

DELLTechnologies /Forum

REAL

TRANSFORMATION

GLOBAL SPONSORS

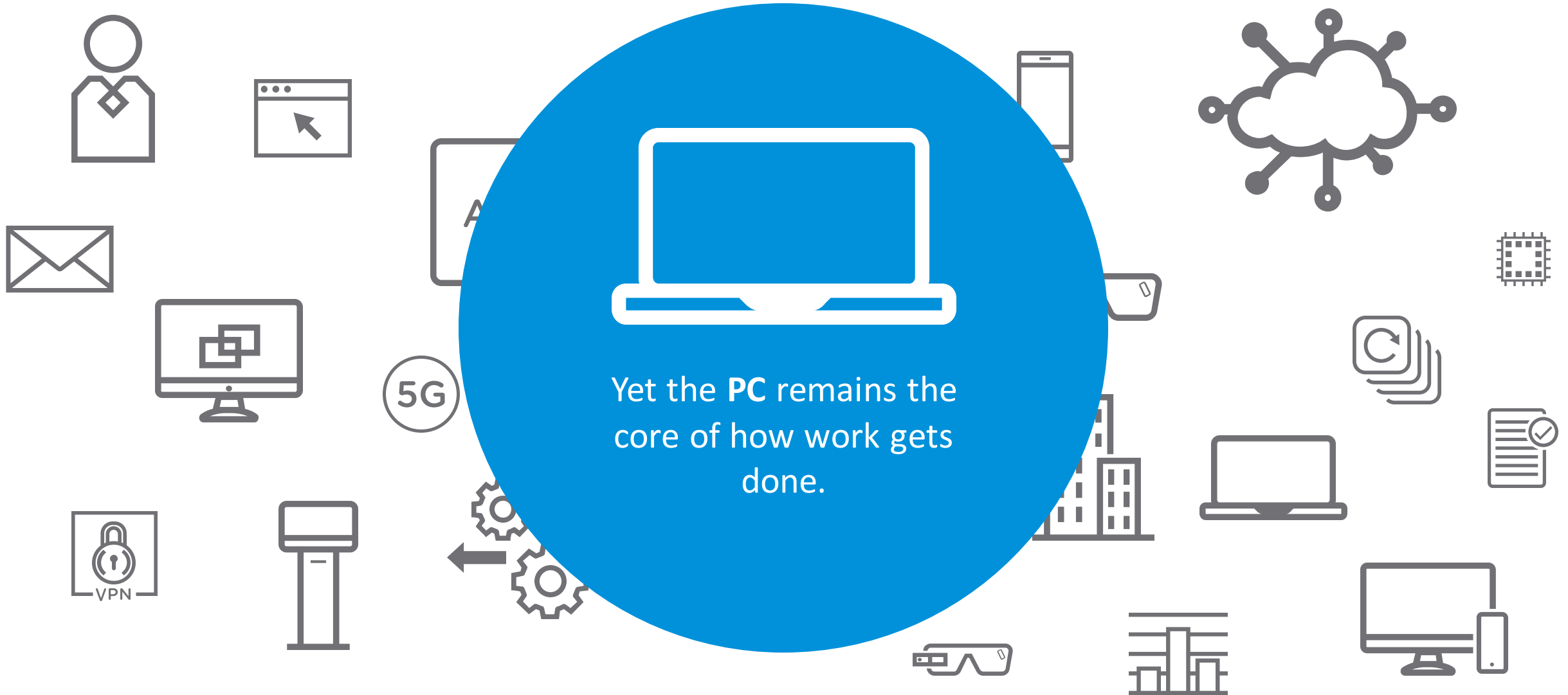


DELLTechnologies / **Forum**

The Intelligence-Driven Digital Workspace Platform

Cristian RADU, Senior SE VMware

The Way People Work is Changing at a Dramatic Pace



Today's Reality is a Barrier to Digital Workspace Success

Traditional PC management hasn't evolved for the modern workforce



Traditional PC Management Hasn't Evolved for This Modern Workforce

Legacy client-server tools negatively impact your business



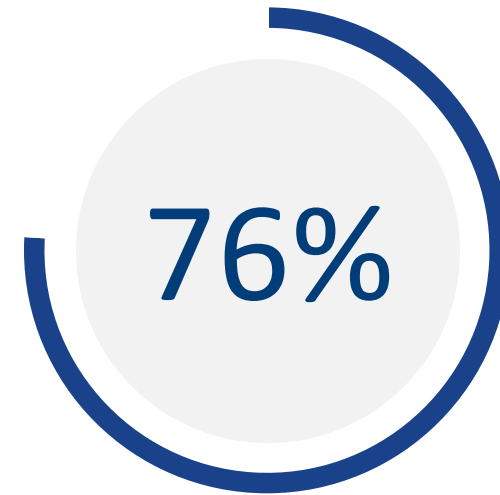
Increased
Cost

Cost of post-deployment PC
management and support



Compromised
Security

Breaches originate at
endpoints



Poor User
Experience

Don't have apps from IT to get work
done



With Windows 10, Microsoft Enables
“Modern Management” of PCs

Integrated MDM
Framework

Simplified Device
Onboarding

Cloud-based
Management

Modern Management Benefits vs. Traditional PCLM Approaches



TRADITIONAL



DEPLOYMENT

High-touch



CONFIGURATION

On-network only



PATCHING

Takes months to patch



APP MANAGEMENT

Resource intensive



SECURITY

Poor compliance



MODERN

BUILT FOR THE
MODERN
WORKFORCE

Out-of-box for day one productivity

Over-the-air, across any network

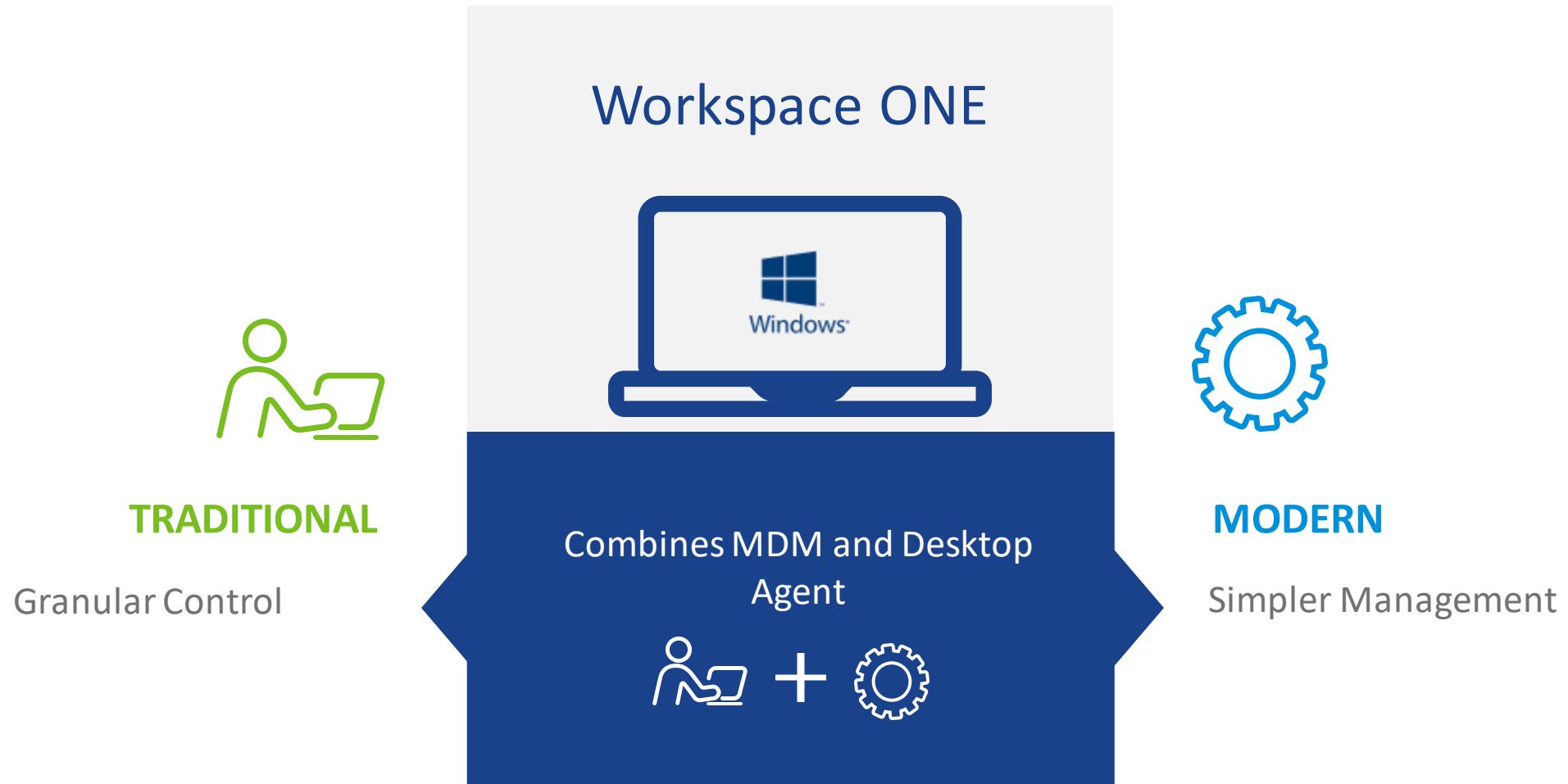
From the cloud in minutes

Cloud-scale with zero CapEx

Real-time detection and remediation

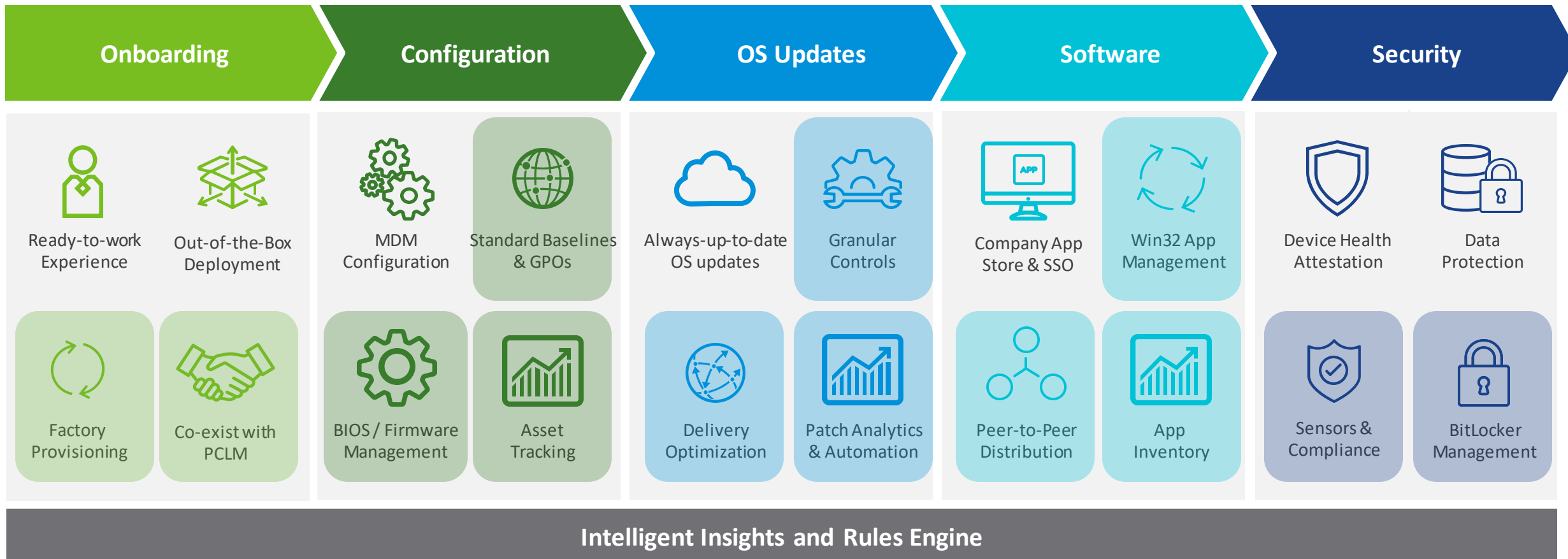
Workspace ONE Uniquely Delivers Full PC Management from Cloud

Combines native MDM simplicity with traditional management control to meet critical PC management needs



Taking a leap beyond PCLM With Best-in-Class PC Lifecycle Transformation

The **only complete Windows 10 modern management** solution to transform the way IT manages PCs



Benefits of Modern Management with Workspace ONE

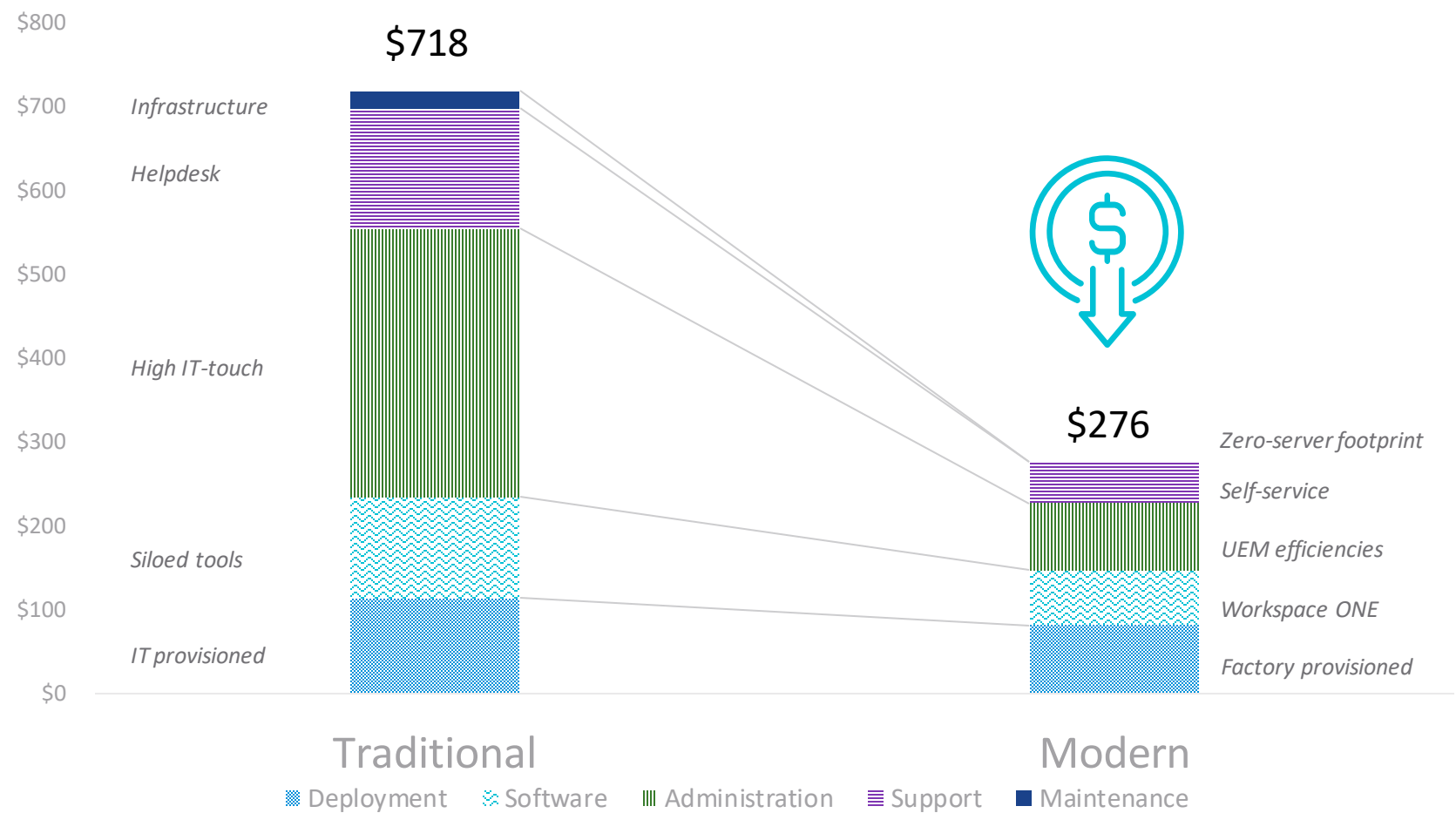
The New Norm to Address Cost and Complexity



Workspace ONE Drives TCO Savings for Organizations

Significant IT and user efficiencies for Windows 10 Management

Note: All costs per device per year. Deployment costs accrued assuming a 3 year refresh cycle.



2/3rd

Cost Reduction

Silo-less management at reduced TCO

VMware Named a Leader in the IDC MarketScape for Worldwide Unified Endpoint Management Software 2018

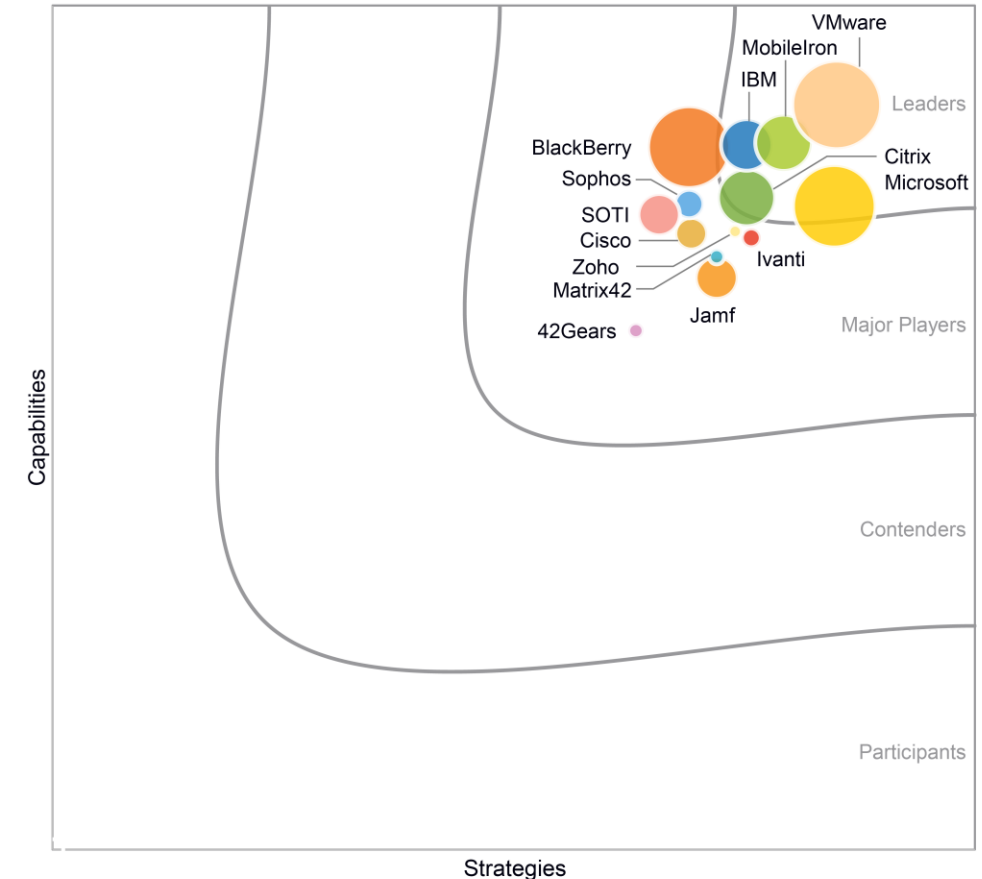
VMware has been recognized for:

- Workspace ONE UEM having among the broadest set of features for managing Windows 10, as well as pre-Windows 10 Microsoft PC deployments, Mac, and Chromebook.
- Support for Win32 app distribution, GPO policy enforcement, and other Windows-centric features for PCLM migration to modern management
- The ability to provide configuration and security settings across a range of Dell devices, including Dell Chromebooks, and BIOS management on Dell PCs.

SOURCE: "IDC MarketScape: Worldwide Unified Endpoint Management Software 2018 Vendor Assessment" by Phil Hochmuth, July 2018 IDC # US43294318

IDC MarketScape vendor analysis model is designed to provide an overview of the competitive fitness of ICT suppliers in a given market. The research methodology utilizes a rigorous scoring methodology based on both qualitative and quantitative criteria that results in a single graphical illustration of each vendor's position within a given market. The Capabilities score measures vendor product, go-to-market and business execution in the short-term. The Strategy score measures alignment of vendor strategies with customer requirements in a 3-5-year timeframe. Vendor market share is represented by the size of the circles. Vendor year-over-year growth rate relative to the given market is indicated by a plus, neutral or minus next to the vendor name.

IDC MarketScape Unified Endpoint Management Software 2018



Source: IDC, 2018

Eliminating Barriers to Modern Management Adoption

Transforming Every Phase of PC Management

#1: Reimagine Employee Onboarding

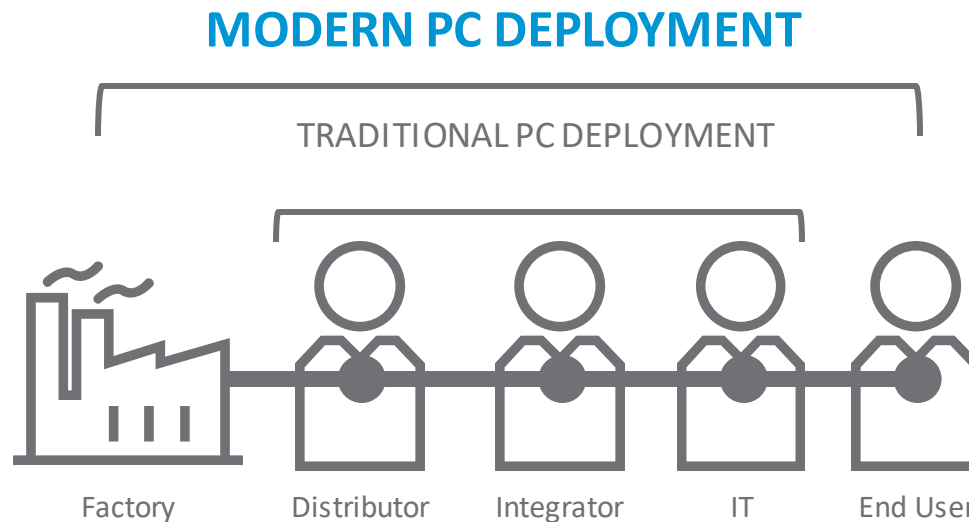
Zero-touch deployment for day one user productivity

Dell Provisioning for VMware Workspace ONE

Eliminate manual PC setup with out-of-box deployment



ONBOARDING



Zero-touch onboarding for day one
user productivity

Turnkey Provisioning

Ready-to-Work Experience

Zero IT Touch PC Restore

Trusted Software Authority

Learn more: https://i.dell.com/sites/csdocuments/Learn_Docs/en/provisioning-for-workspace-one-datasheet-en.pdf

“Provisioning systems with Dell
**saves more than a week of IT
time per 1,000 devices
deployed.**”

A Principled Technologies report; Jan 2019





Onboarding Options to Meet Your IT Needs

Most onboarding options to save cost; drive day zero user productivity



ONBOARDING

IT Driven



Co-managed

With or without AD domain join



Provisioning

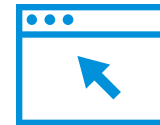
Image based, staged or at runtime



Factory Service

Pre-configured device from factory to user

User Driven



Agent

One-click, self-service onboarding



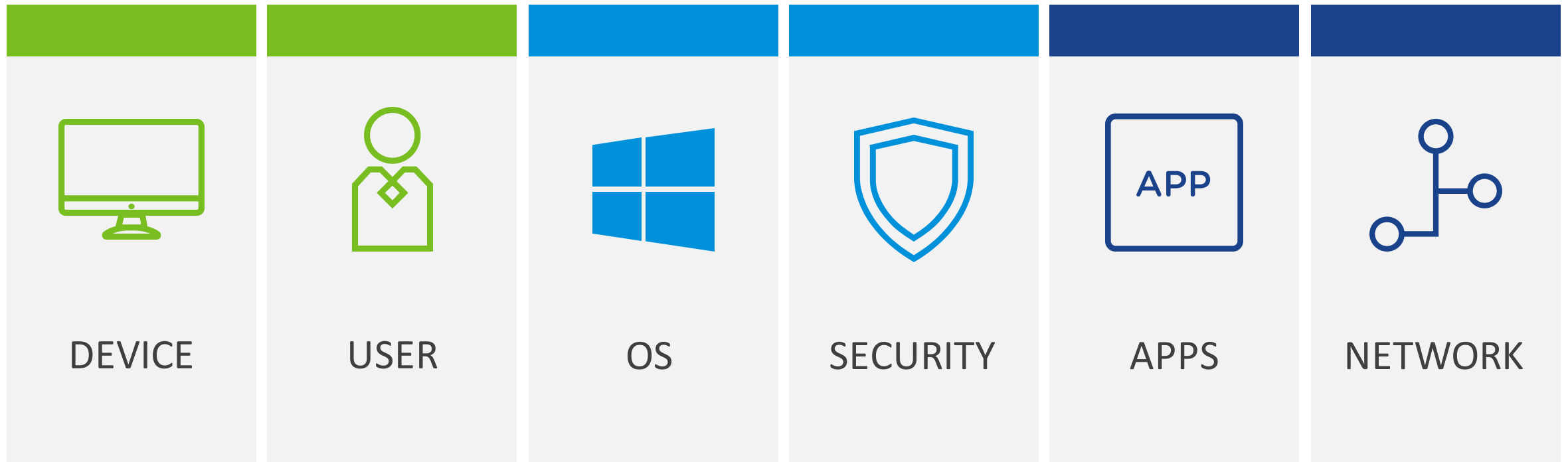
Out-of-the-box

Cloud domain join including Autopilot

#2: Real-time Configuration

100% Policy Management from Cloud

Thousands of Configuration Settings to Sift Through When Managing Windows



Configure Policy Using Industry Standard Security Baselines

Baselines provide security templates from trusted third parties for turnkey and 100% policy compliance, whether MDM or GPO

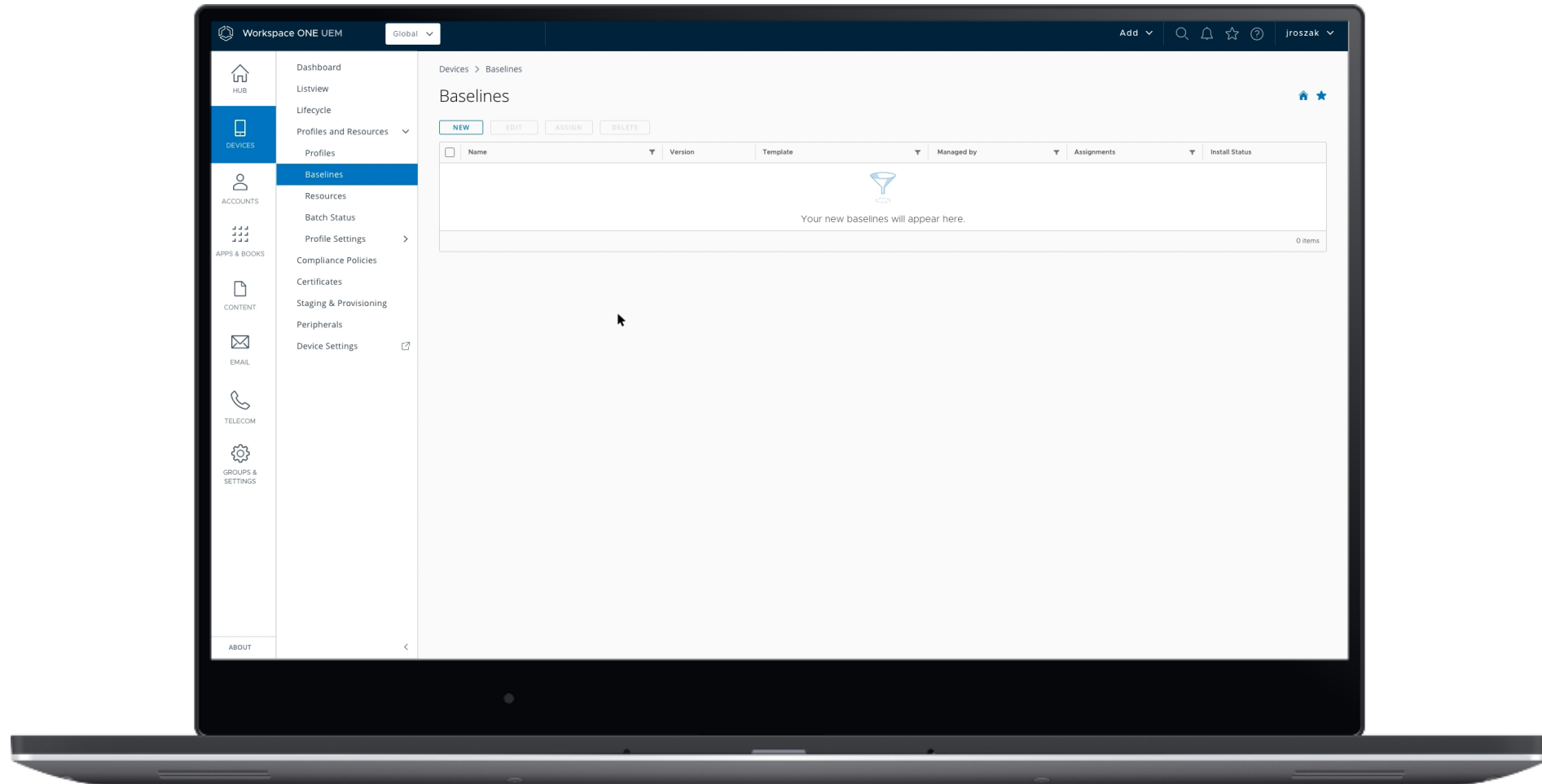


The screenshot shows the 'New Baseline' configuration window. The 'Choose Template' step is active, showing two options: 'Windows 10 Security Baseline' and 'CIS Microsoft Windows 10 Enterprise Benchmarks'. The 'Customize' step is also shown, displaying a tree view of policy categories (Computer Configuration, User Configuration) and a 'Data Collection and Preview Builder' section with various settings like 'Enforce password history', 'Maximum password age', and 'Password must meet complex requirements'.

Hardened PC with **industry standard** security baselines (e.g. CIS, MSFT)

Simpler, **over-the-air** GPO configuration across any device, anywhere in minutes

Customizable for customers' unique InfoSec needs and **100% GPO coverage**

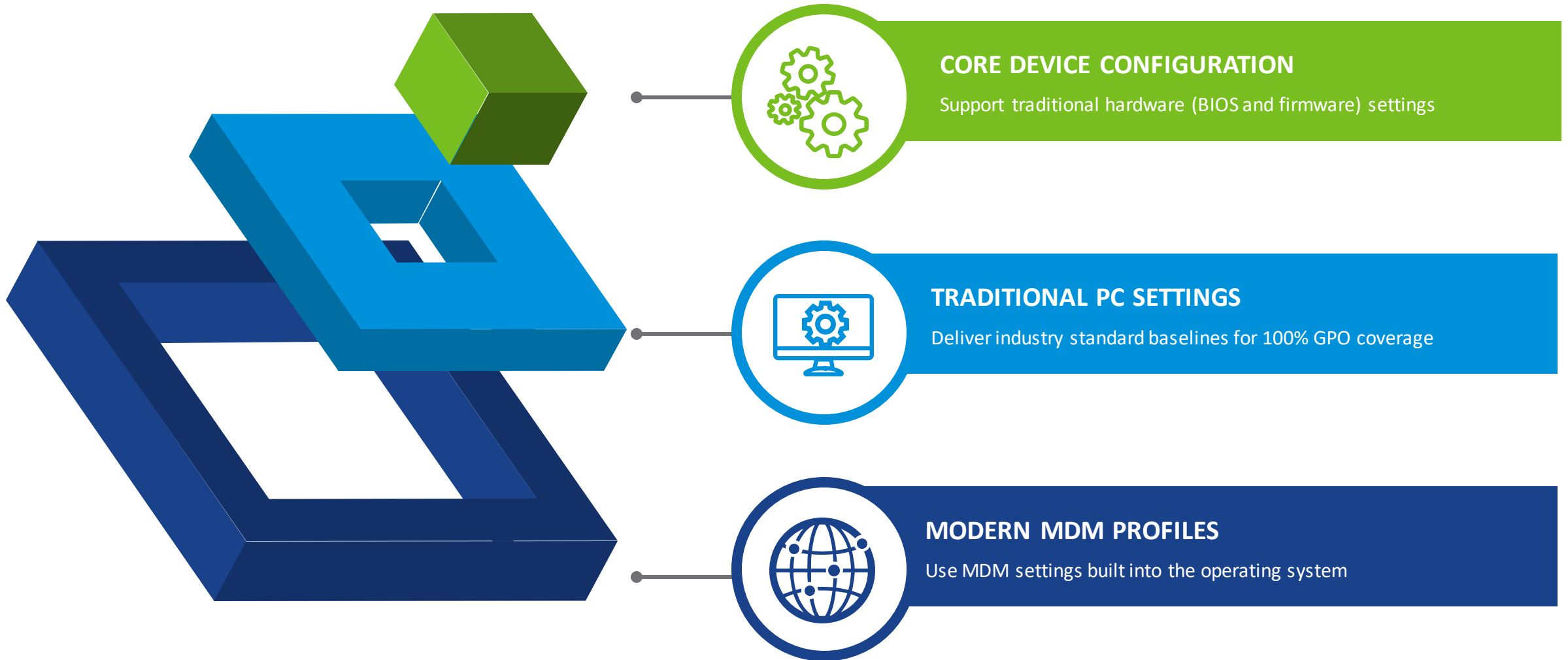


Cloud-Based Configuration Across Any Network

Configure and update settings over the air, across the PC Stack



CONFIGURATION



#3: Always Up-to-date Patching

100% Policy Management from Cloud

A donut chart with a dark blue outer ring and a light blue inner ring. The text "1 in 10" is centered in the white space of the donut chart.

1 in 10

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

Patching is a pain point, especially for large companies.



VMWARE
CUSTOMER
ADVOCACY

Windows as a Service Requires a New Architecture

Semi-annual upgrades and large cumulative updates delivered frequently



OS PATCH
MANAGEMENT



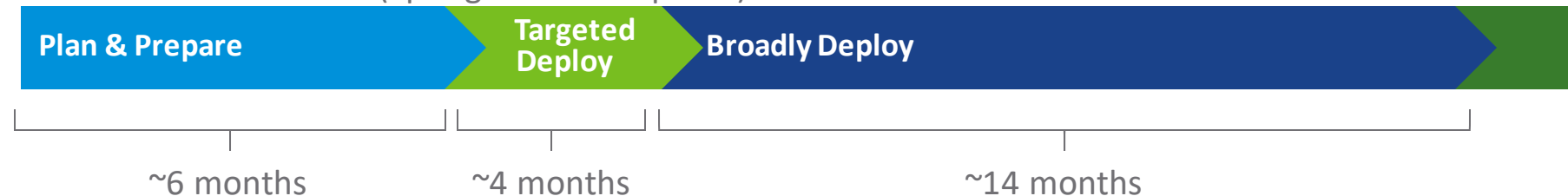
Windows 10 1703 (Creators Update)



Windows 10 1709 (Fall Creators Update)



Windows 10 1803 (Spring Creators Update)

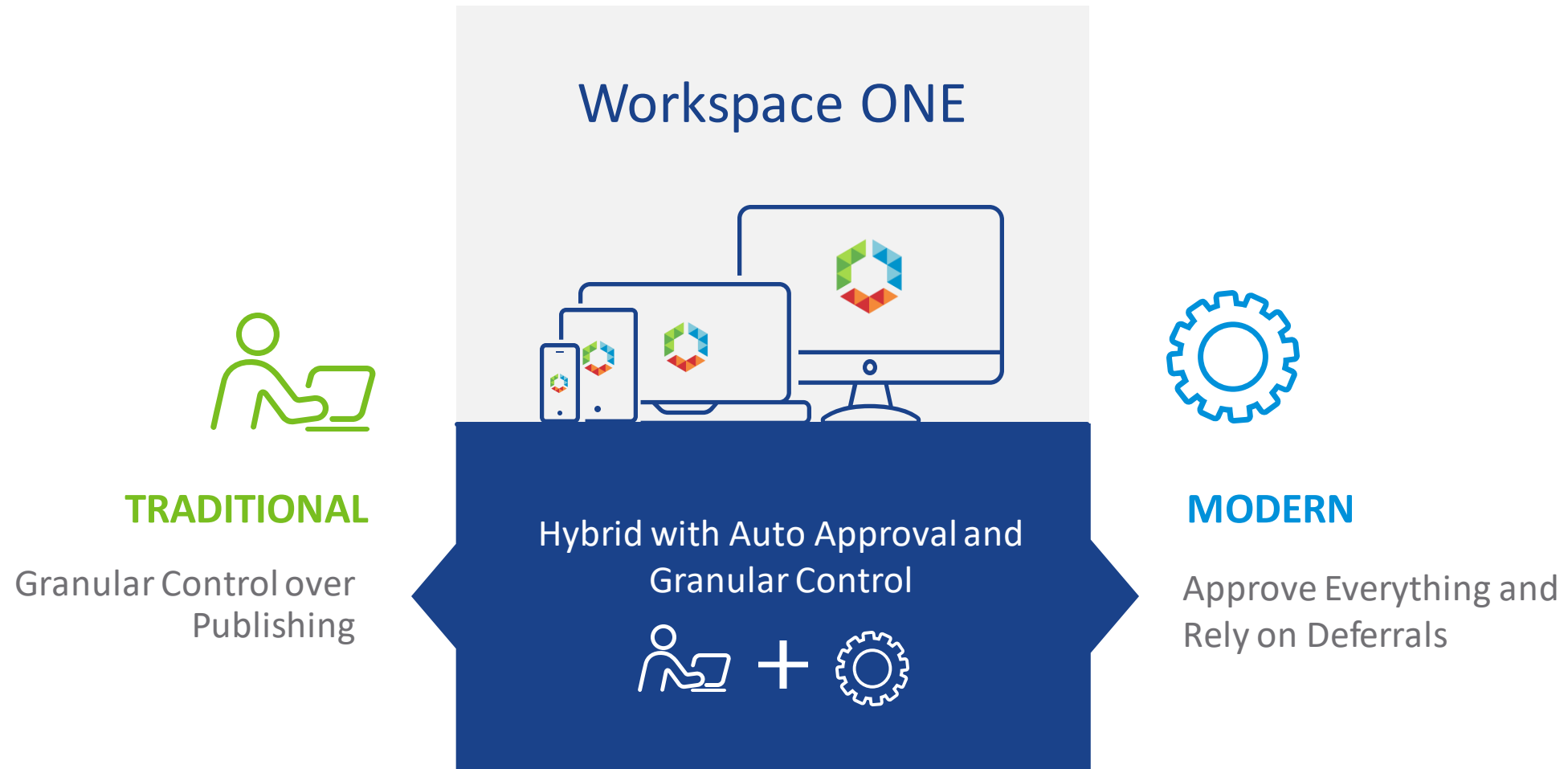


Hybrid of Granular Control and Intelligent Automation

Ensure patch compliance across any network in minutes, not months!



OS PATCH
MANAGEMENT

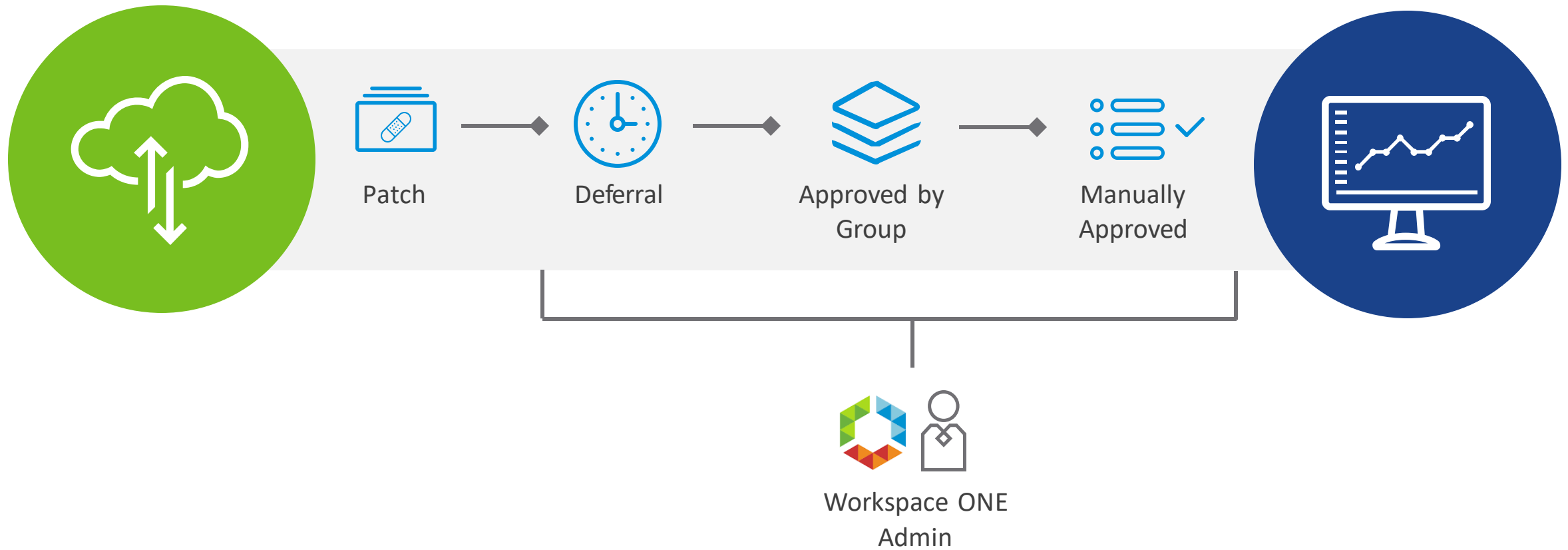


Granular Control Over Updates Publishing

Evolution from a test-first approach to a publish-first approach



OS PATCH
MANAGEMENT

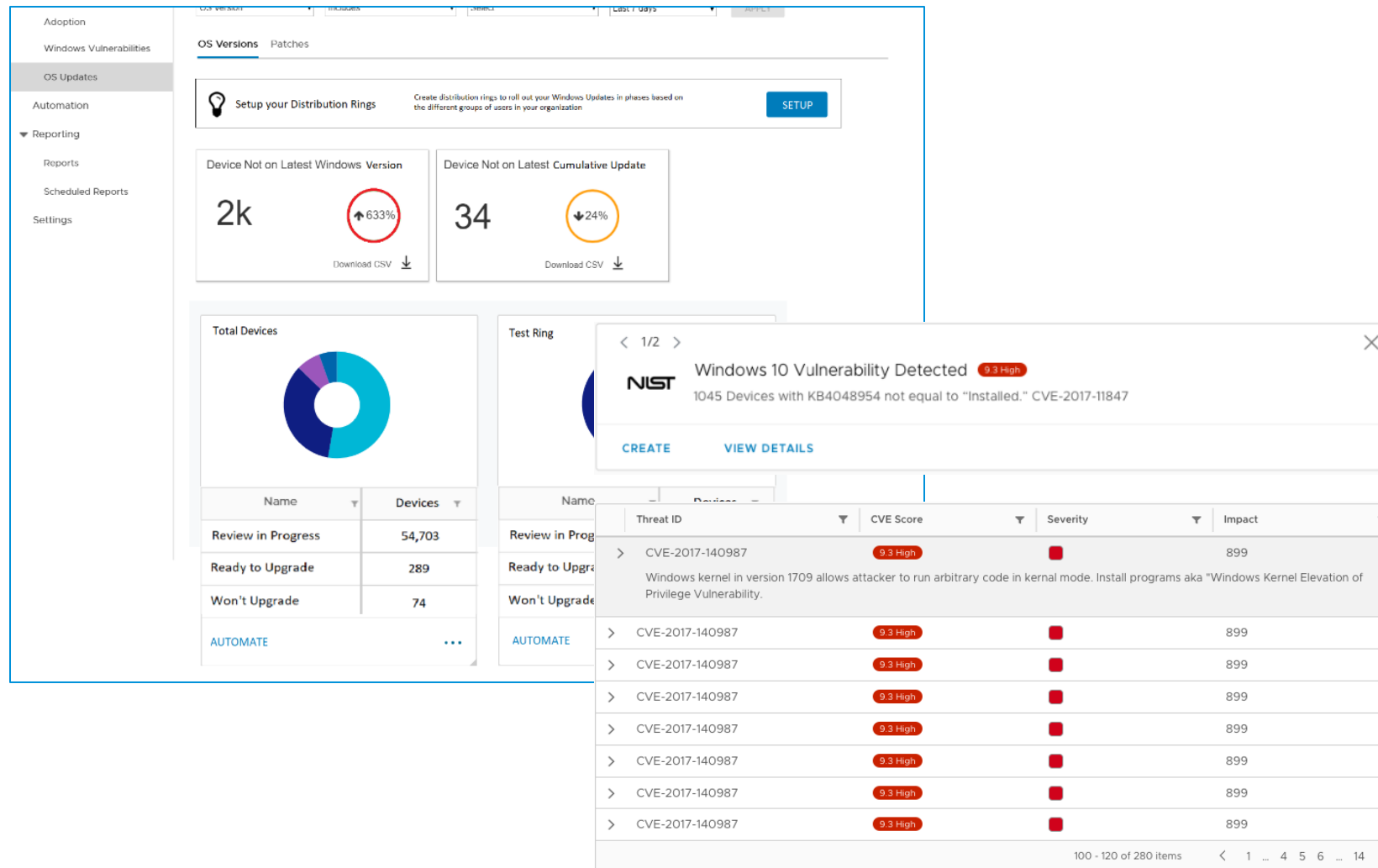


New! Keep PCs Protected with Intelligence and Automation

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



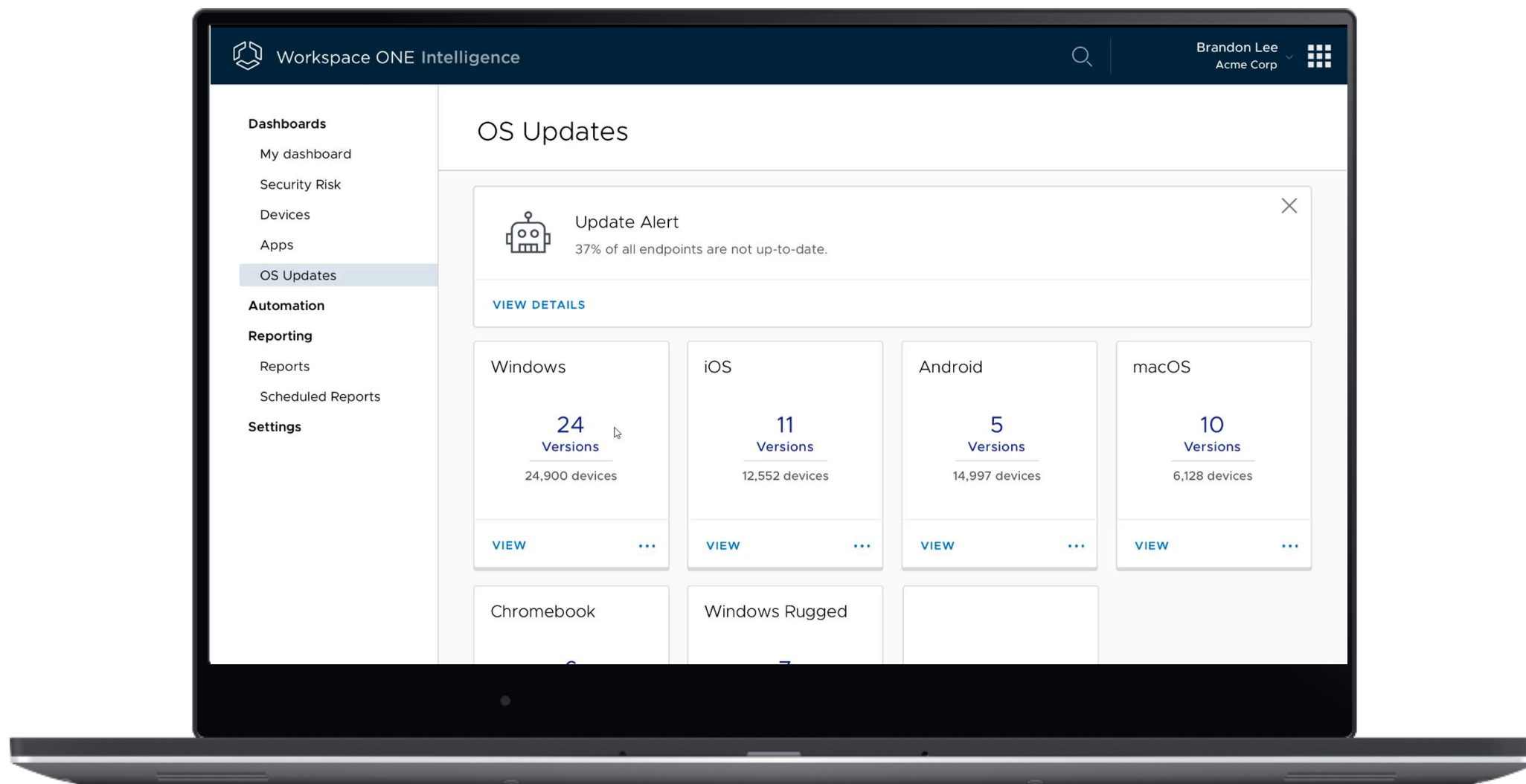
OS PATCH
MANAGEMENT



Update readiness to break free from constant servicing and testing cycles

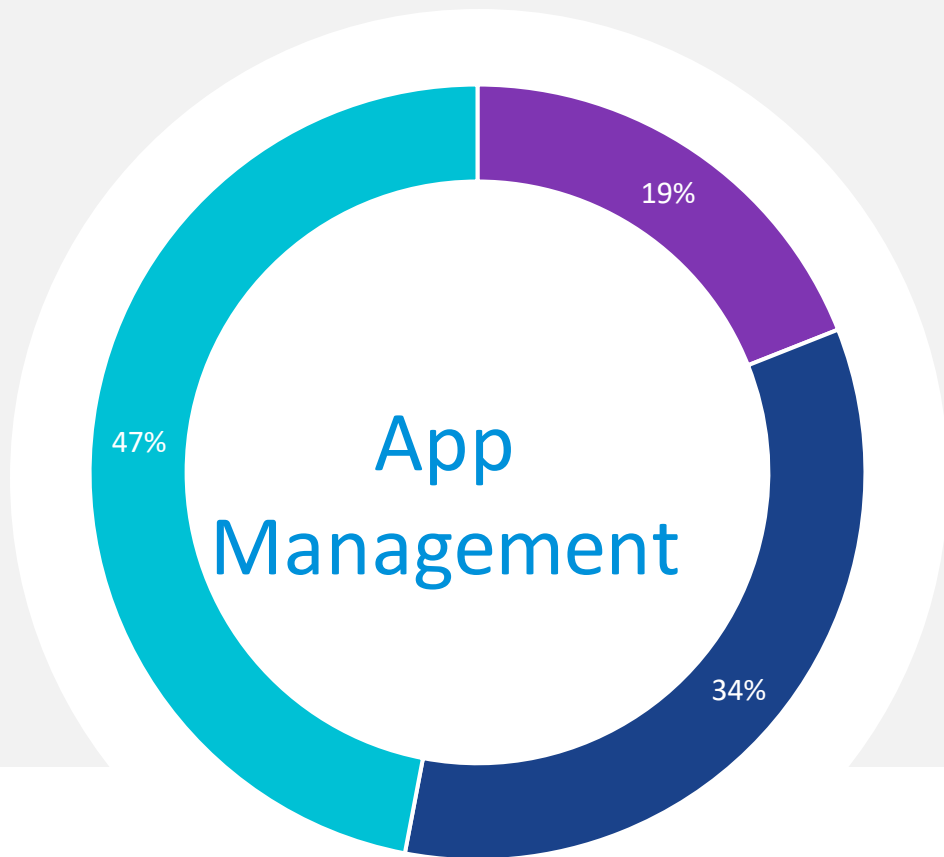
Predictive patching based on device risk (CVE score), reduces time to secure OS

Business steady machines lower downtime and keep users productive



#4: Simplify App Publishing

Modern Management for all Windows apps



A Significant Time Spent in Managing Apps:

5,000+ Hours or 2.5 Full-time IT Admins*

* for a 2,000 employee company

Testing and
Provisioning Apps

Patching, Upgrading and
Supporting Apps

Packaging and Deploying
Apps

Export Apps From Existing Tools for Easy App Publishing

Simply migrate apps from existing tools for easy app publishing




SOFTWARE
DISTRIBUTION

Workspace ONE

Configure apps directly in Workspace ONE UEM console:


Store (UWP) SaaS / Cloud Desktop / Win32

Workspace ONE AirLift

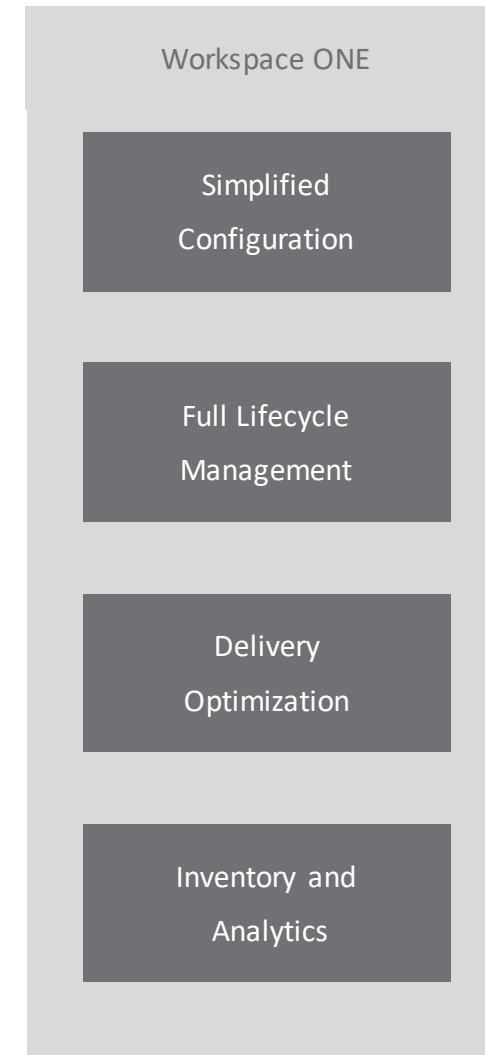


Export apps directly from ConfigMgr (SCCM) to Workspace ONE.

Flexera AdminStudio



Publish your existing desktop app packages to Workspace ONE with no further repackaging effort.



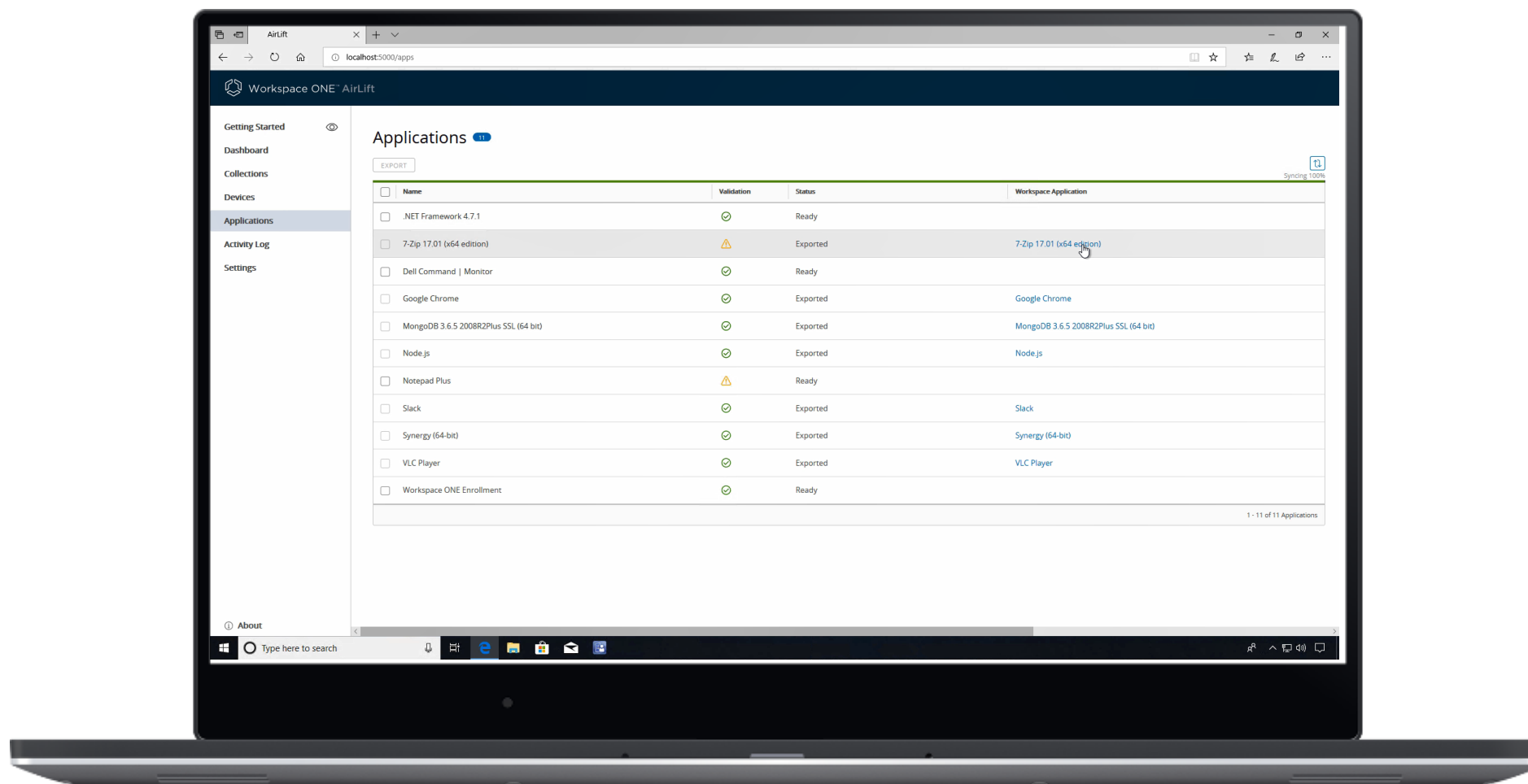
Frictionless and secure access to ALL APPS



App management efficiencies with NO REPACKAGING



Cloud-scale with ZERO server footprint



#5: Zero-trust Security

Compliance from silicon to software

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

Source: VMware's Move to a Digital Workspace: A business value analysis of deploying Workspace ONE

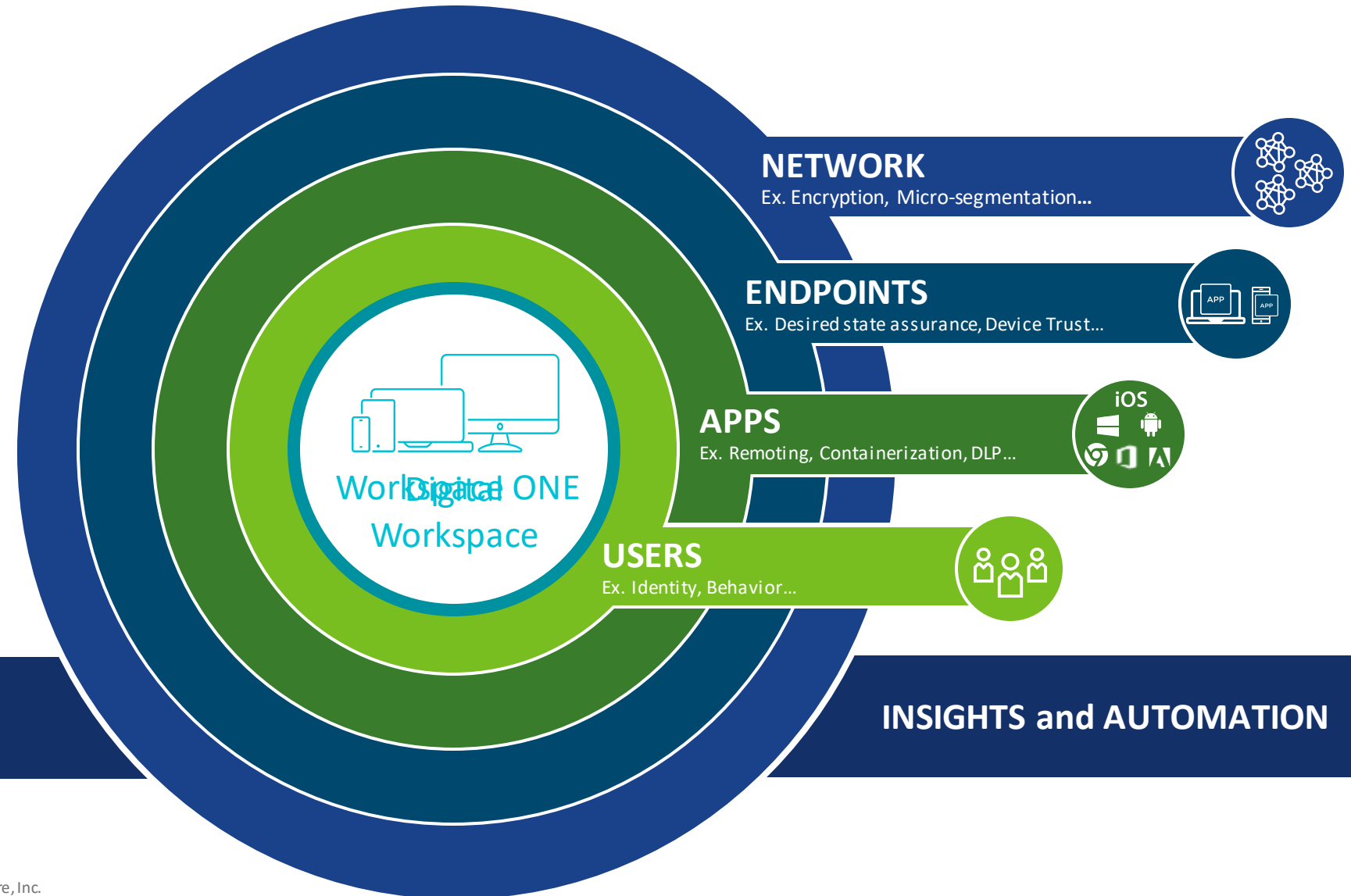
vmware®

Securing the Digital Workspace with Workspace ONE

Proactively secure all attack vectors



CLIENT HEALTH
AND SECURITY



End-to-End Security From Your Device to Data Center

Real-time visibility and security safeguards your EUC environment



CLIENT HEALTH
AND SECURITY



Identity

Strong authentication policies and contextual access to apps and services



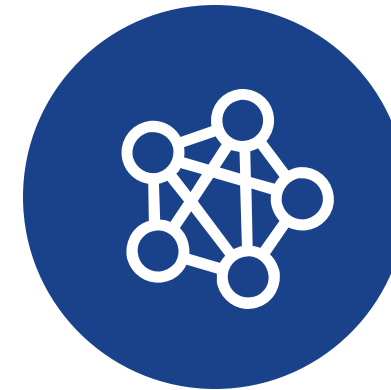
Endpoint

Ensure desired state with real-time health checks and OTA configuration



Apps and Data

Work data protection and instant remote wipe secure sensitive apps and data



Network

Network access restricted to defined servers instead of entire data center



Compliance

Automated compliance ensures hands-free IT and instant remediation

Workspace ONE Sensors Support Your Unique Security Requirements

Query any system attribute for visibility and compliance enforcement



CLIENT HEALTH
AND SECURITY

The screenshot shows the Workspace ONE UEM console interface. The left sidebar contains navigation options: GETTING STARTED, MONITOR, DEVICES, ACCOUNTS, APPS & BOOKS, CONTENT, EMAIL, TELECOM, and GROUPS & SETTINGS. The main content area is titled 'Digital Workspace Tech Zone' and shows the 'Sensors' configuration page. The page has a table of existing sensors with columns for Name, Platform, Trigger Type, Assignment, Managed By, and Value Type. A modal window is open for configuring a new sensor, showing steps for defining the query and response.

Name	Platform	Trigger Type	Assignment	Managed By	Value Type
battery_charging_status	Windows	Schedule	1	Digital Workspace Tech Zone	String
battery_estimated_charge_remaining	Windows	Schedule	1	Digital Workspace Tech Zone	Integer
battery_max_capacity	Windows	Schedule	1	Digital Workspace Tech Zone	Integer
bios_secure_boot	Windows	Schedule	1	Digital Workspace Tech Zone	Boolean
bios_serial_number	Windows	Schedule	1	Digital Workspace Tech Zone	String
bios_smbios_present	Windows	Schedule	1	Digital Workspace Tech Zone	Boolean
bios_smbios_version	Windows	Schedule	1	Digital Workspace Tech Zone	String
bios_status					
bitlocker_encryption					
horizon_broker_url					

Title

1. Sensor

2. Define Query

3. Response

Query Type *

Script/Command *

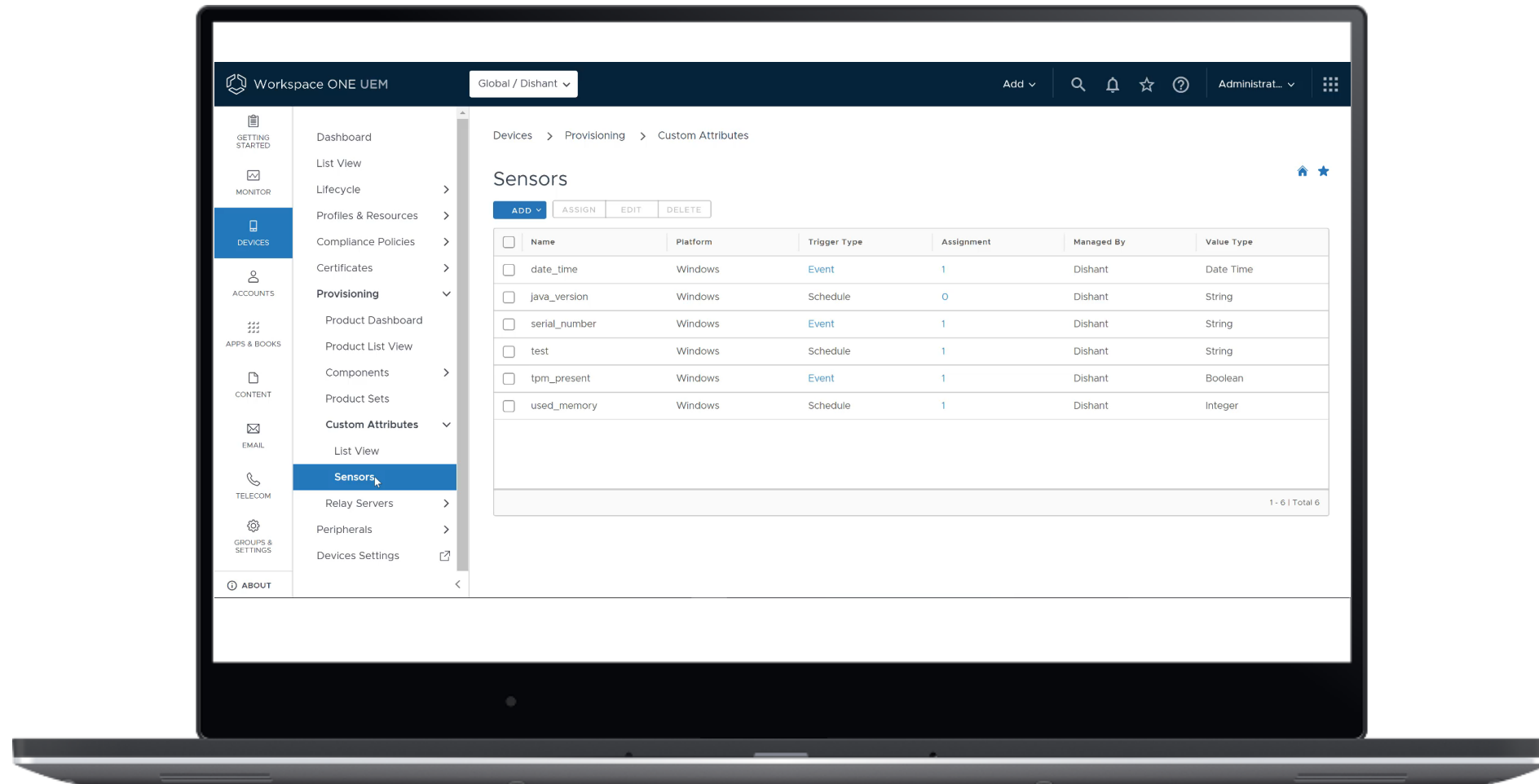
```
body {  
  height: 100%;  
  width: 100%;  
  background-color: #fff;  
  font-family: Arial, sans-serif;  
  font-size: 14px;  
  line-height: 1.2;  
  color: #333;  
}  
  
#button {  
  display: inline-block;  
  padding: 5px 15px;  
  background-color: #3399cc;  
  color: white;  
  border: 1px solid #3399cc;  
  text-decoration: none;  
  cursor: pointer;  
  border-radius: 4px;  
}  
  
background {  
  position: relative;  
  display: -ms-flex-box;  
  display: flex;  
}
```

UPLOAD IMPORT FROM VMWARE

CANCEL NEXT

Seamlessly collect and report on custom device attributes

Automate local or Intelligence-based compliance rules to eliminates policy drift



Unlock the Power of BitLocker within Workspace ONE

Complete BitLocker encryption lifecycle management ensuring higher security at lower TCO



CLIENT HEALTH
AND SECURITY

BitLocker Encryption:

Encrypted Volume	<input type="text" value="Complete Hard Disk"/>
Encryption Method *	<input type="text" value="System Default"/> ⓘ
Only encrypt used space during initial encryption	<input type="checkbox"/>
Custom URL for Recovery Screen	<input type="text" value="https://[Your Device Services Host Name]/mydevice"/>
Force Encryption	<input type="checkbox"/> ⓘ
BitLocker Authentication Settings	
Authentication Mode *	<input type="text" value="TPM"/>
Enforce Encryption PIN on Login	<input type="checkbox"/> ⓘ
Use Password If TPM not present	<input type="checkbox"/>
BitLocker Static Recovery Key Settings	
Create Static BitLocker Recovery key	<input type="checkbox"/> ⓘ
BitLocker Suspend	
Enable BitLocker Suspend	<input type="checkbox"/>

Use TPM for secure auth and ensuring pre-startup OS integrity

Enforce login PIN for MFA and preventing OS auto-resume

Suspend BitLocker for scheduled maintenance tasks

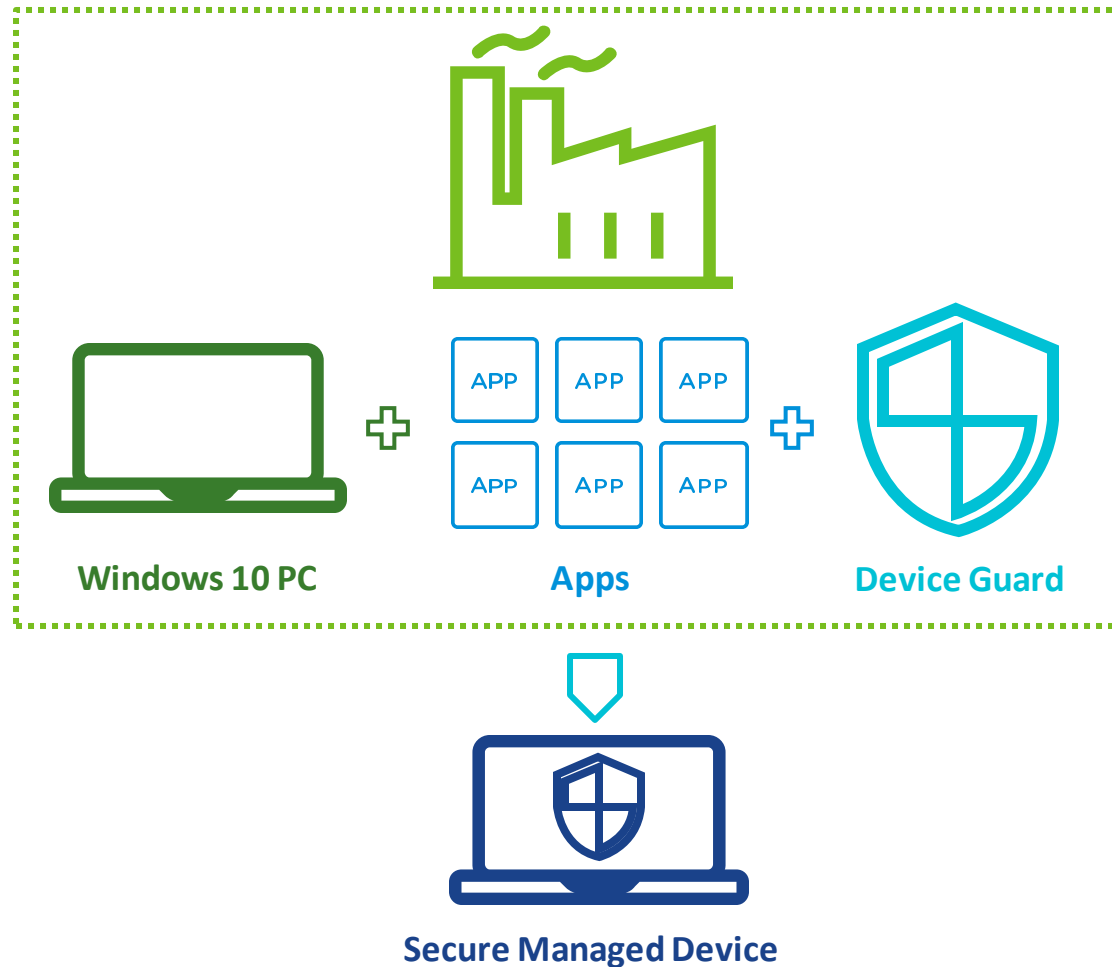
Set recovery key-rotation to meet compliance requirements

Trusted Software Authority for Your Windows 10 PCs

Workspace ONE with Device Guard locks PC to only IT approved apps



CLIENT HEALTH
AND SECURITY



Enterprise secure app environment with Workspace ONE that is free of malware



Enables only IT trusted apps - whether UWP or Win32 - to be installed on the device

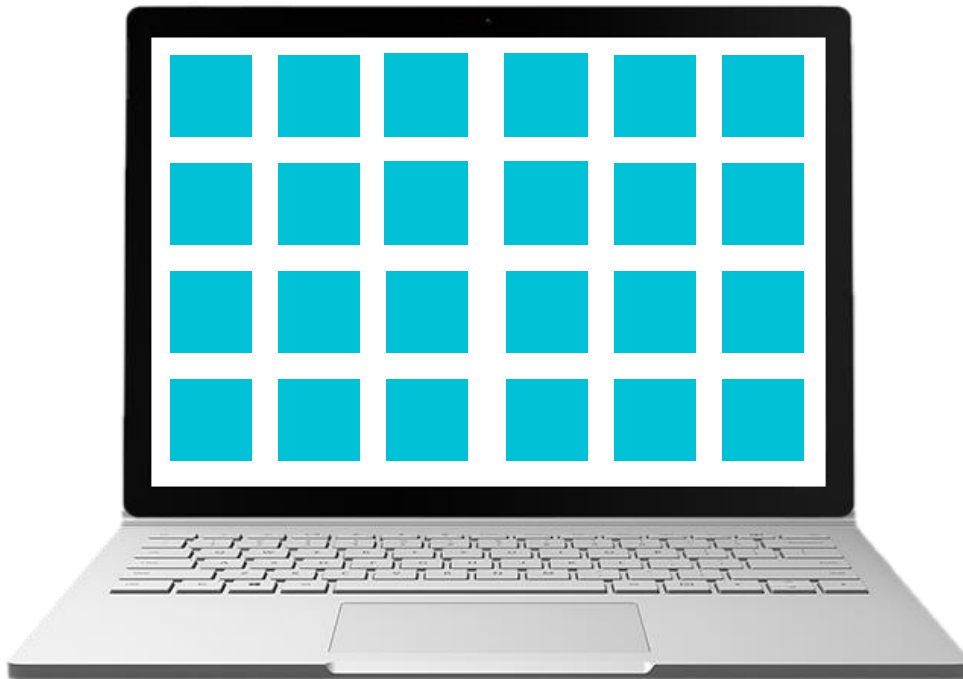


Delivers unparalleled security even in highly regulated environments

Data Security with Windows Information Protection



CLIENT HEALTH
AND SECURITY



Tagging Data: Define data sources to classify as enterprise (IP, domain, SharePoint, and more)



Defining Privileged Apps: Configure privileged apps that can handle enterprise data



Setting Policy Levels: Configure how enterprise data is handled (encrypt, block, audit)



Configuring Per-App VPN: Define which apps can access internal network through VPN



Thank You