Solution Brief

Pulse Secure

Secure Access for Office 365

Protect enterprise data and simplify migration to the cloud

- ✓ Limit Office 365 access to managed devices
- ✓ Eliminate passwords for email and access
- ✓ Integrate with Microsoft Active Directory

Retool for mobile and the cloud

The Pulse Secure Advanced Suite is an easy and simple way to retool your network for Office 365 and mobile access. The Advanced Suite integrates Pulse Connect Secure with Pulse Workspace to provide policy-based connectivity via a BYOD container to any application. Pulse Workspace works on iOS and Android devices, giving users mobile access to the full Office 365 app suite. It also works with other cloud services like Salesforce and Box. Now you have a unified security solution for laptops and mobile devices that enables access to Office 365 and your data center applications.

Challenges

Data Leakage

Authorized users create compliance issues by using unsecured devices such as their home laptop to download sensitive email and content.

Password Issues

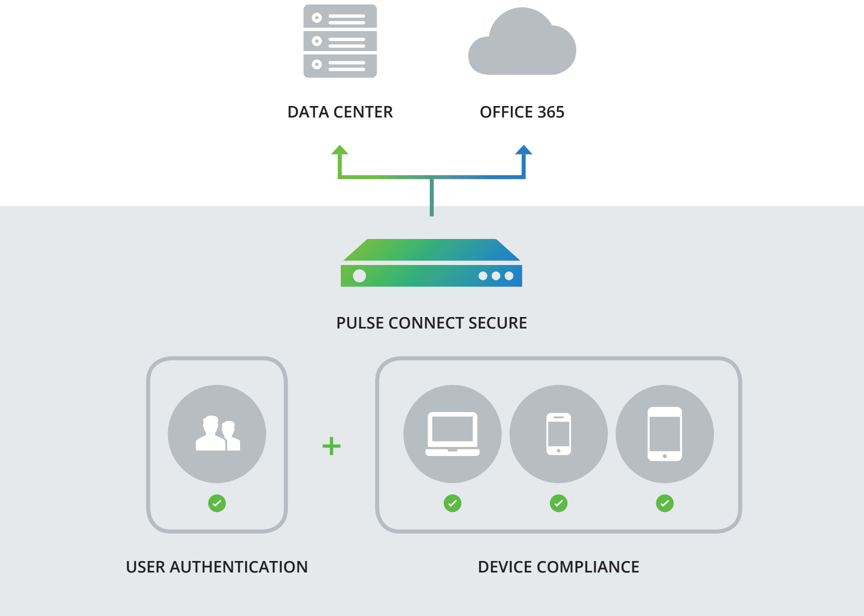
Password complexity and duration policies trigger help desk calls which Forrester estimates annually costs companies $179 per user.

AD Integration

A key migration issue is how to extend the existing user directory for internal resource access to the cloud.

Pulse Secure existing security policies to Office 365

Simplify your migration to the cloud. Enterprises have trusted and relied on Pulse Secure's strong authentication, conditional access and hostchecking to protect data center access and now it can be used to secure Office 365 and other cloud services. It's an all-in-one solution for identity management, device compliance and mobile security. Secure and easy.



Solution Notes

Secure Access Appliance

Requires PSA or virtual appliance.

Mobile Security

Mobile devices can be secured with Pulse Workspace or the solution can be integrated with an existing EMM solution.

Active Directory Integration

Enterprises can use Pulse Connect Secure as their identity provider for Office 365 or integrate with ADFS.

Mobile Devices

Pulse Workspace is compatible with iOS 7+ and Android 5.0+ (with work profile support).

Benefits

Cloud flexibility

Provide secure access to Office 365 and other non-Microsoft services such as Salesforce, Box, Concur, Dropbox and more.

Automatic compliance

Only authorized users with compliant devices can access applications and services in the cloud or data center which prevents data leakage.

No passwords

Single sign-on (SSO) with certificate authentication means no more passwords for users to fuss with.

Productive users

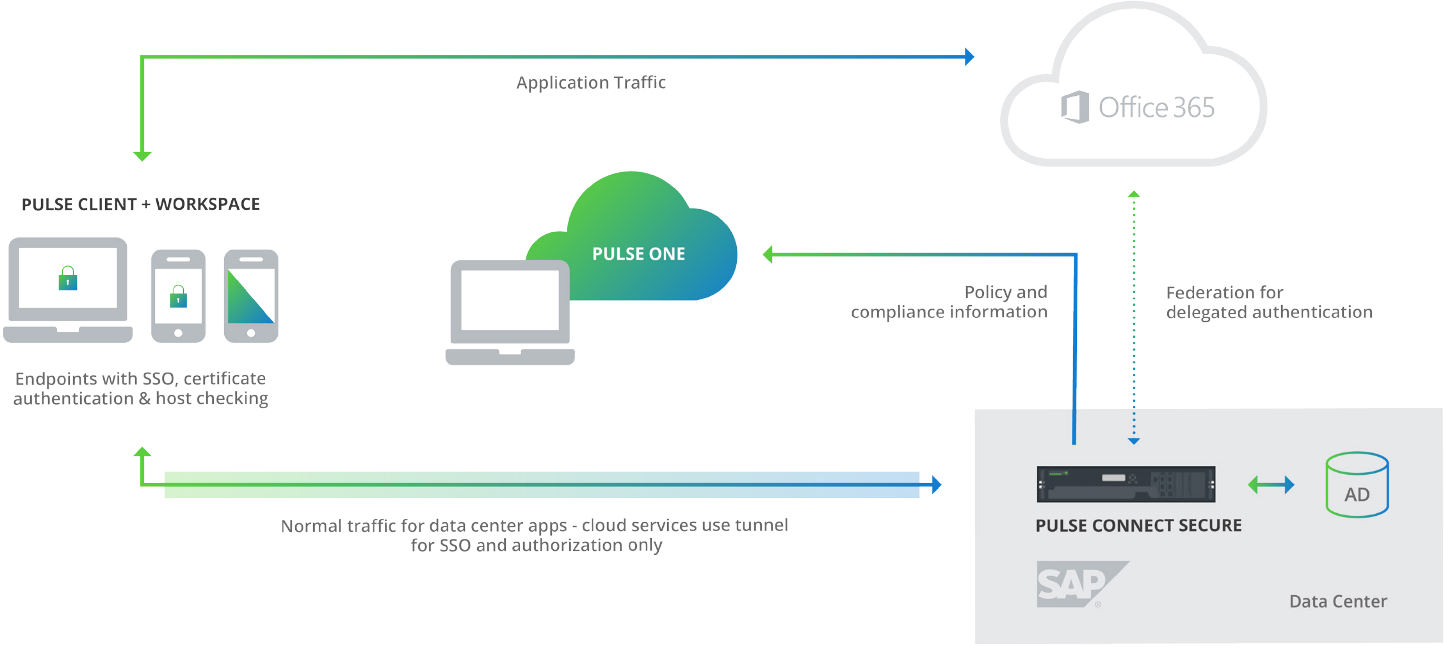
Use native mobile apps such as Word, Powerpoint, Excel and other Office 365 apps to boost worker productivity.

Easy BYOD

An easy to use and deploy BYOD container let's you respect user privacy and wipe enterprise data without affecting personal apps and content.

Simple onboarding

Self-service onboarding auto-provisions email, VPN and WiFi access. Apps are pushed to the user's device based on group policy.


Application Traffic
Office 365
PULSE CLIENT + WORKSPACE
PULSE ONE
Policy and compliance information
Federation for delegated authentication
Endpoints with SSO, certificate authentication & host checking
PULSE CONNECT SECURE
AD
SAP
Data Center
Normal traffic for data center apps - cloud services use tunnel for SSO and authorization only

How does it work?

Pulse Workspace is managed via the Pulse One console. Enterprise administrators send an email invite to users to self-provision their mobile device. The native email client is automatically provisioned to connect with Office 365 using the user's username and a unique token generated by Pulse One. The Connect Secure appliance federates with Office 365 via SAML ECP. Upon receiving a login request, Office 365 delegates authentication responsibility to Connect Secure. Connect Secure verifies the user with Active Directory and checks the security posture of the device with Pulse One. Email and data flow directly between the native email client and Office 365.

Self-Service Provisioning

Automatic configuration of user's email, VPN and Wi-Fi settings eliminates help desk calls.

SSO Access

Certificate-based authentication and SSO give users easy access to Office 365 (MFS) and other cloud services (SAML).

BYOD Container

Android and iOS container security encrypts data, controls app data sharing, selectively wipes data and supports per app connectivity policies.

Identity Management

Leverage existing Active Directory facilities to control access to Office 365 and other cloud services. It's also possible to integrate with Microsoft ADFS and other identity providers such as Ping and Okta.

Hostchecking

Compliance enforcement ensures that only secured devices can access Office 365 and other cloud services. Hostchecking can also be used with third party identity providers.

Mobile App Management

Policy-based push of Word, Powerpoint, Excel and other mobile apps boosts user productivity. An app catalog provides easy access to IT approved software.