Omnissa Workspace ONE for Unified Endpoint Management

Manage, secure, and monitor all devices for every use case

GET STARTED →

omnissa™

Truly unified, cloud native endpoint management

Omnissa Workspace ONE® is an industry leader in cloud native unified endpoint management and security. Workspace ONE gives IT teams control over the highly diversified device deployments found in today's organizations while ensuring enterprise security throughout the lifecycle of every device across every OS platform.

Omnissa Workspace ONE® UEM manages and secures devices and apps, taking advantage of native mobile device management (MDM) capabilities and cloud native management efficiencies to simplify management of all devices at scale with a single powerful product.

Workspace ONE: A cut above the rest

For organizations with global deployments across regions, divisions, and departments, complexity can become an issue. To ensure efficiency and ease of use even in the most complicated scenarios, Workspace ONE UEM is built on a **multitenant architecture** that enables flexible groupings and assignments so that admins can customize the user experience for every stakeholder in the organization. To further enhance efficiency, **role-based contextual dashboards and access controls** allow admins to focus only on the data specific to their job function.

Supported OS platforms*

Windows   Chrome   **Linux**   **QNX**

macOS   iOS   **Knox**   Android

* Sample only: Not all supported OS platforms shown.
  Relationships with OEMs ensure same-day support for new releases.

One UEM for all use cases

Workspace ONE UEM uniquely supports any use case your organization may require.

Bring your own device

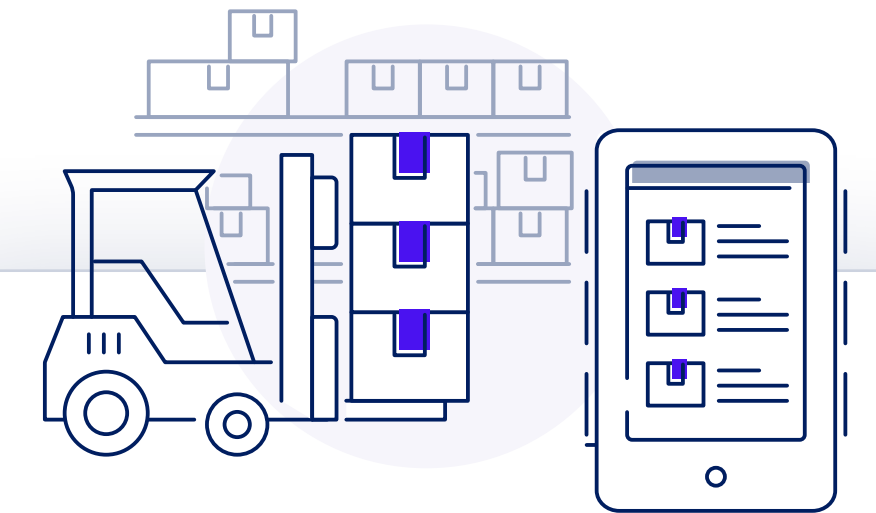Deliver the privacy employees demand with total separation between work and personal resources.

Corporate-owned assets

Admins can employ a stronger supervision mode with advanced capabilities to exert greater control.

Shared devices

Multiuser mode with check-out and check-in functionality enables deployment of settings and apps specific to each user.

Frontline workers

For mobile and line-of-business ruggedized devices in the field, IT can easily provision apps and files and remotely support users.

Save time and money with optimized IT

In a time when organizations are seeking to reduce operational overhead while optimizing IT efficiency, automation is key. Omnissa is evolving the digital workspace from a manual and task-centric system to an autonomous and outcomes-driven one. The result is a digital workspace platform that delivers self-configuring, self-securing, and self-healing actions by leveraging data and data science to inform more advanced automation. With Omnissa Workspace ONE®, your organization can ease the operational burden on your IT workforce via an autonomous workspace, freeing them to focus on higher-value tasks.

Omnissa Workspace ONE® UEM manages all device types on all OS platforms for all use cases, with security built in to every piece.

Its modern architecture supplies self-contained, modular, and loosely coupled microservices that deliver high performance, scalability, and product quality, enabling you to optimize resource delivery throughout the enterprise.

With Workspace ONE UEM, IT can manage all endpoints and keep them continually updated with new policies, patches, and versions without wasting time and money supporting multiple siloed management tools with limited capabilities.

Security: From conventional to Zero Trust

Workspace ONE UEM reinvents device hygiene by addressing security on multiple fronts and providing rich management controls that allow admins to customize an array of security policies and device posture checks. By enabling visibility across all end-user computing environments, Workspace ONE unifies the management of experience and security outcomes without compromising on either vector.

- ✓ Built-in features for system settings, data protection, apps, device controls, and more can prevent data leakage by restricting actions such as sharing sensitive data between apps and syncing with unknown devices. Corporate-owned devices can be supervised for higher levels of control.

- ✓ Certificate lifecycle management enables you to renew certificates automatically or manually.

- ✓ Workspace ONE Tunnel encrypts traffic from individual applications to the back-end systems they talk to with "least privilege access" through the Unified Access Gateway, which proxies and protects the application.

- ✓ Consistent maintenance of desired state management (DSM) unlocks significant opportunities for advanced security and locally enforced device compliance.

- ✓ Omnissa Workspace ONE® Mobile Threat Defense protects mobile devices from phishing and application, device, and rogue network-originated threats.
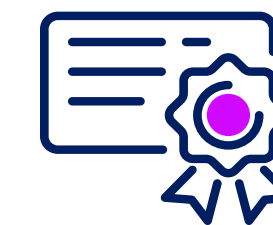
Workspace ONE is certified by a number of security standards organizations so that tightly regulated, security-sensitive companies and institutions can use it to manage their device deployments with confidence.

Before granting access to resources, Zero Trust security checks devices and context in a multitude of ways and takes action to remediate deficiencies as necessary.

A modern architecture for the modern enterprise

Automate device onboarding

New devices register over the air—with zero touch from IT—during initial power-on with customizable configuration tools like Windows 10 and 11 **Out-of- Box Enrollment and drop-ship provisioning**, automated device enrollment with Apple Business Manager, zero-touch enrollment of rugged devices, and more.

With Omnissa Freestyle Orchestrator, admins can create and automate complex workflows with a low-code canvas user interface. These capabilities give employees access to email, apps, and data within minutes of their first login.
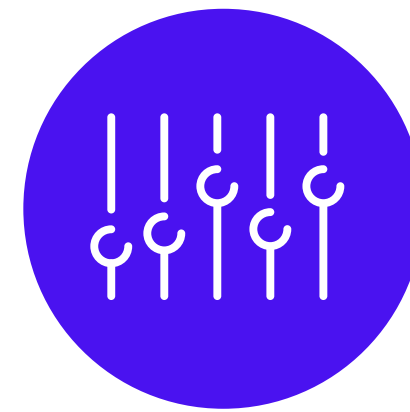
Intelligently configure any endpoint

Set and enforce access and data policies across all apps, devices, and locations in one place.

With automation capabilities and intelligence-driven insights into the entire digital workspace environment, Workspace ONE UEM can quickly and automatically identify out-of-compliance devices, apply the latest security patches, and automate access control policies based on user behavior.

Workspace ONE UEM enables configurations based on **dynamic smart groups** and makes updates automatically as those variables change.
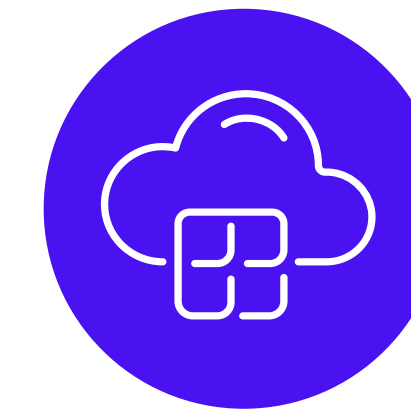
Deliver and manage every app, anywhere

Software distribution enables you to **automatically install, update, and remove software packages,** and secure them with compliance policies.

Create an automated workflow for software, applications, files, scripts, and commands to install on endpoints, and configure installation during enrollment or on demand. Set the application package to install based on conditions such as network status or defined schedules, as well as deploy software updates automatically and notify users when updates occur.

Raise employee satisfaction—and productivity

Today's employees expect the flexibility to work from anywhere, at any time, on any device. They expect to be able to choose the endpoint, or endpoints, they're most comfortable with, irrespective of the OS. And when accessing work apps and data across their devices, they expect to have a consistent and user-friendly experience.

Companies that can meet these expectations have an advantage over the competition in improving employee satisfaction and productivity.

But as device and application deployments continue to grow and become more complex, providing a consistently great employee experience becomes more difficult. This difficulty is compounded when admins are forced to use a handful of expensive, siloed tools that focus on managing discrete functions rather than fully empowering employees.

Workspace ONE helps overcome this challenge with:

- ✓ A self-service unified app catalog that's consistent across all devices and platforms.

- ✓ One-touch access to all types of apps like native, SaaS, virtual, and web helps optimize productivity.

- ✓ Integrated single sign-on (SSO) eliminates multiple logins for better security, speed, and ease of use.

- ✓ Built-in per-app tunneling secures sessions, even with apps behind your firewall.

Omnissa Workspace ONE Assist allows IT to:

- ✓ Connect remotely to problem devices.

- ✓ Protect employee privacy by notifying employees when their screens are visible.

- ✓ Gain insights into pervasive issues, validate assumptions about the root cause, and remediate at scale by leveraging automated workflows.

← →

Intelligence to enlighten and automate

With Omnissa Intelligence, IT teams get real-time visibility into the entire technology environment in one place so they can quickly make informed, data-driven decisions. IT teams can easily **customize dashboards** in infinite ways to provide the data they need, while **advanced analytics** help resolve issues that can negatively affect the user experience. To save time, teams can use premade templates within Omnissa Marketplace.

More than just an analytics engine, Omnissa Intelligence can automate routine processes to minimize manual tasks for the IT team and empower employees with self-service capabilities to reduce support requests.

For example, Omnissa Intelligence can:

- ✓ Proactively recommend support services based on data suggesting a battery is about to fail.

- ✓ Automatically update drivers based on triggers identified during a vulnerability scan.

- ✓ Provide actionable insights and recommendations to IT.

Using AI and machine learning algorithms to analyze complex data sets, Omnissa Intelligence provides proactive insights and recommendations to IT. This, combined with the global orchestration and automation framework, helps drive proactive, data-driven (in comparison to simple rules-based) decisions and automations across management, security, and end-user experience.

Insight-driven workflow orchestration

Streamline IT and automate complex workflows with a built-in orchestration engine, Omnissa Freestyle Orchestrator. With Freestyle Orchestrator, Workspace ONE provides a unified orchestration framework with a single, low-code user interface to create complex IT workflows and sequences of tasks across Workspace ONE and third-party apps. Integrations with third-party apps enable organizations to leverage data and orchestrate actions across entire IT ecosystems—allowing for customization and flexibility directly tailored to each organization's needs.

The drag-and-drop canvas UI enables admins to orchestrate resources (e.g., apps, profiles, scripts), build sequential or nested flows, and use logic-based operations (e.g., IF, AND, OR) to target desired outcomes and gain more control over repetitive manual tasks.

From battery monitoring and response to shared-device check-in notifications to patch compliance and device onboarding, IT teams can automate dozens of workflows for use cases for any type of worker, whether frontline or knowledge workers.

omnissa™

Workspace ONE UEM is the most comprehensive modern management tool in the industry, providing unparalleled levels of automation, self service, user privacy, and intrinsic security while enabling organizations to manage the costs of endpoint diversity. A low-code orchestration system allows users to automate repetitive IT tasks, and a powerful data science engine drives autonomous workspaces with AI-enabled self-healing, self-securing, and self-configuring actions. Those components enable IT teams to focus on employee productivity, satisfaction, and retention.

Manage, secure, and monitor every endpoint in one place with Omnissa Workspace ONE.

LEARN MORE →

Connection®
we solve IT®

Business Solutions	Enterprise Solutions	Public Sector Solutions
1.800.800.0014	1.800.369.1047	1.800.800.0019

www.connection.com/Omnissa