Policy-based split tunneling allows direct connection to the cloud or cloud connectivity via the data center. The Workspace container isolates enterprise data and apps and prevents users from violating data compliance rules. Pulse Workspace can also wipe business applications and data from a device if the device is lost or stolen, increasing your compliance security posture and reducing the possibility of sensitive data loss.

Best Practice Implementation Tips Using Pulse Secure

- Use built-in compliance rule sets for iOS and Android to detect jailbroken and rooted devices
- Deploy Workspace containers on mobile devices that IT can remotely provision, configure with apps, and wipe
- Use per-app, on-demand connectivity for Android and iOS with split tunneling for policy-based cloud and data center access

Reasons to Use

- Less than 39% of organizations change default passwords
- Only 38% use strong/two-factor authentication on their mobile devices
- 14% of organizations use public WiFi for work tasks -- despite it being officially prohibited

(Verizon Mobile Security Index 2018)

[4] Syntonic "BYOD Usage in the Enterprise", 2016

Conclusion

Pulse Secure has helped thousands of government, healthcare, financial services and other security-conscious organizations ensure security compliance for remote users connecting to the data center. Now, starting with Office 365, you can use our compliance know-how and solution to protect applications and information moving to the cloud. Implementing our best practices will help ensure that users are always compliant, regardless of their location or their device. It's simple for both you and your users, and it's proven.

For more information about how to achieve optimal usage of Microsoft Office 365 and other SaaS applications through identity-based access control and robust compliance, please see our Office 365 security page at https://www.pulsesecure.net/solutions/o365/overview/ or contact us at www.pulsesecure.net.

SSO enhances security by reducing the possibility of stolen credentials and streamlines user productivity by eliminating multiple logins.

About Pulse Secure

Pulse Secure, LLC offers the easiest, most comprehensive Secure Access solutions that provide visibility and seamless, protected connectivity between users, devices, things and services. The company delivers suites that uniquely integrate cloud, mobile, application and network access to enable hybrid IT. More than 20,000 enterprises and service providers across every vertical entrust Pulse Secure to empower their mobile workforce to securely access applications and information in the data center and cloud while ensuring business compliance. Learn more at www.pulsesecure.net.