Understanding Device Enrollment
Workspace ONE Device Modes

Andreano Lanusse, Staff Architect, VMware

Christina Minihan, Staff Architect, VMware

vmworld® 2021

vmware®

Why Enrollment Method Matters

Terminology Overview

Workspace ONE Management Mode Comparison

Management Options Landscape

Management Options for Specific Platforms

    Android

    iOS

    macOS

    Windows 10

How Intelligent Hub Abstracts Platform Complexity for the End-User

Example Use Cases

Additional Resources

Why Enrollment Method Matters

"Enrollment is the first interaction between the user and Workspace ONE. It must be simple, easy, secure and delights end-users."

"Any bad experience can easily spread across the organization by word of mouth and slow down adoption."
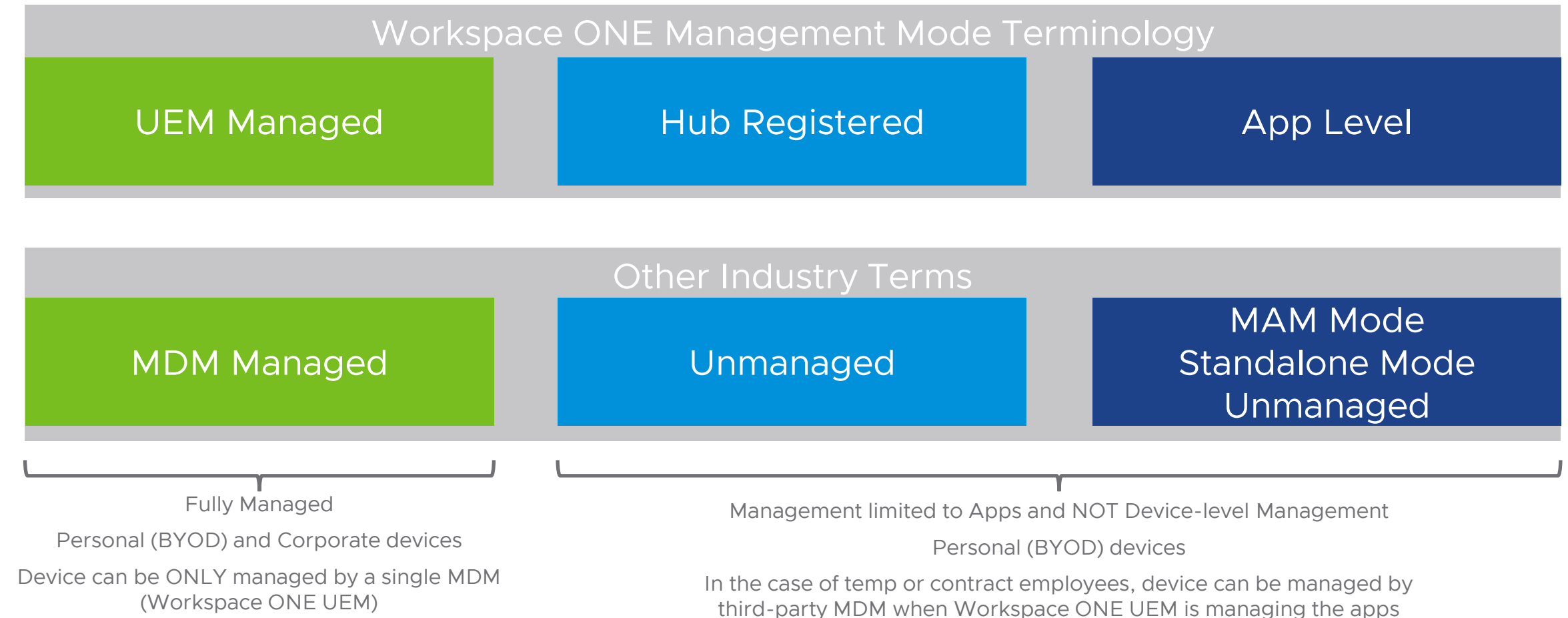
"A well-defined device management strategy is directly correlated to a higher adoption."

"Provide users clearly-defined terms of use, transparency and communication."

Terminology Overview

Workspace ONE Management Modes

What does it all mean?

Workspace ONE Management Mode Terminology		
UEM Managed	Hub Registered	App Level

Other Industry Terms		
MDM Managed	Unmanaged	MAM Mode Standalone Mode Unmanaged

Fully Managed

Personal (BYOD) and Corporate devices

Device can be ONLY managed by a single MDM (Workspace ONE UEM)

Management limited to Apps and NOT Device-level Management

Personal (BYOD) devices

In the case of temp or contract employees, device can be managed by third-party MDM when Workspace ONE UEM is managing the apps

5

UEM Managed vs Registered Mode vs App Level
Overview

UEM Managed
macOS iOS android

Device is fully managed by UEM admin

Push commands, configurations, policies and applications to the device

Requires Intelligent Hub and MDM Profile

Hub Registered Mode
iOS android

Management is limited to:

- enforce policies
- wipe restricted to applications

Exception for Windows 10:

- Administrator can apply device baselines and collect device information through sensors

Requires Intelligent Hub

- Administrator can't push apps to the device, user must request through Hub

No MDM Profile

App Level (MAM)
iOS android

Management restricted to SDK applications, such as:

- Workspace ONE Web
- Workspace ONE Boxer
- Workspace ONE Content

Workspace ONE SDK required

Enrollment starts with the SDK-based app

Intelligent Hub not required

- No catalog, people search, notifications, etc.

No MDM Profile

Workspace ONE UEM Console

List of enrolled devices with management mode and compliance status

Workspace ONE **UEM**   ACME Corp ⌄   Add ⌄   🔍 🔔³¹ ⭐

GETTING STARTED

FREESTYLE

MONITOR

DEVICES

RESOURCES

ACCOUNTS

CONTENT

Devices

List View

Filters »   ⊕ ADD DEVICE   LAYOUT ⌄ ⟳ EXPOR

☐	Last Seen ▲	General Info	Platform	User	Enrollment	Compliance Status ⓘ
☐ ✎	20s	moliver VMware7,1 Windows Desktop 10.0.19... ACME Corp / Field Contractors Hub Registered | Corporate - Dedicated	Windows Desktop VMware7,1 10.0.19042	moliver@airwlab.com moliver Mary Oliver	✓ Enrolled	⚠ Not Available
☐ ✎	41s	llopez VMware Virtual Platform Windows Desk... ACME Corp / Corporate Headquarter (HQ) UEM Managed | Corporate - Dedicated	Windows Desktop VMware Virtual Platform 10.0.19042	llopez@airwlab.com llopez Linda Lopez	✓ Enrolled	✓ Compliant
☐ ✎	49s	ALanusse Desktop Windows Desktop 10.0.190... ACME Corp / Corporate Headquarter (HQ) UEM Managed | Corporate - Dedicated	Windows Desktop VMware7,1 10.0.19042	alanusse@airwlab.com ALanusse Andreano Lanusse	✓ Enrolled	✓ Compliant
☐ ✎	4m	ALanusse Desktop Windows Desktop 10.0.190... ACME Corp / Field Contractors Hub Registered | Corporate - Dedicated	Windows Desktop XPS 13 9360 10.0.19042	alanusse@airwlab.com ALanusse Andreano Lanusse	✓ Enrolled	⚠ Not Available
☐ ✎	4m	ALanusse iPad iOS 14.4.0 ACME Corp / Field Contractors App Level | Employee Owned	Apple iOS 14.4.0	alanusse@airwlab.com ALanusse Andreano Lanusse	✓ Enrolled	⚠ Not Available
☐ ✎	5m	mli Android Android 9.0.0 CW5Y ACME Corp / BYOD UEM Managed | Employee Owned	Android samsung SM-G950U1 9.0.0	mli@airwlab.com mli Michael Li	✓ Enrolled	⚠ Not Available

UEM Managed vs Hub Registered

Device information and actions limited based on the enrollment method

Management Options Landscape

Mobile Management Options Overview

Along the Gradient

Corp-Owned

BYOD

More Admin Control

Full Device Management

OS Partitioned

Containerized Apps

Hub Registered Mode

App Level Management

More User Privacy
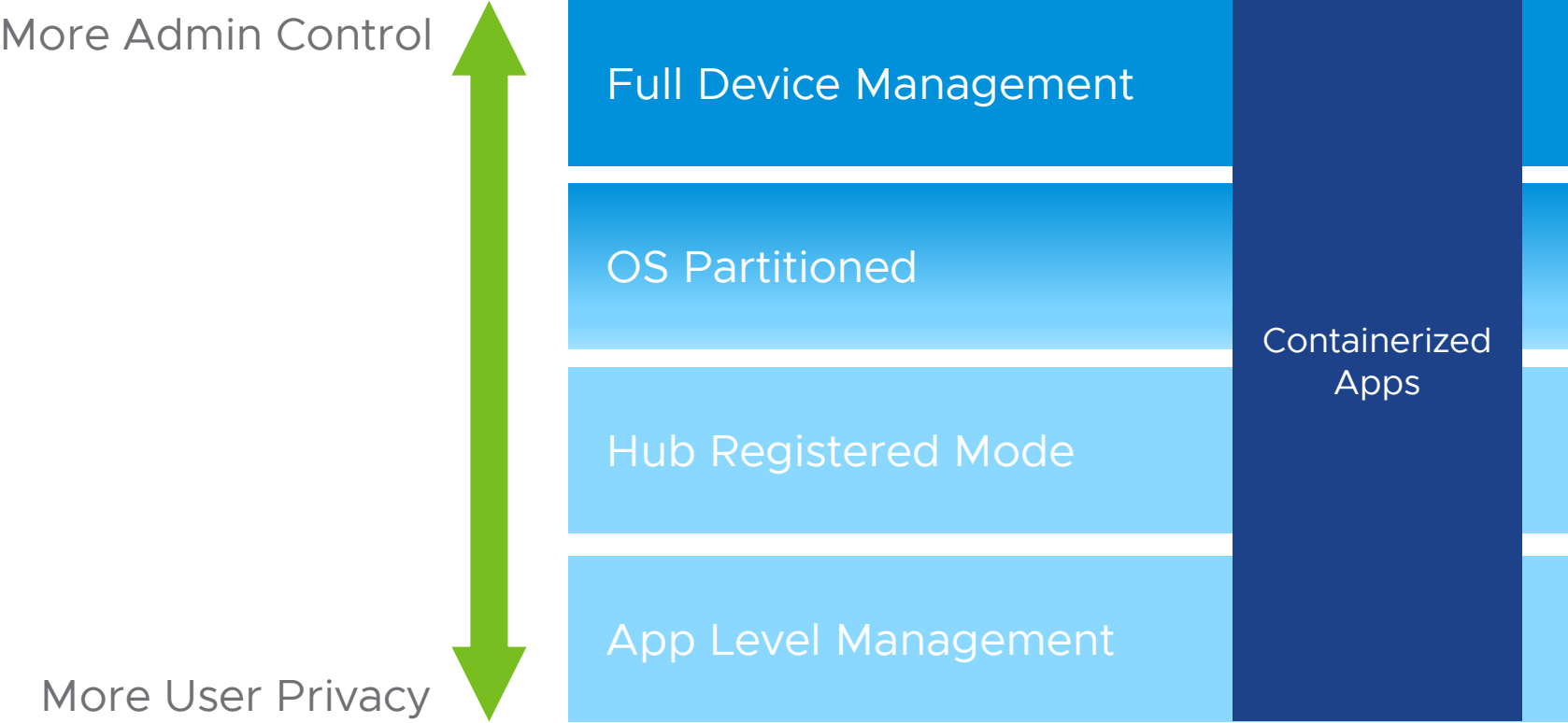
Android Management Options
Along the Gradient

Corp-Owned
BYOD

More Admin Control

Work Managed (aka Device Owner Mode)

Corporate Owned Personally Enabled (COPE)

Knox for Play = Work Profile + Samsung Knox

Work Profile Mode

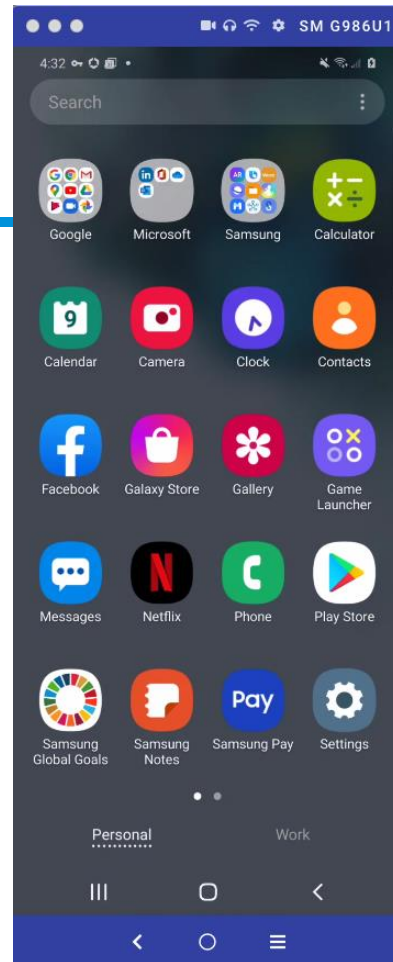Hub Registered Mode (Intelligent Hub Registered)
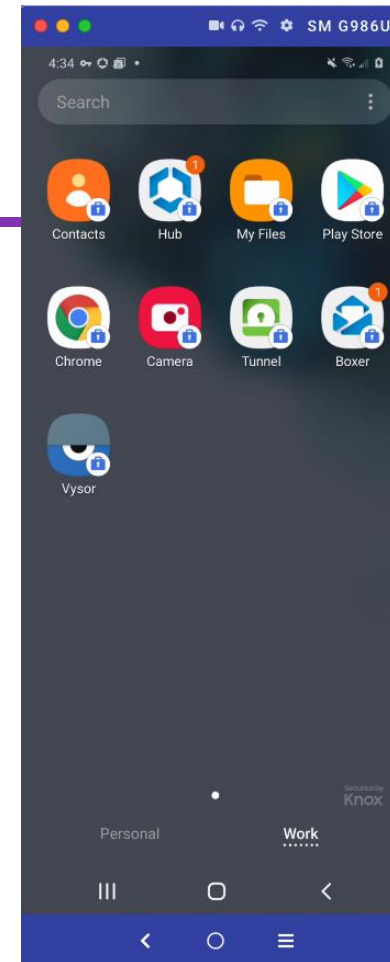
App Level Management

Containerized Apps

More User Privacy

Android Enterprise Work Profile
End User Experience

Personal Profile

Work Profile

iOS Management Options
Along the Gradient

Corp-Owned

BYOD

More Admin Control

More User Privacy

Apple Business Manager or Apple School Manager (Automated Device Enrollment) + Supervised

Supervised Device Enrollment

Unsupervised Device Enrollment

iOS User Enrollment

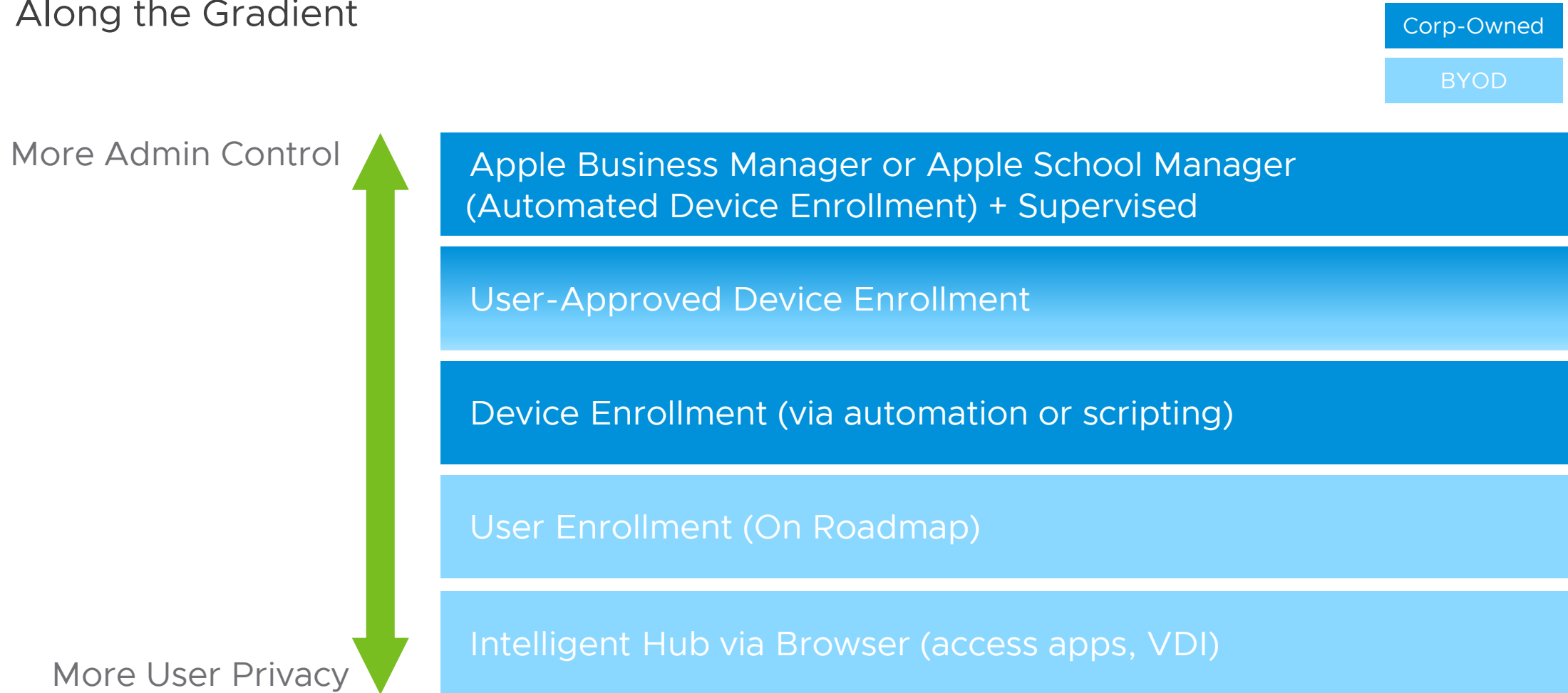Hub Registered Mode (Intelligent Hub Registered)

App Level Management

Containerized Apps

macOS Management Options

Along the Gradient

Corp-Owned

BYOD

More Admin Control

Apple Business Manager or Apple School Manager (Automated Device Enrollment) + Supervised

User-Approved Device Enrollment

Device Enrollment (via automation or scripting)

User Enrollment (On Roadmap)

Intelligent Hub via Browser (access apps, VDI)

More User Privacy

Windows 10 Management Options

Corp-Owned

BYOD

More Admin Control

MDM Enrolled (via multiple onboarding methods)

Hub Registered Mode (Intelligent Hub Registered)

Intelligent Hub via Browser (access apps, VDI)

More User Privacy

How Intelligent Hub Abstracts Platform Complexity for the User

Fragmentation Impacts Cost, Security and Employee Experience

Siloed endpoint management practices haven't evolved to support the modern workforce

Legacy Technology

Increased Cost

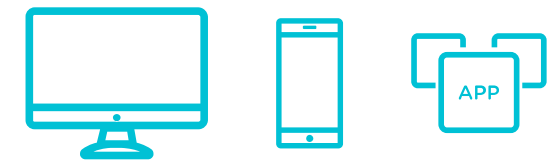**80%** Cost of post-deployment management and support

Increasing Threats

Compromised Security

95% Breaches originate at endpoints
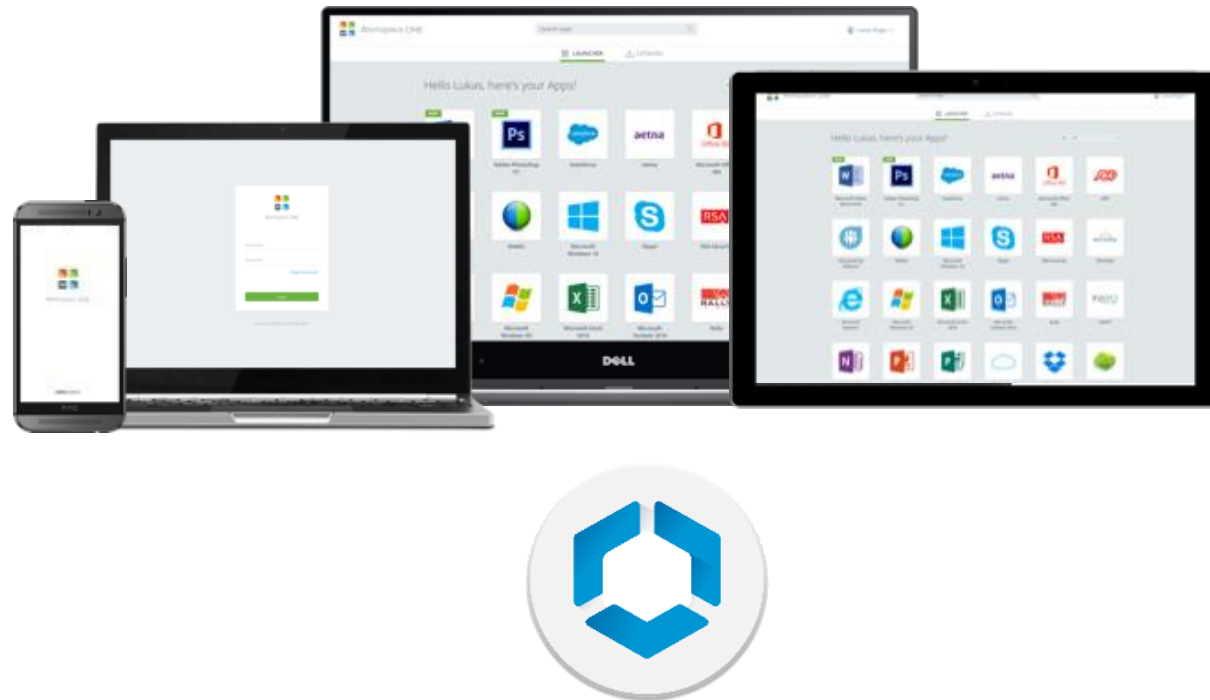
Siloed Organization

Poor User Experience

76% Don't have apps from IT to get work done

Frictionless Access to All Applications
Workspace ONE Intelligent Hub ensures consistent user experience on every device

One place for all your business apps, optimized by device type

One-touch mobile single sign-on using device trust

Simple self-service onboarding for new users and new devices

Easy multi-factor authentication using any mobile device

Privacy by design assures users personal apps and data remain invisible to IT

When do I use each management mode?

Example Use Cases

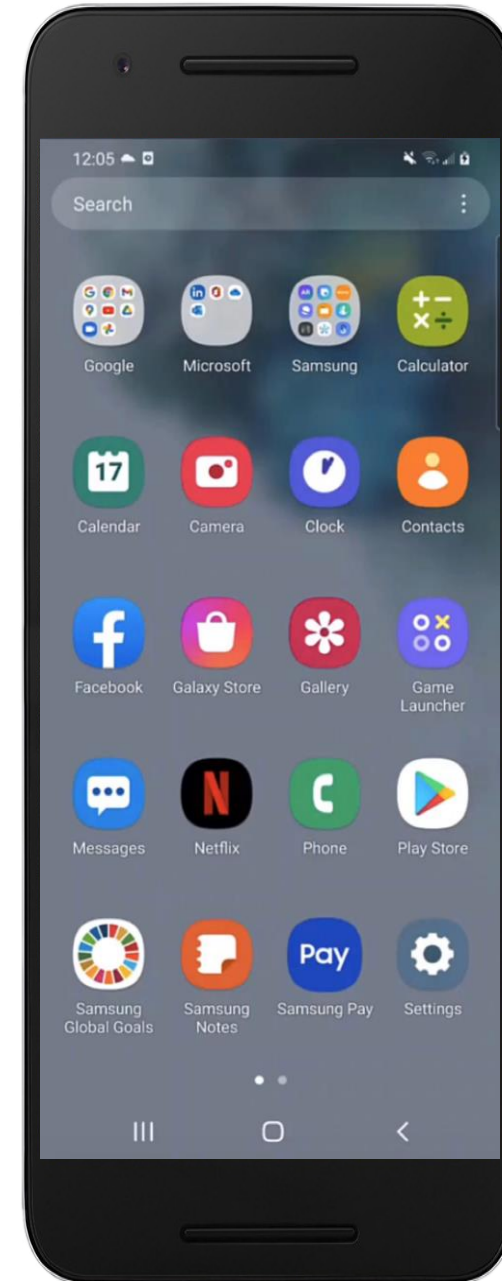# "I just need email access on my phone."

Entry-level use case

Contract Employee, BYOD, Temp Worker, etc.

Workspace ONE Intelligent Hub not installed

Stand-alone Workspace ONE Boxer email client

App Level management mode

"I just need email access on my phone."
App Level Management - UEM Console View

"Contractors need access to internal web applications."

OPTION 1 – Workspace ONE Web

Enrollment through Workspace ONE Web

App Level Management

No App Catalog

Only bookmarks in Web app

DLP on the Web App

"Contractors need access to internal web applications."
OPTION 2 – Intelligent Hub (Registered Mode) with Workspace ONE Web
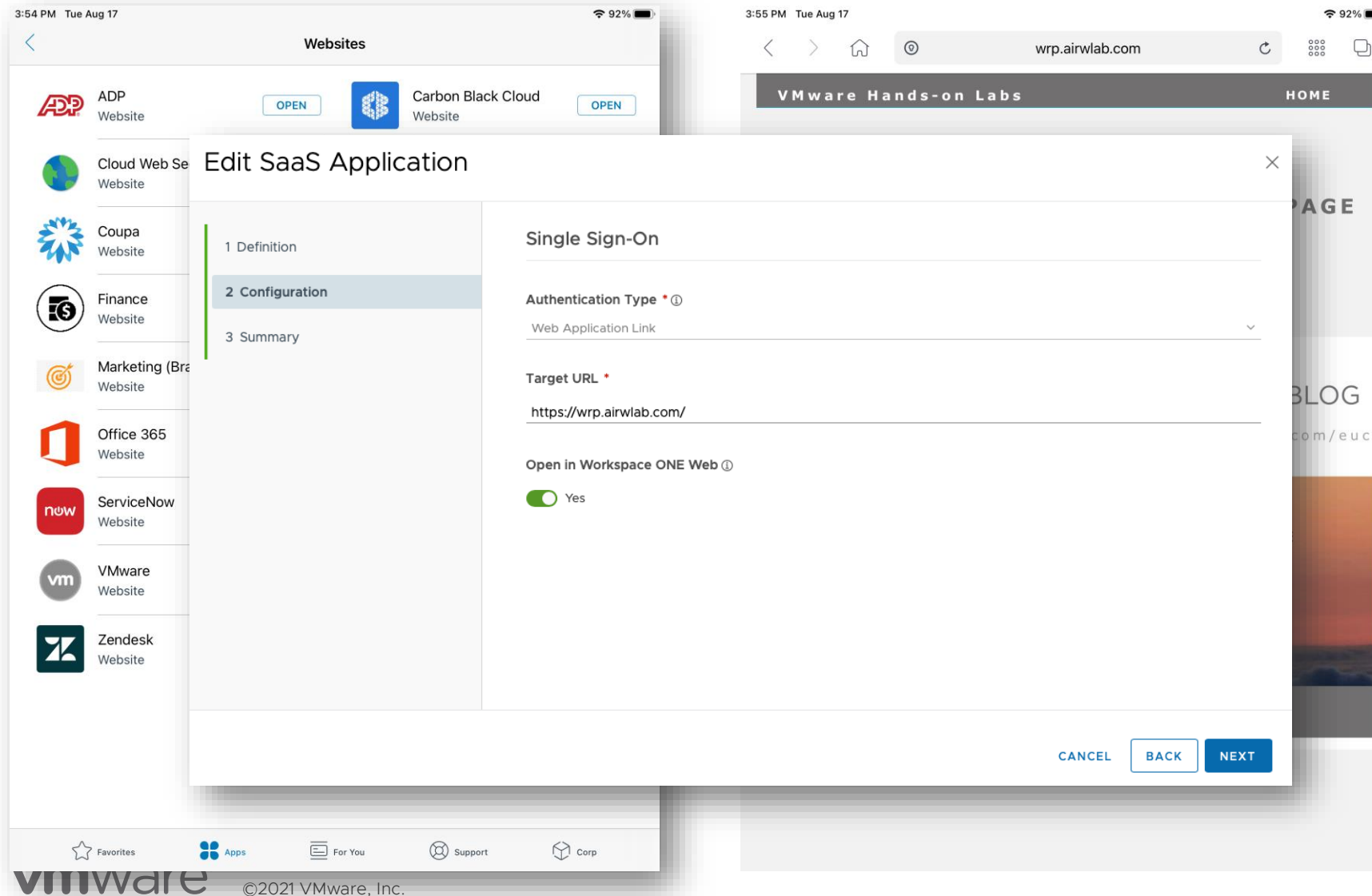
Registered Mode Intelligent Hub

App Catalog and Web Clips

Install native mobile apps from the catalog

Federated Apps integrated to launch through Web, requires Workspace ONE Access

Better User Experience

"I need access to corporate Wi-Fi in several offices."
Any Device Platform

Users and Devices

Cert-Auth

On-Premises

Outbound Only
443

AirWatch Cloud
Connectors

Certificate
Authority

Workspace ONE UEM
(SaaS)
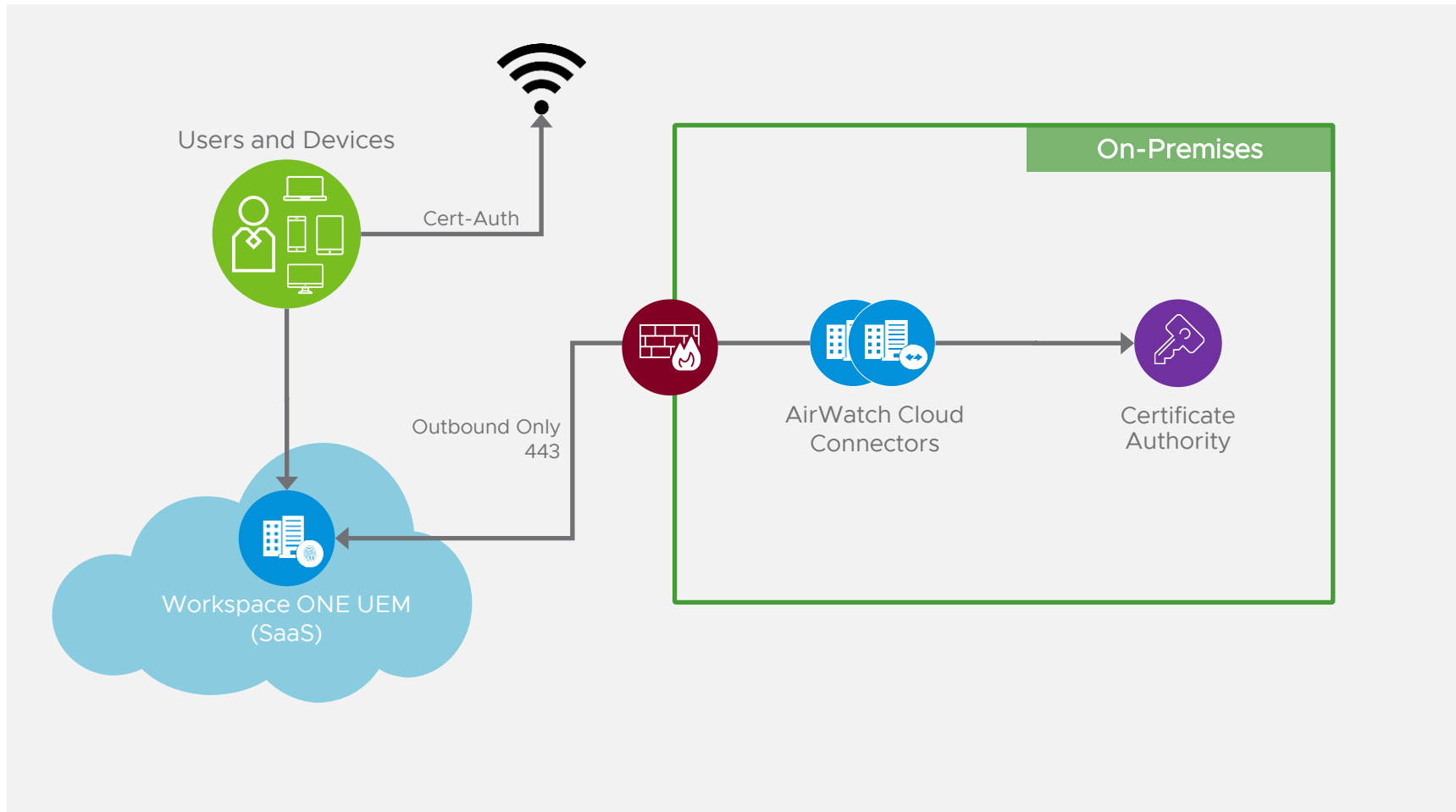
UEM Managed required

Must authenticate device

Certificate auth for Wi-Fi, eliminating password entry

Can be extended to email, web applications, etc.

"I need access to restricted internal applications, SaaS and VDI."

Any remote workers

Hub Unified Catalog

- Deploy Native Apps
- SaaS, Web, Internal, VDI

Conditional Access (Device Compliance + User Risk Score) to determine access to applications – requires UEM managed
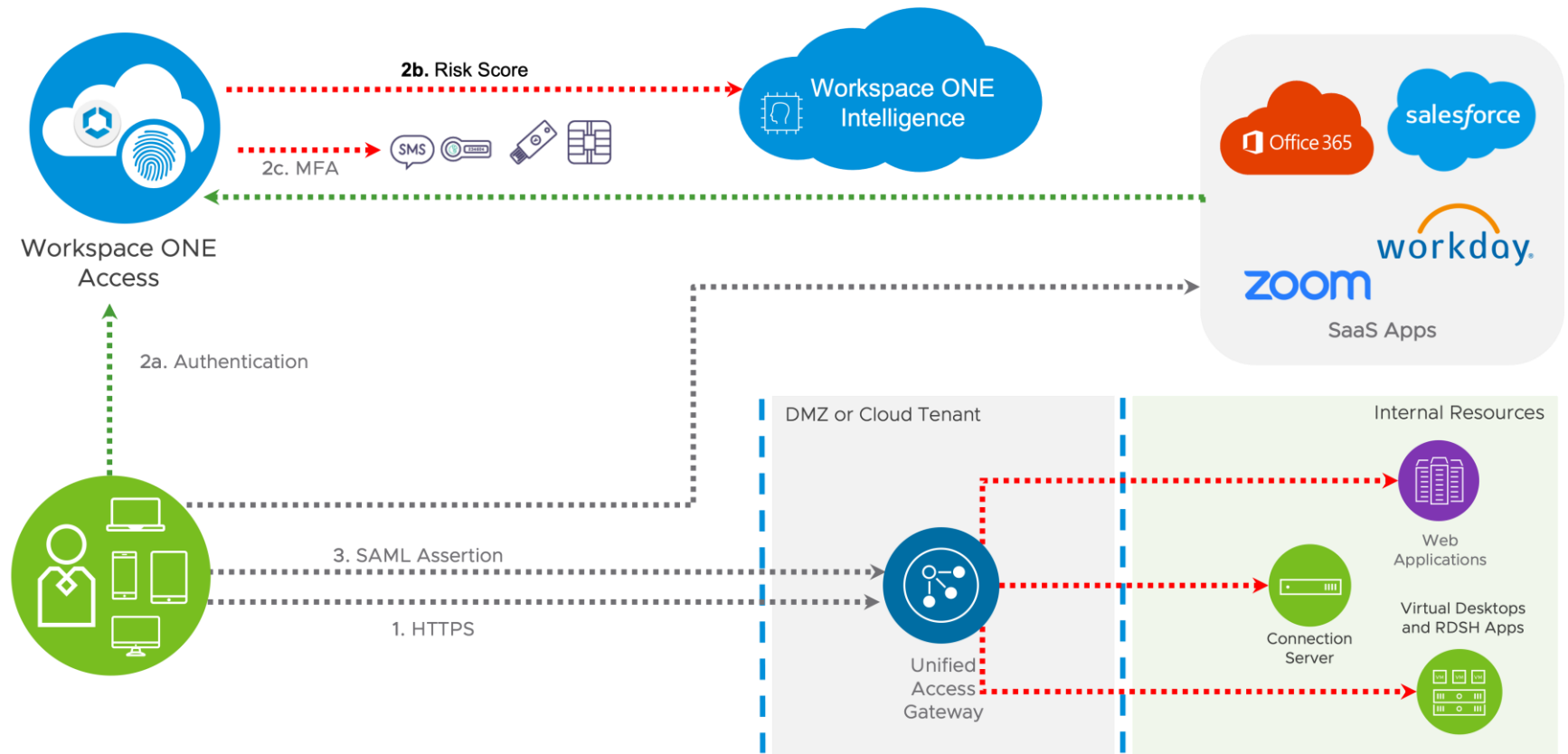
''Apply Zero Trust principals to determine application access"

Secure access to Web, SaaS, Virtual Desktops and Published Applications

2b. Risk Score

Workspace ONE Intelligence

2c. MFA

Workspace ONE Access

2a. Authentication

3. SAML Assertion

1. HTTPS

Office 365

salesforce

workday

zoom

SaaS Apps

DMZ or Cloud Tenant

Internal Resources

Unified Access Gateway

Connection Server

Web Applications

Virtual Desktops and RDSH Apps
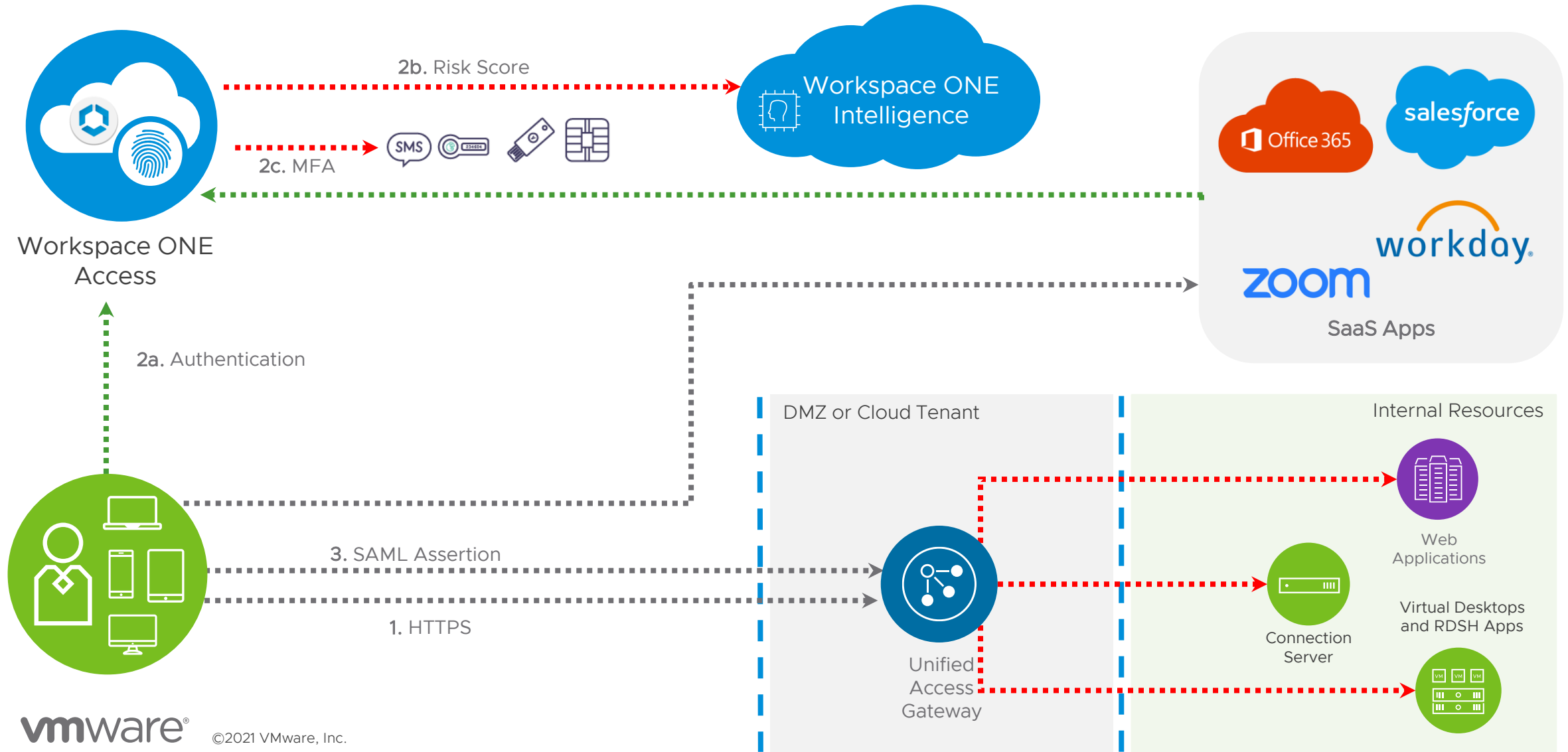
Risk Score Aggregation

Compute a personalized Risk Score for every device and user in an organization

Are there unknown, rare or questionable apps?

Is the device's OS up-to-date?

Are device security capabilities enabled?

"The user tends to accumulate apps and not consider their reputation"

"The user systematically ignores or keeps delaying software update"

"The device is missing a critical patch"

User Risk Score

Android Device Score

Low		

iPad Device Score

	Medium	

macOS Device Score

	Medium	

Windows 10 Device Score

		High

John Doe

Low	Medium	High

John's devices

vmware®

Risk Indicators
User Behaviors Contributing to Risk Score

Device	Apps	Threats
Laggard Update	Compulsive App Download*	Anomalous Alert Activity (Carbon Black)
Risky Setting	Unusual App Download*	
Persistent Critical CVE*	App Collector*	
High Number of CVE*	Rare App Collector*	
	Based on UEM Privacy Settings	
	Unmanaged apps only	

*Managed device only

Summary
General Guidelines for UEM Managed vs Registered Mode vs App Level

UEM Managed
macOS iOS android

Provide access to corporate resources and fully manage the device

Use Cases:

- Personal device (BYOD)
- Corporate Dedicated
- Corporate Shared

Hub Registered Mode
iOS android

The user can access the catalog of corporate applications without full management of the device

– Desktops: IT can enforce baselines on Windows 10 and use sensors to collect additional device info

Use Cases:

- End-user requires access to corporate resources from personal device without giving IT full control of the device

App Level (MAM)
iOS android

Allow organizations to provide access to corporates resource on a per-app bases

Use Cases:

- Employee needs access to email only without providing IT management of the device
- Contractors needs access to internal websites from personal devices, and IT needs to apply security policies only to the corporate app

Ready to Learn More?

euc.techzone.vmware.com

TECH ZONE CONTENT

- How to Enable Intelligent Hub and Workspace ONE Apps without Full Management

- Enabling Registered Mode for Windows 10 and DEEM

- Steps to Enable a Remote Workforce with Workspace ONE - Part 1

- Steps to Enable a Remote Workforce with Workspace ONE – Part 2

- VMware Workspace ONE and Horizon Reference Architecture

- Mastering Workspace ONE

- Onboarding Options for macOS

Resources to Get You Started
We have you covered whether you are learning, testing, or ready to deploy…

Learn more about Workspace ONE UEM

Workspace ONE Hands on Labs:

http://labs.hol.vmware.com/HOL/cat alogs/catalog/878

Test Drive Workspace ONE UEM on your devices

Workspace ONE on TestDrive

https://portal.vmtestdrive.com/

Get Started on Your UEM PoC or Deployment

Workspace ONE Operational Tutorials

- https://euc.techzone.vmware.com/

vmware® DIGITAL WORKSPACE
TECH ZONE

techzone.vmware.com

Your Fastest Path to Understanding, Evaluating and Deploying VMware Products

Other Tech Zone Sites

go.techzone.vmware.com

**CARBON BLACK
TECH ZONE**

carbonblack.vmware.com

**NETWORKING AND
SECURITY TECH ZONE**

nsx.techzone.vmware.com

**THE CLOUD PLATFORM
TECH ZONE**

core.vmware.com

**VMWARE CLOUD
TECH ZONE**

vmc.techzone.vmware.com

vmworld®

IMAGINE
that

Thank you!

vmware® ©2021 VMware, Inc.