



# Enterprise Mobility Management Made Easy

Secure enterprise mobility that is easy to deploy and maintain



## Features

- Easy-to-use Enterprise Mobility Management (EMM) console with administrative dashboard, app management and compliance monitoring
- Manage corporate-owned devices with specialized features for geolocation, full device wipe and Apple DEP and Google Corp Device enrollment
- On-demand, per-app VPN connectivity for both Android and iOS devices
- BYOD container security for enterprise data, apps, and communications. Zero-touch containerization secures mobile apps without the use of an SDK or manual app wrapper.

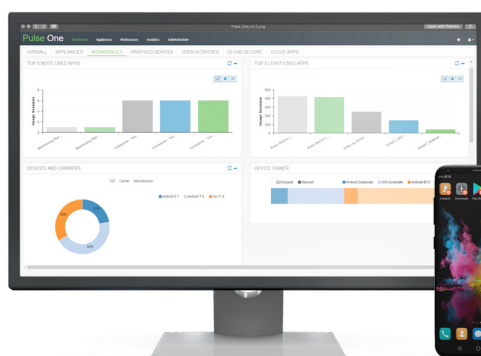
## Benefits

- Protect enterprise resources with Zero Trust access for mobile users
- Enable BYOD with device choice for iOS and Android
- Deliver secure, easy user access with the touch of an app
- Boost productivity for mobile users with native apps purchased from app stores or developed internally

Has your mobile strategy outgrown your mobile device management solution? Are you worried that a traditional EMM solution is overkill? Pulse Secure provides a powerful, yet easy to deploy and use solution that enables BYOD, mobile apps and cloud service access from iOS and Android devices.

The Pulse One management platform is designed with IT administrators in mind, providing a single, centralized console to control enterprise access and manage enterprise mobility. Use it to manage your security appliances and the corporate-owned and BYOD devices that connect to them. Pulse Workspace is the perfect container for BYOD use, with security that separates enterprise and employee data, supports enterprise wipe, and can be used with any mobile app without modification via an SDK or manual app wrapper.

Together, Pulse One and Pulse Workspace provide a holistic solution that is both user and IT friendly.



*The Workspace dashboard reveals what apps are hot and the level of user BYOD participation*

*Only from Pulse Secure -- Android for Work support includes enterprise apps with on-demand, per app VPN connectivity*

Enterprise mobility is complicated. Users want to access enterprise applications from their laptop, smartphones and tablets. BYOD is now the rule, not the exception: nearly 70% of companies view BYOD as a strategic way to mobilize more workers. At the same time, data breaches are becoming more common costing an average of \$4M each. IT departments must protect data in-motion and at-rest, while boosting worker productivity.

To address these challenges, market influencers often steer IT teams to best of breed EMM solutions. These platforms can be overly complex, full of features that are overkill for smaller IT teams that are overtasked and under resourced. Many find that they just don't have the time or skill sets to rollout and support an EMM solution.

## A Simple and Powerful EMM Solution

Harness the power of enterprise mobility without the headaches of deploying a complex EMM platform. Pulse Secure provides a holistic solution that is cloud-deployed and integrates directly with your VPN. Manage iOS and Android users to a single security and compliance standard that protects corporate information while also enabling the use of mobile apps, BYOD and cloud services.

### Manage Corporate Devices

Enterprises rely on Pulse Workspace to expand and simplify mobility to meet their business and operational needs. Pulse Workspace provides core EMM capabilities needed to protect corporate-issued devices and enable their use with mobile application and cloud services. All via a centralized console that can be deployed in the cloud or on premise.

CHALLENGES	PULSE SOLUTION
Protecting company data from device loss and data leakage	Implement native policy support for device pin, encryption of all data, controlled data sharing between apps, on-demand VPN, policy-based split tunneling, and remote device wipe
Onboarding devices	Pre-approved devices can be registered through Apple DEP and Google Corp Device enrollment for simplified onboarding
Deploying enterprise mobile applications	Curate by user group a catalog of enterprise apps that can be mandatorily pushed or optionally downloaded
Enforcing security compliance	Host checking for iOS jailbreak and Android rooting ensures safeguards are persistent
Eliminating password resets and helpdesk burden	Single sign-on (SSO) with certificate-based authentication eliminates headaches for your help desk and users

### Enable BYOD Usage

Enable employees to use their preferred personal device, keeping their data private while ensuring enterprise data security. Pulse Workspace implements a fully separated, secure container that isolates enterprise applications and data from personal items such as photos. This gives IT complete governance over corporate information while not infringing on user privacy.

CHALLENGES	PULSE SOLUTION
Protecting company data from device loss and data leakage	Implement native policy support for device pin, container separation and enterprise wipe of the container
Onboarding devices	Self-service provisioning automatically configures personal devices with the user's email, VPN, WiFi settings and apps
Deploying enterprise mobile applications	Curate by user group a catalog of enterprise apps that can be mandatorily pushed or optionally downloaded to the enterprise container
Enforcing security compliance	Host checking for iOS jailbreak and Android rooting ensures safeguards are persistent
Eliminating password resets and helpdesk burden	Single sign-on (SSO) with certificate-based authentication eliminates headaches for your help desk and users
Providing device choice	Support for iOS and Android enables the use of preferred devices for work with the same user experience including on-demand app connectivity
Respecting user privacy	Container separation ensures user privacy enterprise wipe selectively wipes corporate data and applications without affecting user data

## Deploy, Manage and Scale with Ease

Pulse One lets IT administrators manage mobile devices and control enterprise access to the data center and cloud from a centralized console. Because it's hosted in the cloud, there's no need to deploy, maintain and scale an EMM server within your data center. However, if you prefer Pulse One can also run in the data center

CHALLENGES	PULSE SOLUTION
Lack of visibility	Pulse One provides dashboard visibility of all access appliances and the devices that connect to them. Use the dashboard to monitor network access and drill down to proactively address operational and administrative issues.
Integration with existing infrastructure	Pulse Workspace provides per-app connectivity that leverages the existing user directory, enterprise VPN and network access control (NAC) for simplified deployment and proven network scale while also facilitating seamless use of cloud services along with data center applications.
More training needed for IT admins	While other EMM solutions require multiple servers and days of training to support them, Pulse Secure's cloud-based approach keeps things simple. No servers and an intuitive system that can be up and running in minutes.

Pulse Workspace is a Pulse One capability that can be deployed via the cloud or an on-premise appliance. Customers can purchase this capability as part of the Pulse Access Suite Advanced and Enterprise Editions. Get the mobility management capabilities you need without the headaches of traditional EMM solutions.

## Key Features and Advantages

FEATURE	ADVANTAGE
Container Security	A single security standard for iOS and Android that includes encryption of all data, controlled data sharing between apps, on-demand VPN, policy-based split tunneling, and enterprise wipe.
Service Auto-Provisioning	Automatic configuration of user's email, VPN and Wi-Fi settings eliminates help desk calls.
Single Sign-On	Eliminate the need for passwords with Workspace SSO. Users can access any mobile app simply by unlocking their Workspace and touching an app. No more password problems or help desk calls
Compliance Enforcement	Host checking for iOS jailbreak and Android rooting ensures safeguards are persistent.
Cloud Access	SSO with device host checking ensures that only authorized users with compliant devices access Office 365, Box, Dropbox and other SaaS offerings.
App Management	Curate by user group a catalog of enterprise apps that can be mandatorily pushed or optionally downloaded.

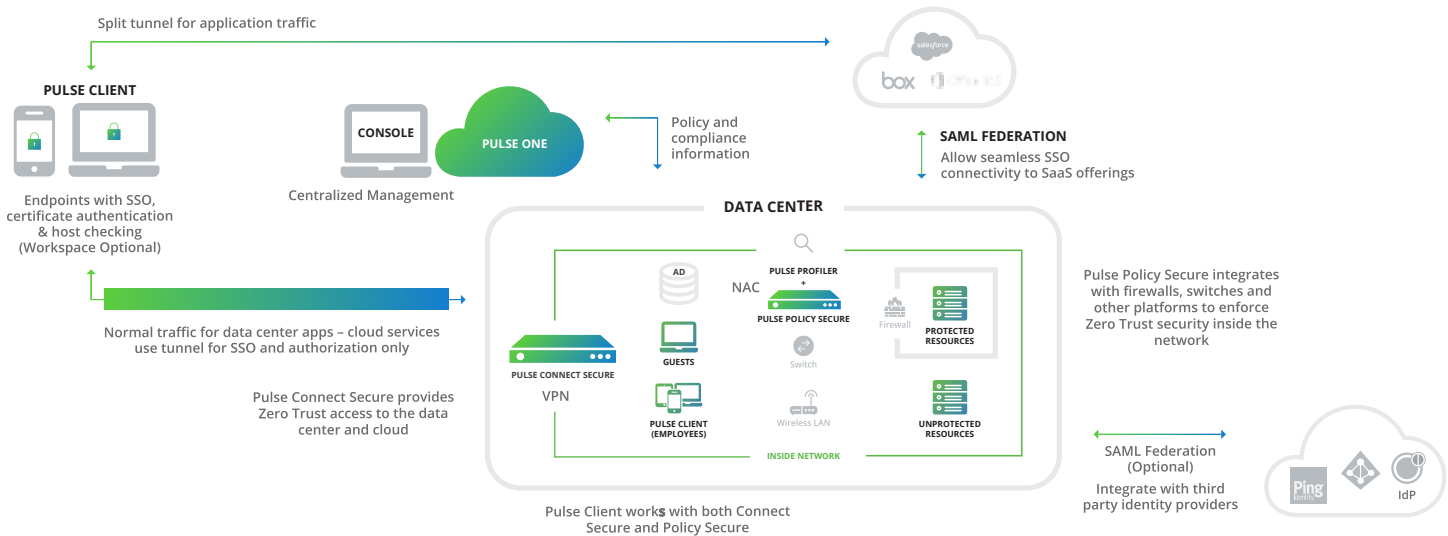
*"Workspace was an easy sell to executives. Not only did it meet and exceed all of our security needs, but it was easy to deploy and enabled our employees to provision their own mobile devices."*

*Brett Safford, IT Manager at Integration Partners.*

# How Pulse Workspace Works

Pulse Workspace can be purchased as part of the Pulse Access Suite. Both the Advanced Suite Edition and the Enterprise Suite Edition include Pulse One and Pulse Workspace, providing customers with a Zero Trust solution that is ready for any mobile requirement.

The Pulse Access Suite connects workers to company resources and protects company devices, regardless of location – in the data center, cloud or mobile. Pulse Secure delivers access to all company resources via a single client or mobile application – dramatically simplifying access and increasing user productivity. Administrators configure Zero Trust policies to control access based on devices, locations, resources, users and groups, or even endpoint profiling. Policies can be extended to internal networks, allowing organization to identify, profile, secure and manage IoT devices, provide guest user access, and secure BYOD endpoints. Centralized management and reporting meet the needs of the toughest regulatory compliance environments.



**Corporate and Sales Headquarters**  
**Pulse Secure LLC**  
2700 Zanker Rd. Suite 200  
San Jose, CA 95134  
[www.pulsesecure.net](http://www.pulsesecure.net)

## ABOUT PULSE SECURE

Pulse Secure, LLC offers software-defined Secure Access solutions that provide visibility and easy, protected connectivity between users, devices, things and services. The company delivers suites that uniquely integrate cloud, mobile, application and network access control for hybrid IT. More than 20,000 enterprises and service providers across every vertical rely on 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](http://www.pulsesecure.net).



[linkedin.com/company/pulse-secure](https://www.linkedin.com/company/pulse-secure)



[twitter.com/PulseSecure](https://twitter.com/PulseSecure)



[www.facebook.com/pulsesecure1](https://www.facebook.com/pulsesecure1)



[info@pulsesecure.net](mailto:info@pulsesecure.net)