ENABLING DIGITAL TRANSFORMATION WITH CHROME OS AND WORKSPACE ONE
Harness the Speed, Security and Simplicity of Chrome OS in the Enterprise

A Digital Workspace to Empower Users on Chrome OS Devices
Consumerization in the enterprise has led to users expecting to have the choice between any device while having access to critical work apps and data. With the ease of use, quick startup time and affordability, Chromebooks have been seeing increasing popularity in both the business and consumer markets. Combine these benefits with a consumer-simple digital workspace that streamlines access with single sign-on capabilities to all user work applications and data, to make Chromebooks an ideal option for business productivity across many use cases. A digital workspace provides the framework to enable end users with access to any application – cloud, web, virtual and native – without compromising security. VMware Workspace ONE and VMware Horizon provide a seamless experience to enable instant access to the apps that end users need to be successful on Chromebooks.

Manage Chrome OS Devices Alongside All Form Factors in a Unified Console
Workspace ONE is built on the scalable, industry leading VMware AirWatch Unified Endpoint Management technology to manage and secure all enterprise devices from a single-pane-of-glass. Chrome OS can be managed alongside all other endpoints throughout the entire device lifecycle using the unified platform for streamlined deployment, remote troubleshooting and reporting. Policies can be deployed to Chrome devices 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, shared devices or configure Chrome devices to be used for kiosks or digital signage.
ENABLING DIGITAL TRANSFORMATION WITH CHROME OS AND WORKSPACE ONE

Secure Chrome Devices Throughout the Device Lifecycle
Chrome devices come with built-in features that keep corporate data protected from boot up to shut down. The multi-layered security makes sure that if one layer is bypassed then 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 and will repair itself to revert to a safe version. Chrome OS includes features such as sandboxing, automatic updates and data encryption that keeps work data isolated and secure. Integration with AirWatch UEM further secures Chrome OS devices by delivering data loss prevention (DLP) policies and enabling remote actions. From the AirWatch Console, admins can configure settings to prevent unauthorized users from logging into the device and from accessing apps. Conditional app access can be enabled which enforces authentication strength and restricts access by network scope or by other criteria set by the administrator. If a device is lost or stolen, the admin can remotely enterprise wipe the device which removes the corporate apps and data from the device.

Enable User Productivity with Any App and Virtual Desktop
Workspace ONE can be deployed to Chromebooks as an Android application on select devices or through the Chrome browser. From Workspace ONE, end users have access to a customizable launcher of work-critical applications. The launcher includes all cloud, web, native and virtual applications and makes them accessible to the end user from one centralized location. End users authenticate into the catalog using their corporate credentials. Simple authentication plus the ability to integrate with identity providers (IdPs) for single sign-on (SSO) alleviates the difficulty of users having to remember multiple credentials and URLs. For additional security, administrators can require two-factor authentication to access specific, mission-critical applications.

LEARN MORE
For more information, visit
http://www.vmware.com/products/workspace-one
www.vmware.com/go/horizon7
www.airwatch.com

For information or to purchase VMware products, call 877-4-VMWARE, visit www.vmware.com, or search online for an authorized reseller. For detailed specifications and requirements, refer to the product documentation.

VMware Horizon enables Chromebook users to access virtual Windows desktops and hosted applications through on-premise, cloud-based, or hybrid deployment models to fit desired cost requirements. From the Workspace ONE launcher, an end user can select a virtual application or full Windows desktop and Horizon quickly delivers it to the user. VMware Horizon Blast Extreme Adaptive Transport (BEAT) protocol is fully optimized for Chrome OS and delivers the best remote user experience while reducing CPU and power consumption, even in low bandwidth environments. 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.

Figure 2: Workspace ONE delivering apps and virtual desktops to Chromebooks

“The consumerization of the enterprise has left IT managing multiple operating systems on a variety of devices – some provided by the business and others brought in by employees. As Chrome OS continues to gain momentum, our customers are eager to manage these devices consistently along with all other endpoints including mobile devices. Using Workspace ONE, our customers can securely manage the lifecycle of Chromebooks along with all their other end points giving them better security and a consistent user experience across all devices.”

— SUMIT DHAWAN, SENIOR VICE PRESIDENT AND GENERAL MANAGER, END-USER COMPUTING, VMWARE