Solution Brief

Pulse Secure

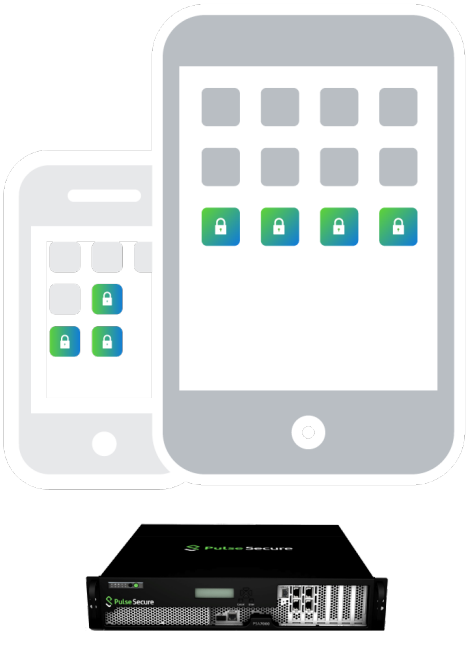
Secure Access to SaaS

Protect enterprise access to Box, Salesforce and others

- Prevent SaaS access by unmanaged devices
- Eliminate passwords with single sign-on (SSO)
- Use Active Directory for user authentication

Retool security for mobile and the cloud

Retool your security to deliver secure access for laptops and mobile devices to the data center and cloud. Pulse Connect Secure provides a secure access Client that works with your enterprise mobility management (EMM) platform to give secure cloud access. Enterprises can optionally use Pulse Workspace to provide endpoint device management and policy-based connectivity via a BYOD container.



Challenges

Data Leakage

Authorized users download cloud data to unsecured devices, such as their home PC, increasing compliance risk.

Password Issues

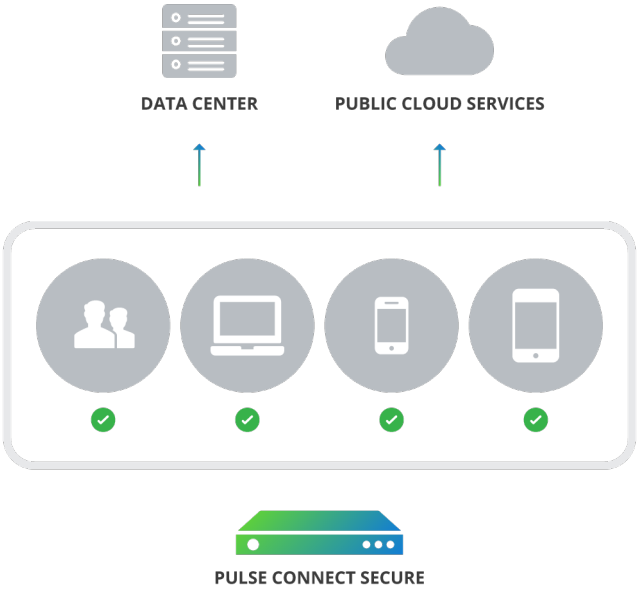
Password complexity and duration policies trigger help desk calls which Forrester estimates annually costs companies $179 per user.

Login Headaches

Separate logins for cloud services and data center applications create task friction for users.

Pulse Secure extends secure access to the cloud

Pulse Connect Secure enables secure access to the data center. Now its strong authentication, conditional access policies and host checking can be used for SaaS offerings such as Salesforce and Box.



Solution Requirements

Secure Access Appliance

Requires PSA, MAG or virtual appliance.

Pulse Client

Pulse Client 5.2r1 or above is required on endpoints. Pulse Workspace can be optionally provisioned on mobile devices.

Pulse Connect Secure

Appliances require 8.2r3 or above software.

Benefits

Cloud flexibility

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

Productive users

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

Automatic compliance

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

Easy BYOD

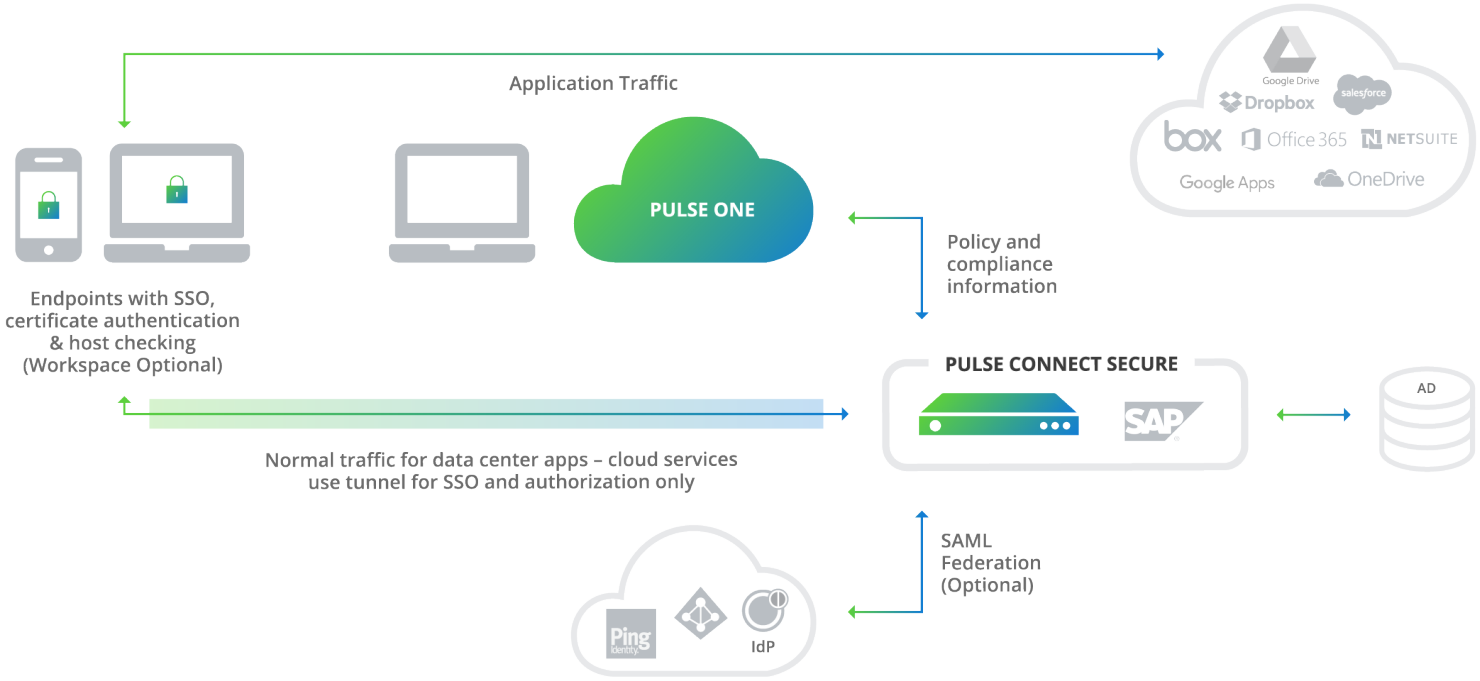
An optional mobile device container provides a simple way to deploy and support BYOD.

No passwords

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

Simple Integration

Integrate with existing identity stores such as Active Directory and leading identity providers like Ping and Okta.



How does it work?

The Pulse Client automatically launches in the background to deliver strong auth and ensure device compliance when users access cloud or data center applications. The client enables SSO use with certificate authentication to eliminate the need for passwords. Traffic to the data center for applications such as SAP use the VPN tunnel. Cloud traffic only uses the tunnel for SSO and authentication with application data flowing directly between the endpoint and the service provider. Existing identity stores such as Active Directory provide authentication. Integration with IdPs can also be configured to support existing cloud deployments. The solution can be used with Pulse Workspace or can be integrated with third party EMM platforms such as MobileIron or AirWatch.

Host Checking

Compliance enforcement ensures that only secured devices access Office 365, Box and other cloud services.

SSO Access

Certificate-based authentication and SSO give users easy access to cloud services using SAML and data center applications via legacy methods.

BYOD Workspace

Optional 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.

Centralized Management

Pulse One provides a centralized console with dashboard visibility, workspace management and reporting.

EMM Integration

Integrate with existing EMM solutions to manage devices and provide compliance status information.