

Enabling the Hybrid Workforce with Chrome Enterprise and VMware Workspace ONE

At a glance

VMware Workspace ONE® and VMware Horizon® provide a consumer-simple experience to deploy, manage and secure ChromeOS devices for the hybrid workforce.

In the hybrid age of work, organizations face challenges beyond offering a mix of remote and on-premises work options. Effective organizations are able to balance productivity, flexibility and collaboration, supporting seamless transitions between work environments and providing employees the freedom to be productive when, where and how it suits them. Further, users expect to have their choice of device while having anytime access to critical work apps and data. With their ease of use, quick startup time and built-in security, Chromebooks have seen increasing popularity in both the business and consumer markets. These benefits, combined with a consumer-simple digital workspace that streamlines access with single sign-on (SSO) capabilities to all user work applications and data, make Chromebooks an ideal option to deliver frictionless employee experiences across various use cases.

Manage Chrome devices alongside all endpoints in a unified console

Workspace ONE is built on scalable, industry-leading VMware Unified Endpoint Management (UEM) technology to manage and secure all enterprise devices from a single pane of glass. IT can manage ChromeOS alongside all other endpoints throughout the entire device lifecycle using the unified platform for streamlined deployment, remote troubleshooting and reporting. Admins can deploy policies using smart groups for granular assignment based on device, operating system, user role, geography, department and more. Workspace ONE supports multiple use cases, and admins can deploy corporate devices and shared devices, including managed guest sessions, or configure Chrome devices to use for kiosks or digital signage.

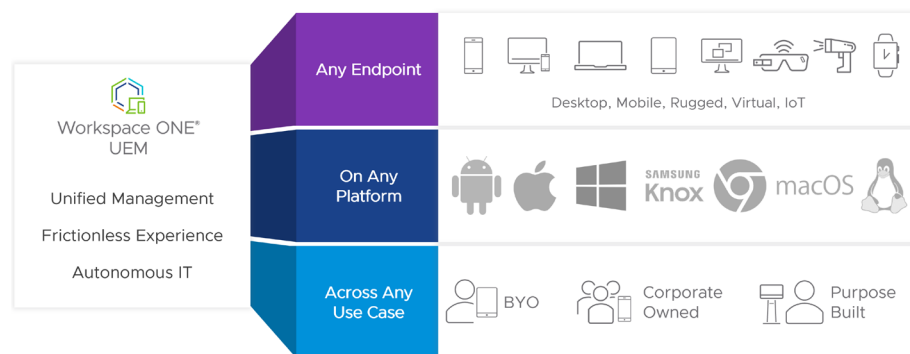


Figure 1: With UEM, simplify IT processes with one platform to manage and secure every operating system and form factor.

Key benefits

- Ability to deploy apps and policies from a unified console alongside all other endpoints through the Workspace ONE integration with the Google Chrome Policy API.
- Unified access to all apps, including Chrome apps and cloud, web and virtual apps.
- Streamlined workflows and a customizable interface for easy access to applications.
- Enterprise-grade security with unique conditional access to apps and data based on device, network, identity and more.
- Virtual Windows apps and desktops served cost-effectively from the data center or cloud.

“Providing more options to workers is key to the future of the digital workspace. With Chrome Enterprise and Workspace ONE, our customers can securely deploy and manage Chromebooks alongside all other endpoints from a single console, providing a frictionless employee experience regardless of the device. Through our partnership with Dell, the first Chrome Enterprise devices can now be managed by Workspace ONE right out of the box.”

Shankar Iyer
Senior Vice President and General Manager,
End-User Computing
VMware

Secure Chrome devices throughout the device lifecycle

Chrome devices come with built-in features that keep corporate data protected from bootup to shutdown. The multilayered security ensures that if one layer is bypassed the others are still in effect to protect the device. Starting with device boot, the device checks if anything in the system has been tampered with and repairs itself by reverting to a safe version. ChromeOS includes features such as sandboxing, automatic updates and data encryption that keep work data isolated and secure.

Integration with Workspace ONE UEM further secures Chrome devices by delivering data loss prevention policies and enabling remote actions. From the Workspace ONE UEM console, admins can configure settings to prevent unauthorized users from logging in to the device and from accessing apps. Admins can also enable conditional app access, which enforces authentication strength and restricts access by network scope or other criteria. If a device is lost or stolen, the admin can remotely wipe the device to remove corporate apps and data.

Get full certificate lifecycle management

The Workspace ONE UEM extension for ChromeOS enables a full-fledged certificate management solution for Chrome Enterprise. With the extension, admins can provision unique user- and device-based certificates for Wi-Fi, VPN, web authentication, SSO and more. Coupled with Workspace ONE UEM's first-class enterprise integration, admins can automatically renew and revoke certificates before they expire. No user interaction is required to enjoy these benefits because the installation of the extension and certificates is silent.

Drive productivity with employee experience

IT can deliver Workspace ONE Intelligent Hub to Chromebooks through the Chrome browser. From Workspace ONE Intelligent Hub, users have simplified access to a customizable launcher of work-critical applications, including all cloud, web, native, and virtual applications from a centralized location. End users authenticate into the catalog using their corporate credentials. Simple authentication, plus the ability to integrate with identity providers for SSO, alleviates users having to remember multiple credentials and URLs. For additional security, admins can require two-factor authentication to access specific, mission-critical applications. With Workspace ONE Intelligence, admins can measure employee experience through key performance indicators, such as device health, OS stability, and app and network performance, and set up triggered automations based on measurements to remediate issues and return employees back to productivity.

For more information on how to harness the speed, security and simplicity of ChromeOS in the enterprise, visit:

vmware.com/products/workspace-one/chrome-os-device-management and vmware.com/products/horizon.

For more information or to purchase VMware products

Call 877-4-VMWARE, visit vmware.com, or search online for an authorized reseller. For specifications and requirements, refer to the product documentation.

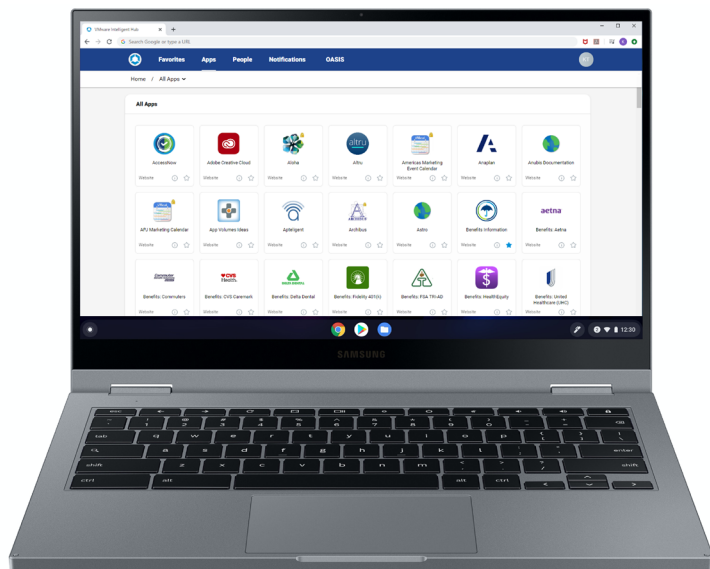


Figure 2: Workspace ONE delivers apps and virtual desktops to Chromebooks.

Enable end users with secure access to virtual desktops and apps

VMware Horizon enables Chromebook users to access virtual desktops and hosted applications with a choice of on-premises, public or hybrid cloud-based deployment models. With the VMware Horizon Client for ChromeOS, an end user can select a virtual application or full desktop on any OS and Horizon quickly delivers it to the user. The VMware Blast Extreme display protocol is fully optimized for ChromeOS and seamlessly delivers desktops and apps providing an exceptional remote user experience. Users get the responsiveness and high-fidelity display that they are accustomed to, even in low-bandwidth environments, while reducing CPU and power consumption. The combination of Horizon with Chromebooks provides IT an efficient, secure and cost-effective platform to deliver, manage and monitor virtual desktops and hosted apps.