

DELL Technologies / Forum

REAL TRANSFORMATION

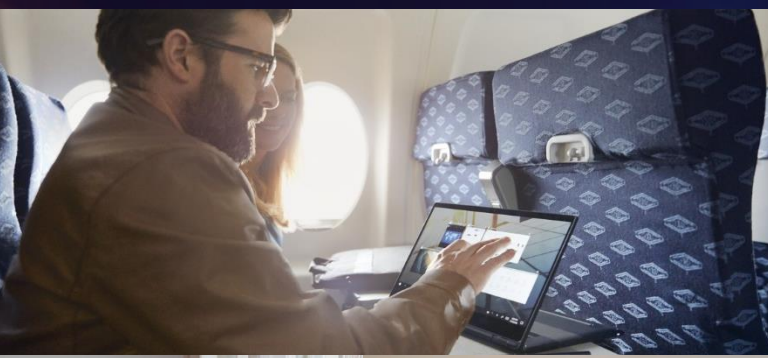
GLOBAL SPONSORS



DELLTechnologies /Forum

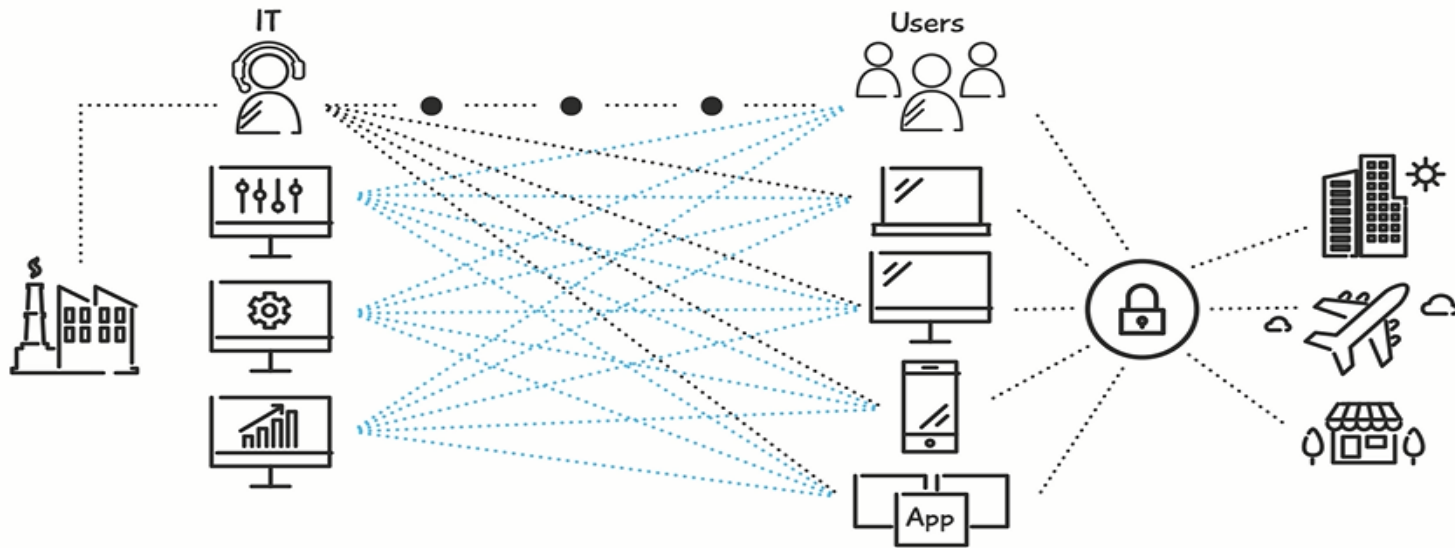
Modern Management on Your Terms

VMware Workspace ONE powering Dell Technologies
Unified Workspace



Technology and end users are transforming the way work gets done.

How do you balance transformation complexities?



Nearly 7 full workdays to deploy 1000 devices

53% of IT leaders are struggling to keep up with the increasing diversity of devices

ITDMs spend up to **25%** of their time **monitoring and troubleshooting**

Dell Technologies Unified Workspace

Powered by VMware Workspace ONE



DEPLOY

Award-winning
Devices

Secureworks®

SECURE

Trusted
Security

vmware
Workspace™ ONE™

MANAGE

Modern
Management

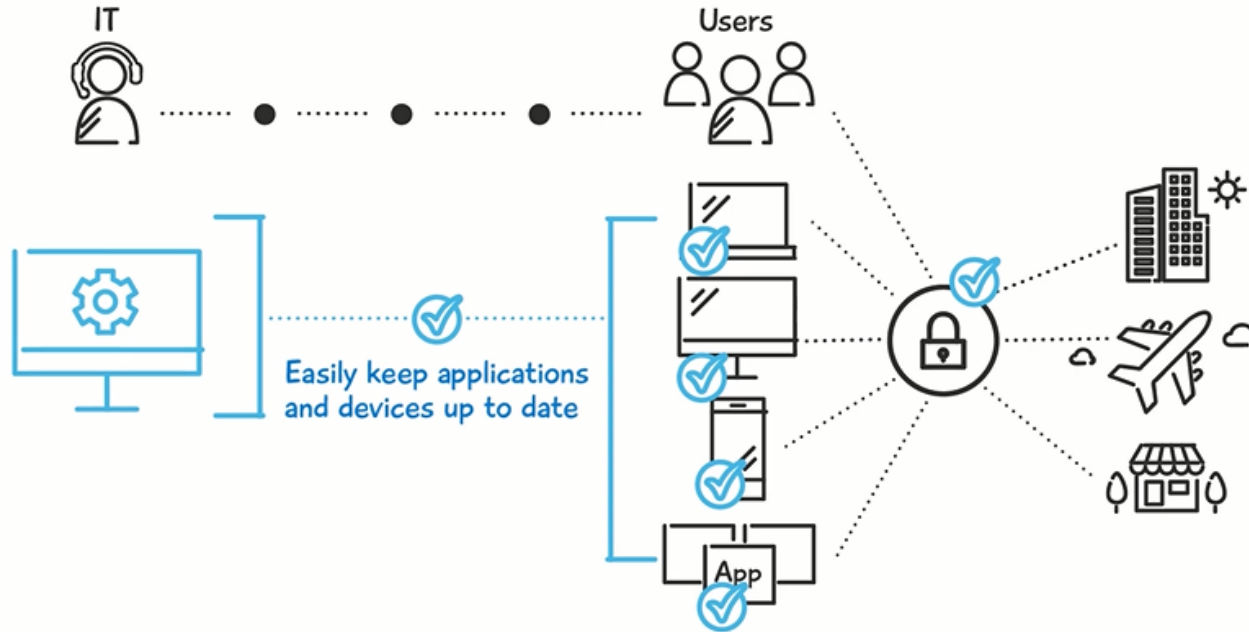


SUPPORT

Services &
Support

Industry's most comprehensive solution to **deploy, secure, manage, support** virtually all devices from the cloud

Modernized Business



Redefine modern deployment and management






Simplification through intelligent automation





Day Zero Productivity

Modern device deployment approaches

Mobile	 <p>iOS</p>	Apple Device Enrollment Program as part of Apple Business/School Manager
	 <p>Android</p>	Google: Android zero-touch enrollment Samsung: Knox Enrollment
Desktop	 <p>macOS</p>	Apple Device Enrollment Program as part of Apple Business/School Manager + VMware Bootstrap Package
	 <p>Windows 10</p>	Microsoft: OOBЕ and Windows Autopilot Dell: Cloud and factory based provisioning
Things	 <p>Non-Traditional Endpoints</p>	Rugged: Sideload Staging, Barcode Enrollment, QR Code, NFC Bump and Android ZTE IoT: QR code for Google Glass Enterprise Edition

ProDeploy in the Unified Workspace

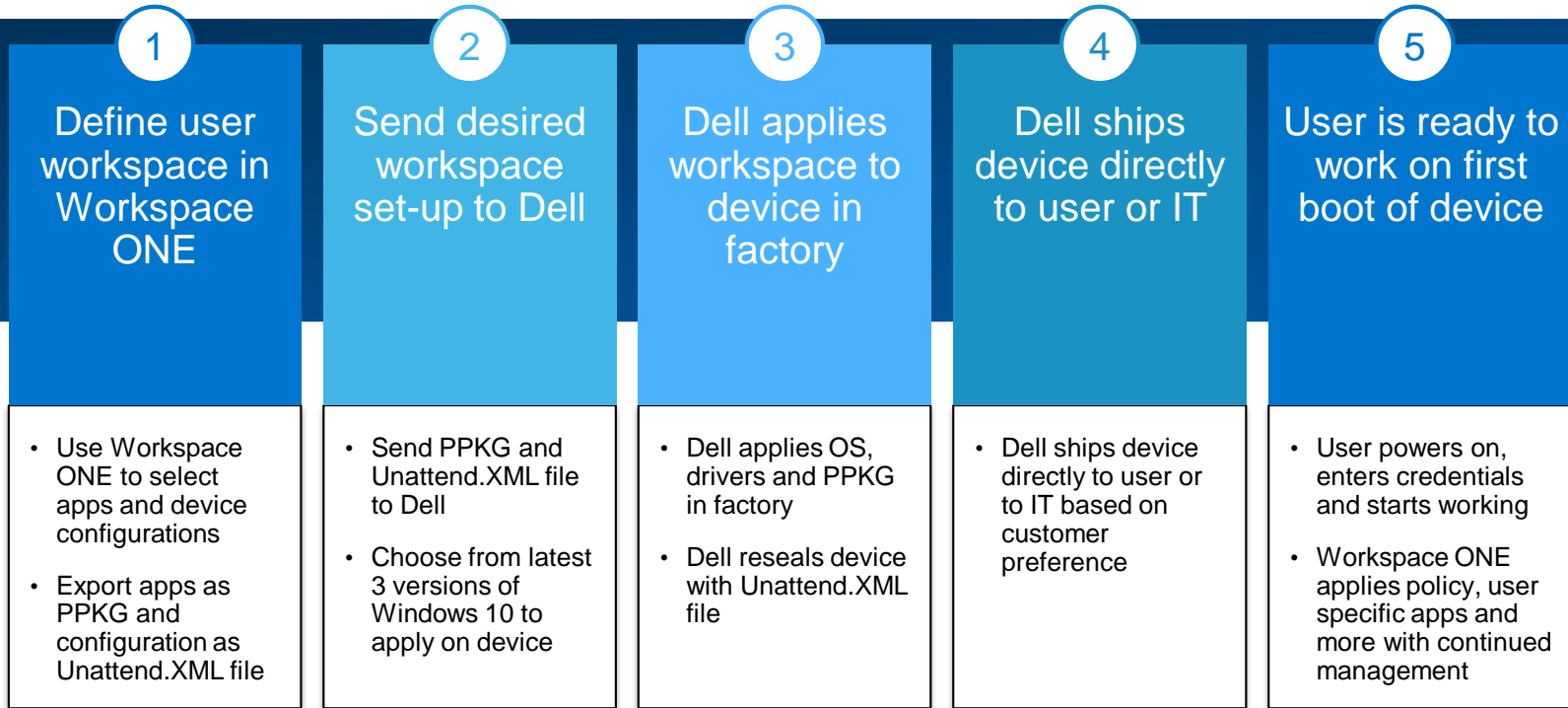


ProDeploy in the Unified Workspace



Provisioning systems with Dell **saves up to nearly a week of IT time per 1,000 devices deployed**

Five steps to day-one productivity on new Dell PC's

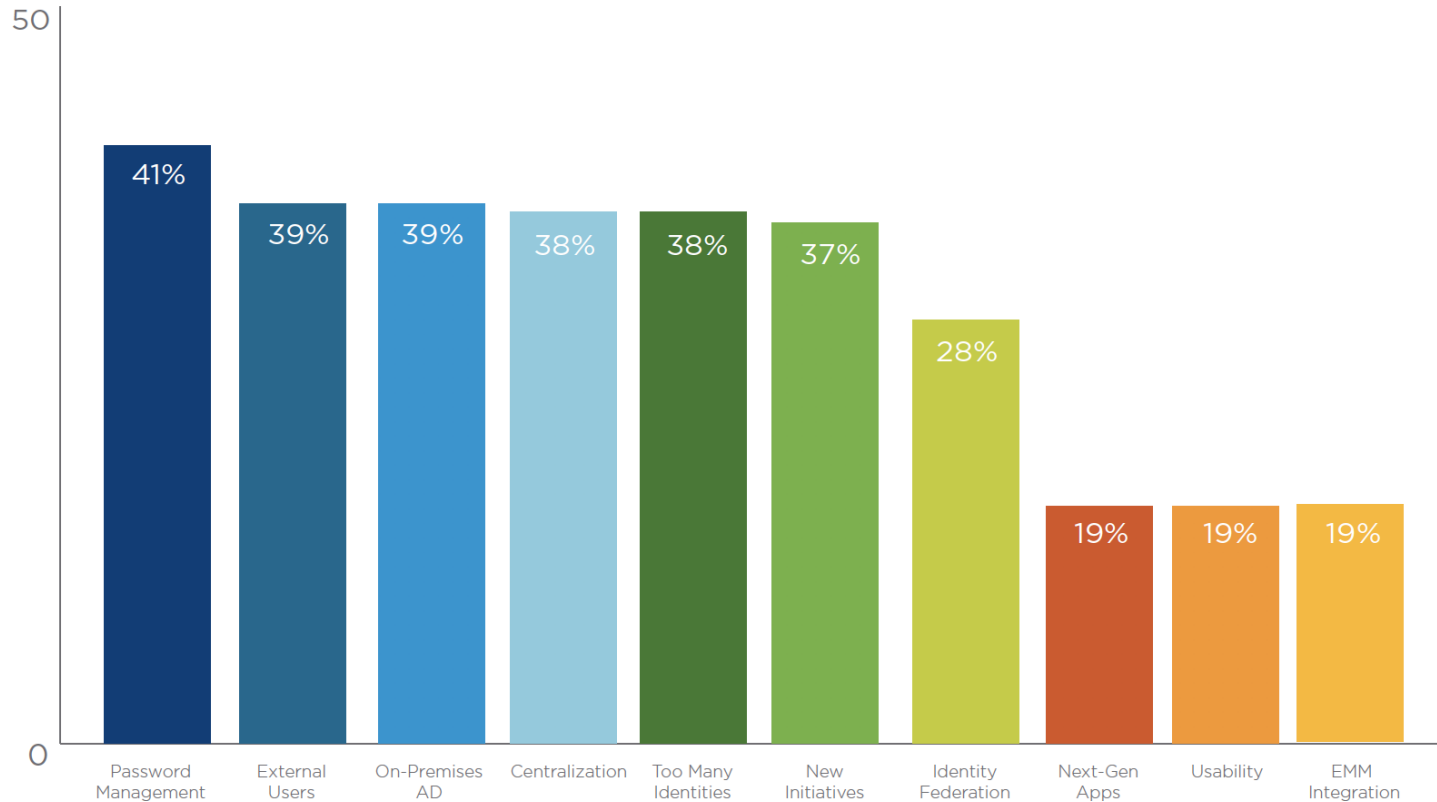




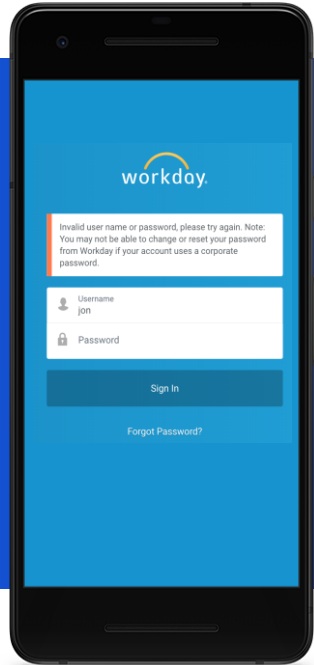
Self Service Empowerment

Employee Experience Challenges with App Access

What are the main challenges your company faces related to identity management today?



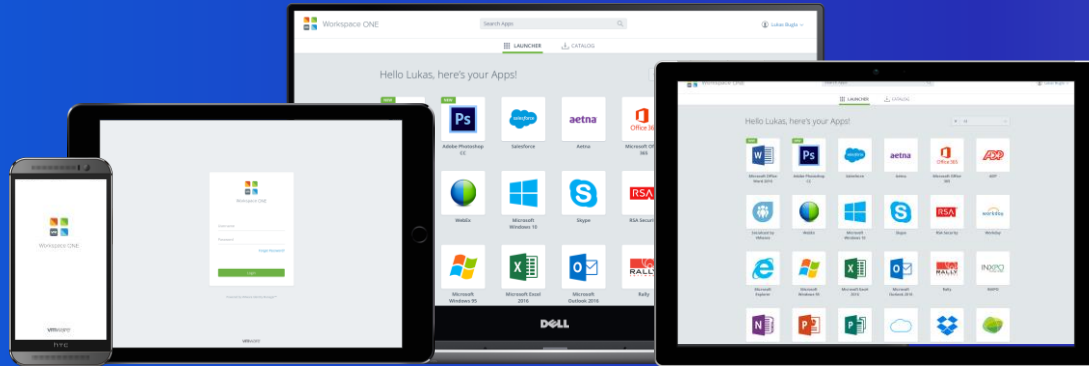
The Disjointed App Access Experience



Issues employees face with no unified app catalog:

- Disparate locations to access various types of apps
- Wait hours/days to install new apps (IT often must login as admin)
- Submit tickets for AD lockouts/password resets
- Poor security practices with no SSO (e.g. sticky notes with passwords)
- Poor adoption of enterprise apps that make employees more productive

Empower Employees with Self Service



- Unified Catalog to for easy access to any app on any device
- No more remembering passwords for various apps or logging into VPN
- Seamlessly install additional apps with no IT intervention
- Self service password reset and BitLocker recovery



Always Up to Date and Actionable Insights



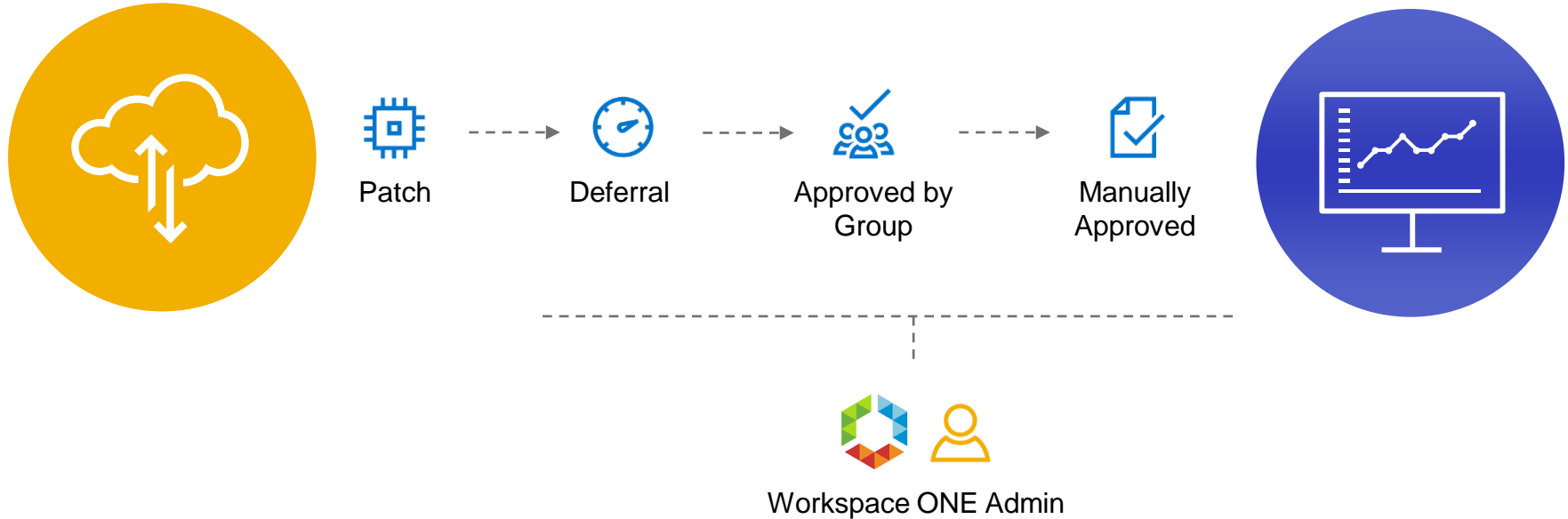
1 in 10

Enterprises take **a year or more to deploy Windows patches** affecting most or all of their endpoints

“...average **time to identify incidents over 200 days** and the average **time to contain incidents over 60 days**”

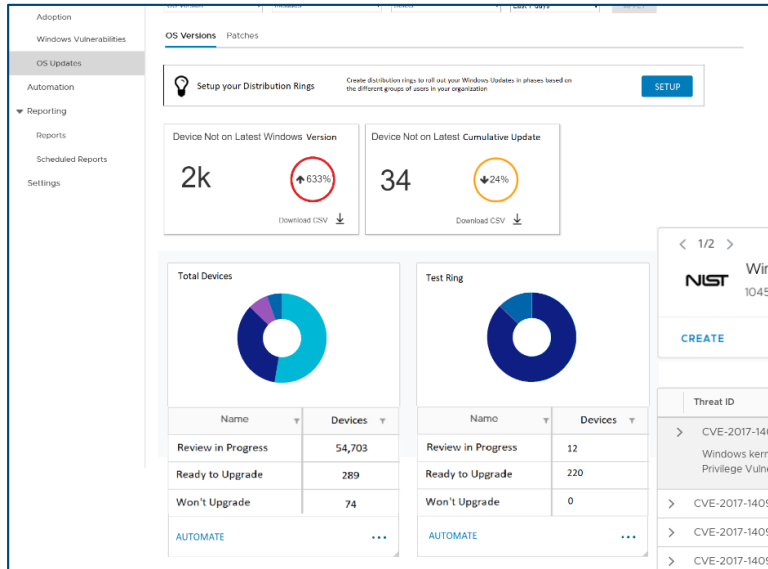
Flexibly Deploy Windows Updates

Supports WSUS, Distribution Rings or Device Update Readiness to reduce complexity with capability testing



Keep PCs protected with intelligence and automation

Always-up-to-date patching features risk scoring, analytics & automation



Windows 10 Vulnerability Detected (0.3 High)

1045 Devices with KB4048954 not equal to "Installed." CVE-2017-11847

Threat ID	CVE Score	Severity	Impact
CVE-2017-140987	0.3 High	High	899
Windows kernel in version 1709 allows attacker to run arbitrary code in kernel mode. Install programs aka "Windows Kernel Elevation of Privilege Vulnerability."			
CVE-2017-140987	0.3 High	High	899
CVE-2017-140987	0.3 High	High	899
CVE-2017-140987	0.3 High	High	899
CVE-2017-140987	0.3 High	High	899
CVE-2017-140987	0.3 High	High	899
CVE-2017-140987	0.3 High	High	899
CVE-2017-140987	0.3 High	High	899

Predictive patching based on device risk (CVE score), reduces time to secure OS

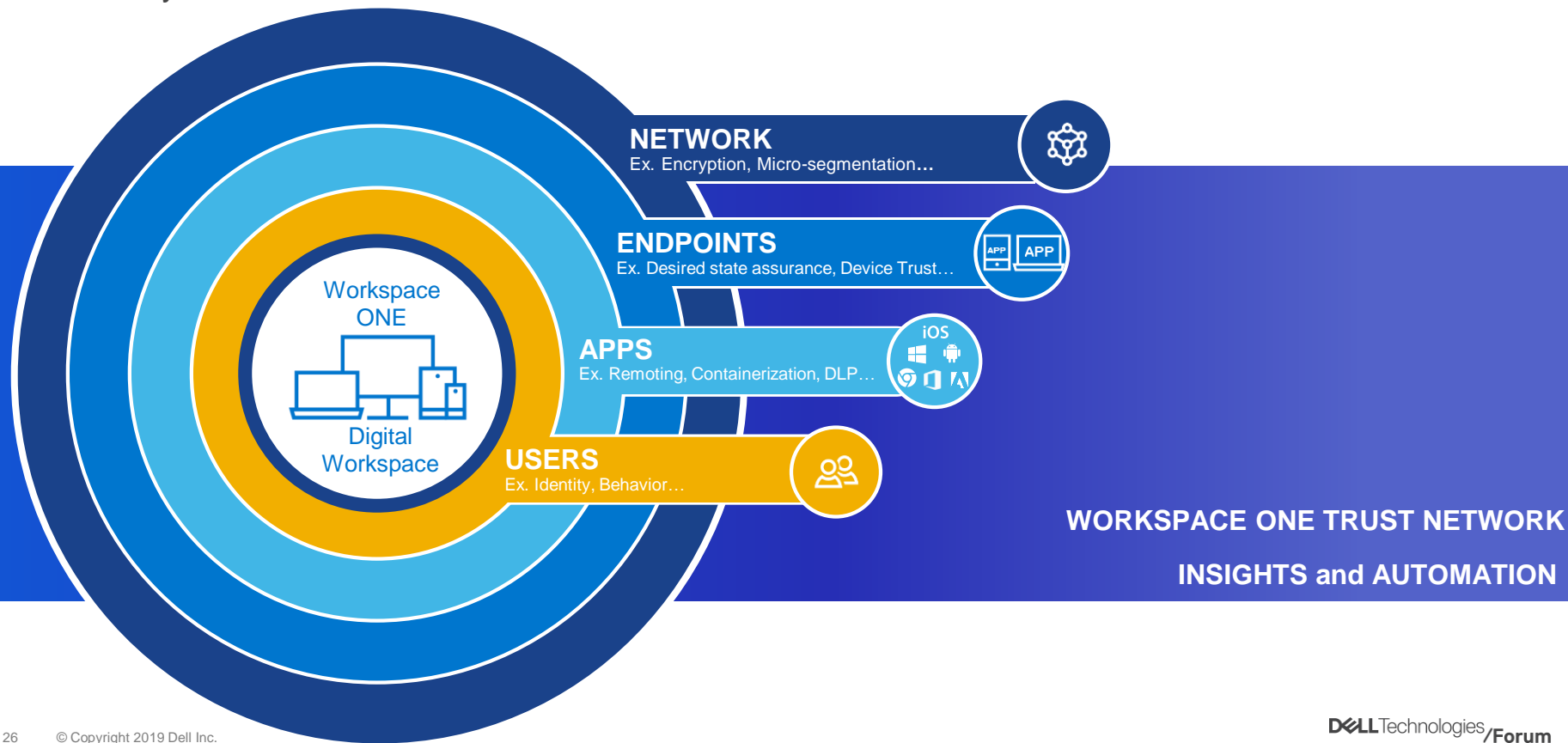
Business steady machines lower downtime and keep users productive



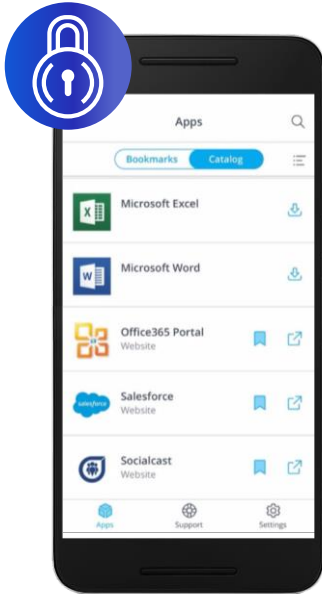
Zero Trust Security

Securing the digital workspace with Workspace ONE

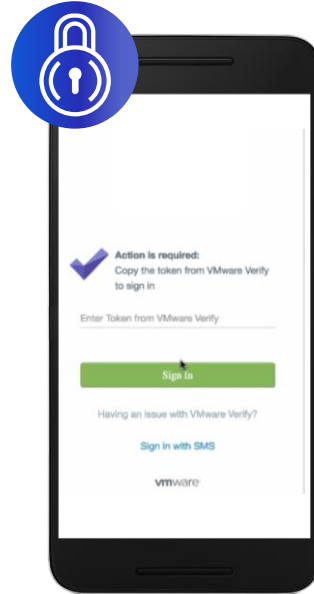
Proactively secure all attack vectors



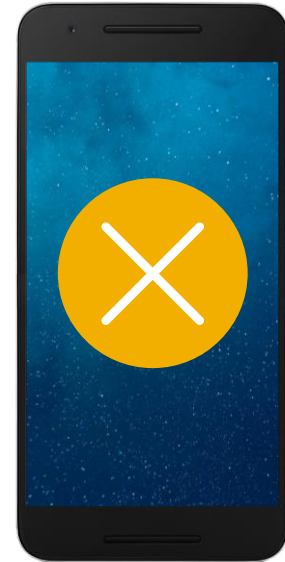
Zero Trust Conditional Access to Secure Corporate Data



Managed Device
& In Network Scope

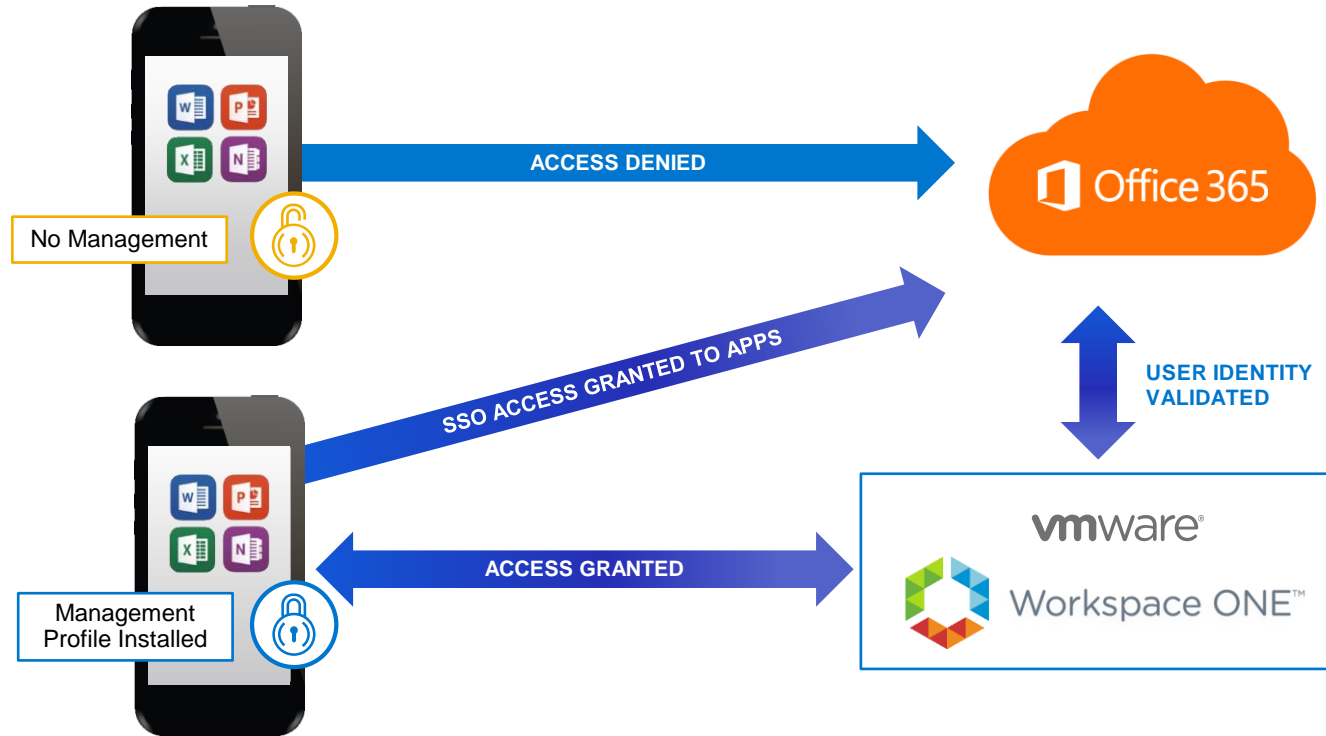


Managed Device
& Out of Network Scope



Jail Broken Device
& Out of Network Scope

Zero Trust Conditional Access Use Case



Zero Trust for Dell devices running Windows 10

Device: BIOS configuration and updates, and now BIOS verification

Operating System: Windows 10 Health Attestation

Users: Identity

Applications: Certificates and Application Guard

Network: Trust Network, per app VPN + NSX and Secureworks

All backed by automated compliance and conditional access



Leverage Sensors for Better Visibility and Compliance

Query any system attribute for visibility and compliance enforcement

The screenshot displays the Workspace ONE UEM Scripting interface. The main view shows a table of sensors with columns for Name, Platform, Trigger Type, Data Type, Assignment, and Success Rate. Three sensors are listed: Battery Status (MacOS, Login, Type, 100/200 return), Adobe Reg Version (Windows, Logout, Type, 100/200 return), and App Process ID (Windows, Schedule 1 hour, Type, 100/200 return). A configuration dialog is open in the foreground, showing the 'Define Query' step. The dialog includes a 'Script/Command' field with a code editor containing the following script:

```
#!/bin/bash
#ScriptName: #APPID
#Platform: #OS
#Data Type: #APPID, #APPID, #APPID, #APPID
#Trigger Type: #APPID
#Success Rate: #APPID
}

#Action: #APPID
#ScriptName: #APPID
#Platform: #OS
#Data Type: #APPID, #APPID, #APPID, #APPID
#Trigger Type: #APPID
#Success Rate: #APPID
}

#Assignment: #APPID
#ScriptName: #APPID
#Platform: #OS
#Data Type: #APPID, #APPID, #APPID, #APPID
```

The dialog also features 'UPLOAD' and 'IMPORT FROM VWARE' buttons, and 'CANCEL' and 'NEXT' buttons at the bottom.

Dynamic targeting of inventory attribute from the cloud

Automated local compliance enforcement eliminates policy drift

Visit TechZone & Test Drive for More Information

Test Drive to Try Yourself
TestDrive.VMware.com

TechZone for Technical Resources
TechZone.VMware.com

Support Today's Increasingly Mobile, Dynamic Workforce

Ready to Use Experiences

Get started exploring VMware products right away on a completely set-up and integrated environment.

vmware
Workspace ONE

VMware Workspace ONE powered by AirWatch, is a simple, secure, and intelligence driven enterprise platform that delivers and manages any app on any device.

LAUNCH

vmware
Workspace ONE UEM

Workspace ONE Unified Endpoint Management (UEM) is a leading technology that powers desktops and mobile devices. It includes full device management, app-level management for BYOD and much more.

Disable Product

LAUNCH

vmware DIGITAL WORKSPACE TECH ZONE

Start - Workspace ONE Horizon Tools Blog Log in

Advanced Search

Modernizing Windows 10 Management: VMware Workspace ONE Operational Tutorial

VMware Workspace ONE UEM 9.5 and later
VMware Identity Manager 3.2 and later

Overview

Introduction

VMware provides this operational tutorial to help you with your VMware Workspace ONE environment. This tutorial consists of a series of exercises that walk through transitioning (co-managing) or transforming (replacing) Microsoft System Center Configuration Manager (SCCM) to VMware Workspace ONE UEM (unified endpoint management).

Audience

This operational tutorial is for PC lifecycle management (PCLM) administrators and Workspace ONE IT administrators. Familiarity with networking and storage in a virtual environment is assumed, including Active Directory, identity management, and directory services. Knowledge of additional technologies such as VMware Identity Manager and VMware Workspace ONE UEM is also helpful.

- Overview
- Initial Configurations
- Enabling Workspace ONE AirLift
- Migrating Devices and Users from SCCM
- Migrating Applications from SCCM
- Migrating GPOs from SCCM
- Managing CSPs Using VMware Policy Builder
- Removing the SCCM Client
- Summary and Additional Resources

f in t e

Any Questions?

DELL Technologies



DELL EMC

Pivotal

RSA

Secureworks

virtustream

vmware