SHI vmware

WORKSPACE ONE UNIFIED ENDPOINT MANAGEMENT

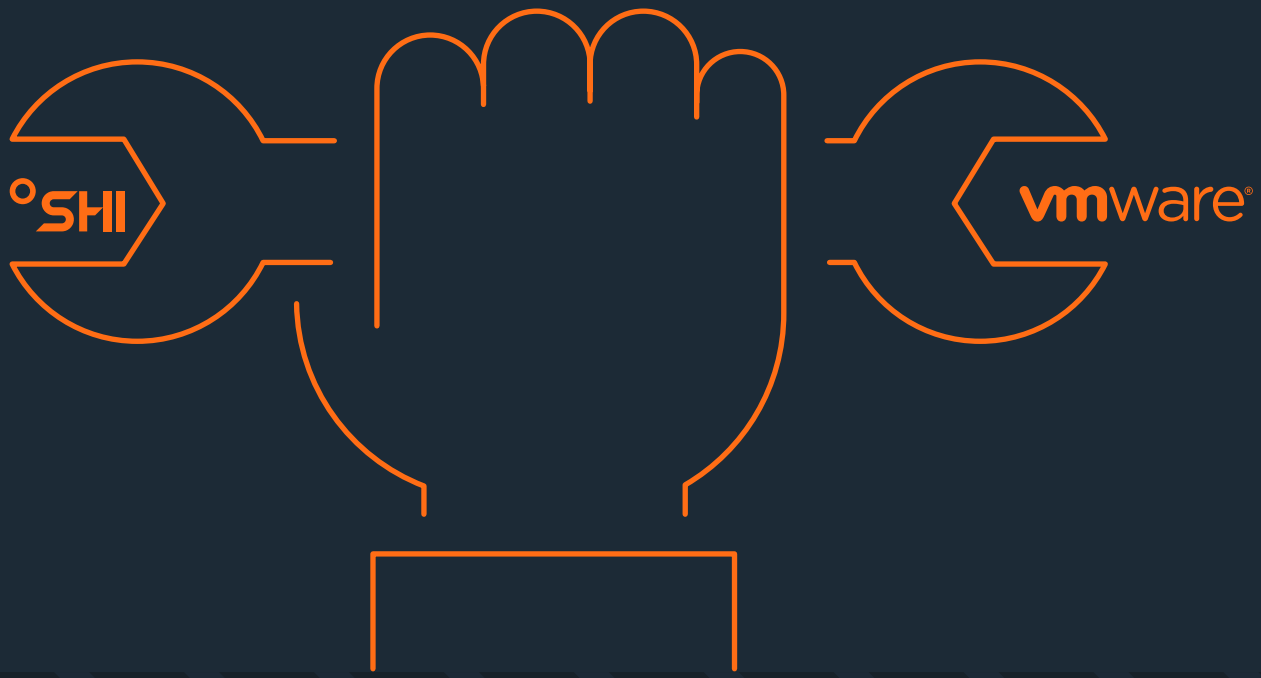
A Single Comprehensive Solution to Manage and Secure All Devices Across All Platforms

EBOOK

THIS IS INNOVATION AT WORK

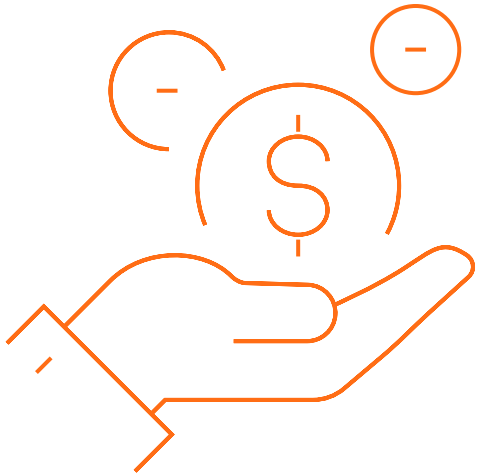
POWER YOUR WORKLOADS, CLOUDS, AND DEVICES WITH THE SHI-VMWARE PARTNERSHIP

SHI and VMware have teamed up to offer you state-of-the-art technologies with expert strategy, deployment, integration, implementation, and management. With our technical expertise and guidance, you can speed up your business growth and realize your full potential.



SAVE TIME AND MONEY WITH A WORLD-CLASS REPLACEMENT FOR MULTIPLE LIMITED IT TOOLS

In today's modern decentralized workforces, employees expect their companies to offer technologies that enable them to work from anywhere, at any time, on any device. They expect the ability to choose the platform they're most comfortable with, whether that's Windows 10, macOS, iOS, Android, ChromeOS, or a combination of platforms on multiple devices. And when accessing work apps and data across all 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 recruiting and retaining top talent.[1] But device and application deployments continue to grow and become more complex, making it difficult for IT teams to provide a consistently great employee experience. The difficulty is compounded when admins are forced to use a handful of expensive siloed tools that focus on managing discrete things rather than fully empowering employees.



1. Randstad North America, Inc. "Hiring and Developing Digital Leaders." 2018.

VMWARE: A GLOBAL LEADER

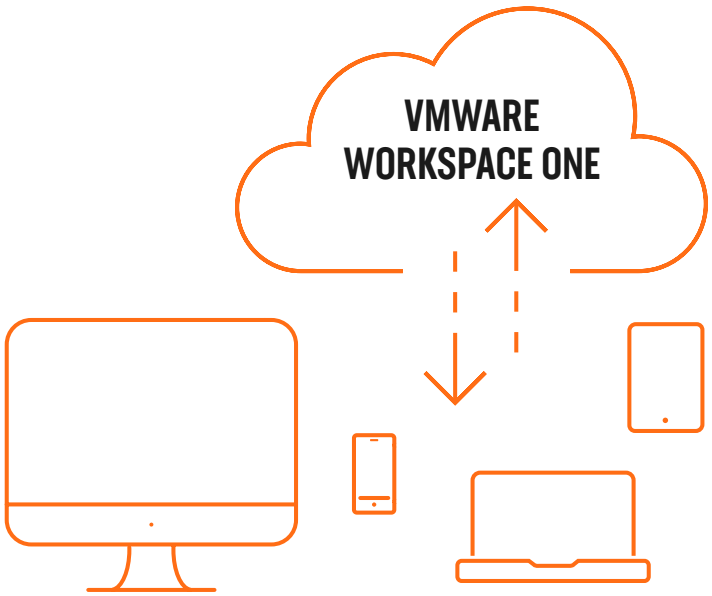
VMware Workspace ONE® is an industry-leading cloud platform for modern management and unified endpoint management (UEM) that gives IT teams control over the highly diversified device deployments found in so many organizations today, while ensuring enterprise security outside the hardened perimeter. Workspace ONE UEM provides device lifecycle management across all platforms in **a single comprehensive solution that empowers IT** to

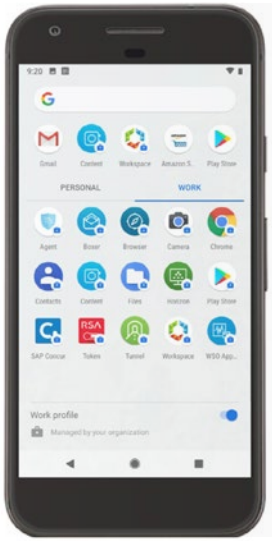
- Automate the onboarding process over the air
- Intelligently manage every device on every platform
- Flexibly support all use cases – BYOD, corporate-owned, frontline, or purpose-built
- Easily manage apps and provide a consistently positive self-service employee experience
- Make data-driven decisions and automate important repetitive processes
- Secure devices, apps, and data at rest and in transit

VMware Workspace ONE UEM is a single solution to manage all device types on all platforms in all use cases. It incorporates modern device management, application management, and security that's effective outside the corporate perimeter.

AUTOMATED OUT-OF-THE-BOX DEVICE ONBOARDING

Workspace ONE UEM enables **device lifecycle management from onboarding to retirement**. New devices register over the air (with zero touch from IT) during initial power-up with customizable configuration tools like Windows 10 Out-of-Box Enrollment, automated device enrollment with Apple Business Manager, zero-touch enrollment of rugged devices, and more. Admins can easily set up and customize the imageless configuration of work profiles such as email, VPN, Wi-Fi, apps, content, intranet sites, and other back-end resources. This gives employees access to email, apps, and data within minutes of device startup, all of which ensures immediate user productivity and **a positive employee experience right from the start**.

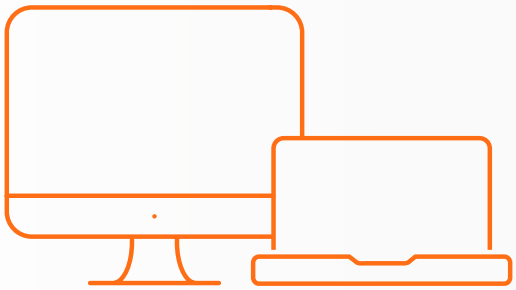




MODERN MANAGEMENT ACROSS ALL ENDPOINTS

Workspace ONE UEM manages and secures devices and apps, taking advantage of native MDM capabilities (iOS and Android) and mobile-cloud management efficiencies (Windows, Mac, and Chrome) to simplify management of all devices at scale with a single powerful solution.

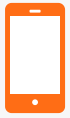
Supported Device Types



Desktops and laptops

Tablets

Smartphones



Rugged devices

Smart watches

Smart glasses

VR headsets

Mobile printers

Interactive kiosks

COMPREHENSIVE MANAGEMENT REACH

This comprehensive reach ensures IT can manage all endpoints and keep them always up to date on policies, patches, and the newest versions without wasting time and money supporting multiple siloed management tools with limited capabilities.

Supported Platforms*

*Relationships with OEMs ensure same-day support for new releases.

With so many variables, complexity can become an issue for companies with global deployments across regions, divisions, and departments. 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 admins can customize the user experience for every stakeholder in the organization. And for the IT team, role-based contextual dashboards and access controls allow admins to focus only on the data specific to their job function.

ONE SOLUTION FOR ALL USE CASES

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

- In BYO situations, you can easily deliver the level of privacy employees demand with total separation between work and personal resources.
- With corporate-owned assets, admins can use a stronger supervision mode with advanced capabilities to exert greater control.
- Where multiple employees share a single device—such as shift schedules in a warehouse or retail store—multiuser mode has check-out and check-in functionality so you can deploy settings and apps specific to each user.
- For mobile and line-of-business ruggedized devices in the field, IT can easily provision apps and files and remotely support users.

Recognizing that privacy plays a critical role in modern management, we created Workspace ONE Privacy Guard, designed to manage privacy policies and communicate them proactively to employees to ensure the **best possible employee experience** regardless of the use case. Workspace ONE Privacy Guard also creates a new role in the Workspace ONE console called "Privacy Officer," which provides access to view system settings that affect users and has full editing rights around privacy.

APP MANAGEMENT AND CONSISTENT EMPLOYEE EXPERIENCE

Workspace ONE UEM helps employees work effectively on the go by providing a self-service unified app catalog that is consistent in look, feel, and function across all devices and platforms. The app catalog optimizes productivity with unified one-touch access to all types of apps—native, SaaS, virtual, and web. 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. This consistent, quick, and secure **self-service access to the apps employees need can improve their experience and reduce trouble tickets** and other routine IT support requests.

And in cases where employees do need IT support—for any reason—there's VMware Workspace ONE® Assist. This support solution allows IT to connect remotely to problem devices from the Workspace ONE console and either view or control them to troubleshoot and resolve issues in real time, minimizing downtime. To ease privacy concerns, Workspace ONE Assist notifies employees when their screens are visible, and they can pause remote sessions.

INTELLIGENCE TO ENLIGHTEN AND AUTOMATE

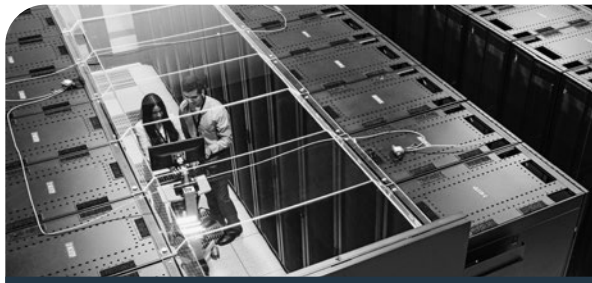
With VMware Workspace ONE® Intelligence, IT teams get **real-time visibility into the entire technology environment** in one place so they can quickly make informed, data-driven decisions. Dashboards can be customized in infinite ways to give admins the data that matters most, and analytics help IT resolve issues that can negatively impact the overall user experience.

But Workspace ONE Intelligence is not just an analytics engine. Using dynamic policy engines, admins can automate routine processes to minimize manual tasks for the IT team. Similarly, they can empower employees with self-service capabilities to reduce support requests. For example, Workspace ONE Intelligence may predictively recommend support services based on data suggesting a battery is about to fail. Or it may proactively take action, such as updating drivers based on data retrieved during a vulnerability scan or optimizing firmware settings to improve performance and stability.

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.

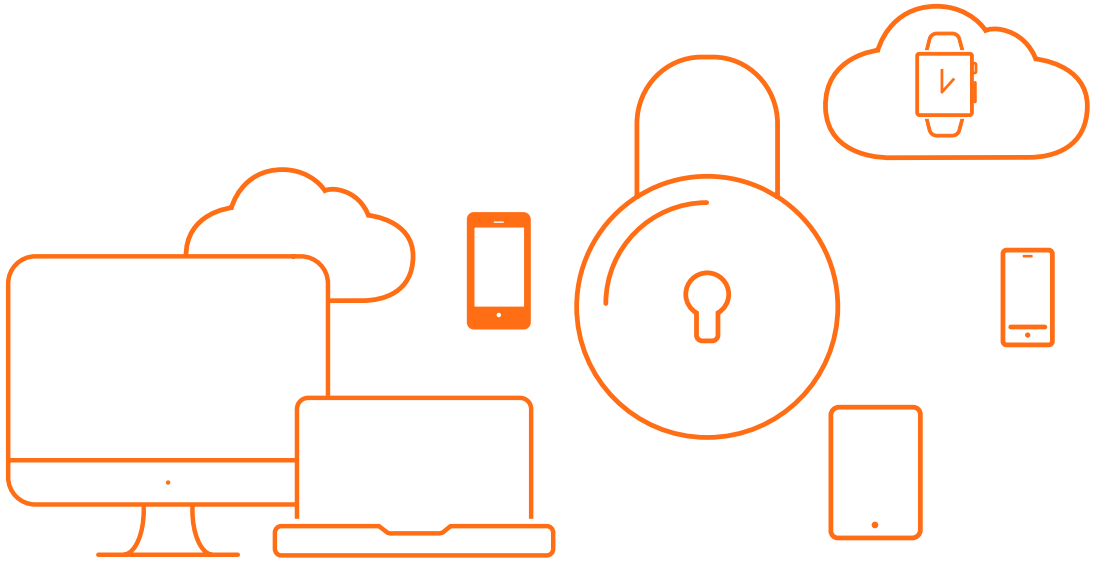
- Built-in features for system settings, data protection, apps, device controls, and more can restrict actions like sharing sensitive data between apps and syncing with unknown devices to **prevent data leakage**. Corporate-owned devices can be supervised for higher levels of control.
- Certificate lifecycle management is a service that can renew certificates automatically or manually.
- VMware Workspace ONE® Tunnel encrypts traffic from individual applications to the back end systems they talk to with “least privilege access” through the VMware Unified Access Gateway™, which proxies and protects the application.



Workspace ONE is certified by a number of security standards organizations so that tightly regulated, security-sensitive companies and institutions can use Workspace ONE UEM to manage their device deployments. Certifications for both on-premises and cloud architectures are kept up to date and prominently displayed on the VMware websites.

ZERO TRUST CONDITIONAL ACCESS

VMware introduced the zero trust security model to accommodate the distinctive needs of the modern decentralized workforce. The VMware Workspace ONE® Access identity layer queries UEM to **determine device compliance** and can also **pick up on user behavioral anomalies** and other attributes to assess the security risk at the moment of login. For example, built-in intelligence will find out if a device has been jailbroken or rooted, if the passcode is insufficient, or if there has been an unusual spike in download activity, among many other things. And through VMware Workspace ONE® Trust Network integrations with the most popular endpoint protection providers like Carbon Black, Netskope, Lookout, and many others, Workspace ONE can enhance its contextual risk assessment with **real-time threat data**.

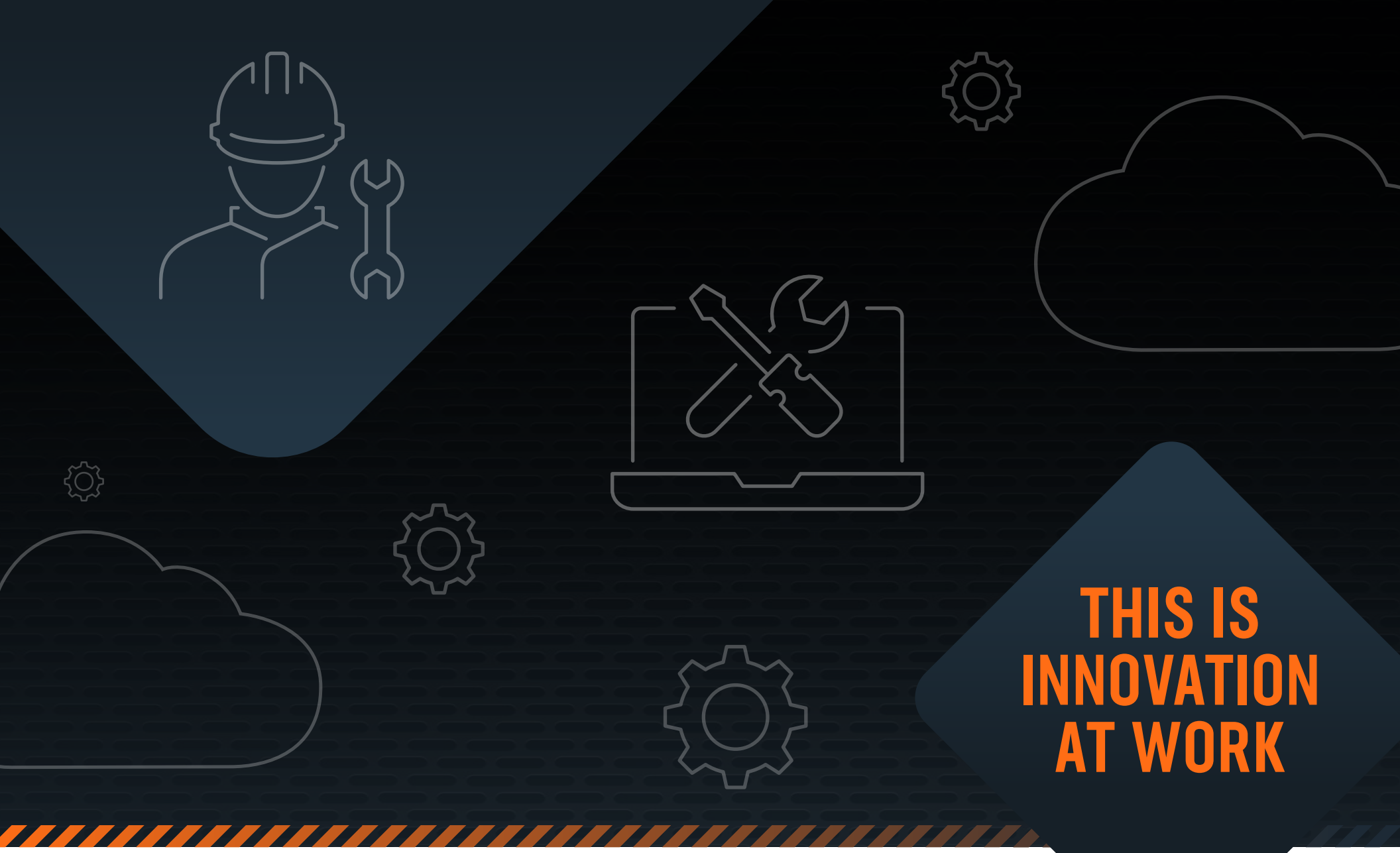


ZERO TRUST CONDITIONAL ACCESS TAKES ACTION

Once the security risk is fully understood, **Workspace ONE can take any of several actions**. If everything checks out, the user can immediately be granted full access to corporate resources. Alternatively, multi-factor authentication can be enforced, or a device that's out of compliance may be automatically remediated. Or, if the risk is unacceptable, access may be denied completely. Lost or completely compromised devices can also be remotely wiped.

Any Endpoint			Any App	
Encryption	**Passcode**	**Compromised**	**Configurations**	**Data and Apps**
AES 256-bit encryption	Complexity	Jailbroken	Whitelist	Office 365 support
Device-level encryption	Expiration	Remote wipe	Blacklist	Sharing permissions
Hardware security	Device and app	Malware	Tethering	Copy / paste
Biometric integration		Conditional access	Settings	Geofencing
			Wi-Fi	Watermark
			TLS	Data backups
			Siri	
			Tunnel	

Before granting access to resources, zero trust security checks devices and context in a multitude of ways and can take actions to remediate deficiencies or even wipe a device.



SHI vmware®