

Configuring Workspace ONE Access for the Anywhere Workspace

The logo for vmworld 2021 is displayed in a glowing, blue, sans-serif font. The word 'vmworld' is on the top line, followed by a registered trademark symbol (®), and '2021' is on the line below. The background of the slide features a dark blue, textured, abstract shape on the right side, resembling a nebula or a splash of paint, with some white star-like specks and faint white orbital lines.

Sascha Warno, Staff Architect

EUC Technical Marketing, VMware

SESSION ID: EUS1964

#vmworld #EUS1964



Challenges with access to resources

Improving the User Experience

Enforcing Multi Factor Authentication

Seamless Sign On Experience

Contextual and Risk based access rules

An Anywhere Organization

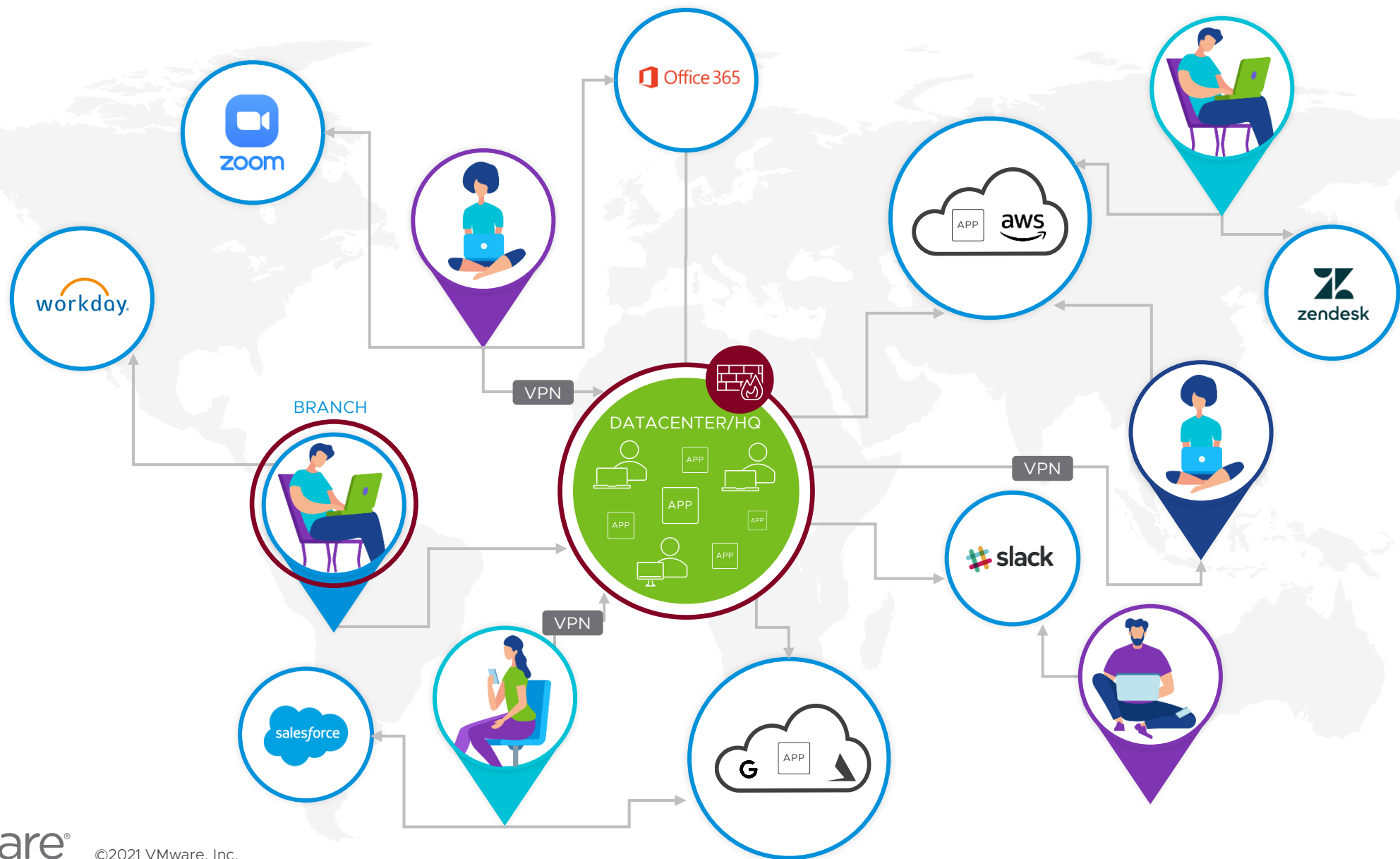


Onboarding
Challenges



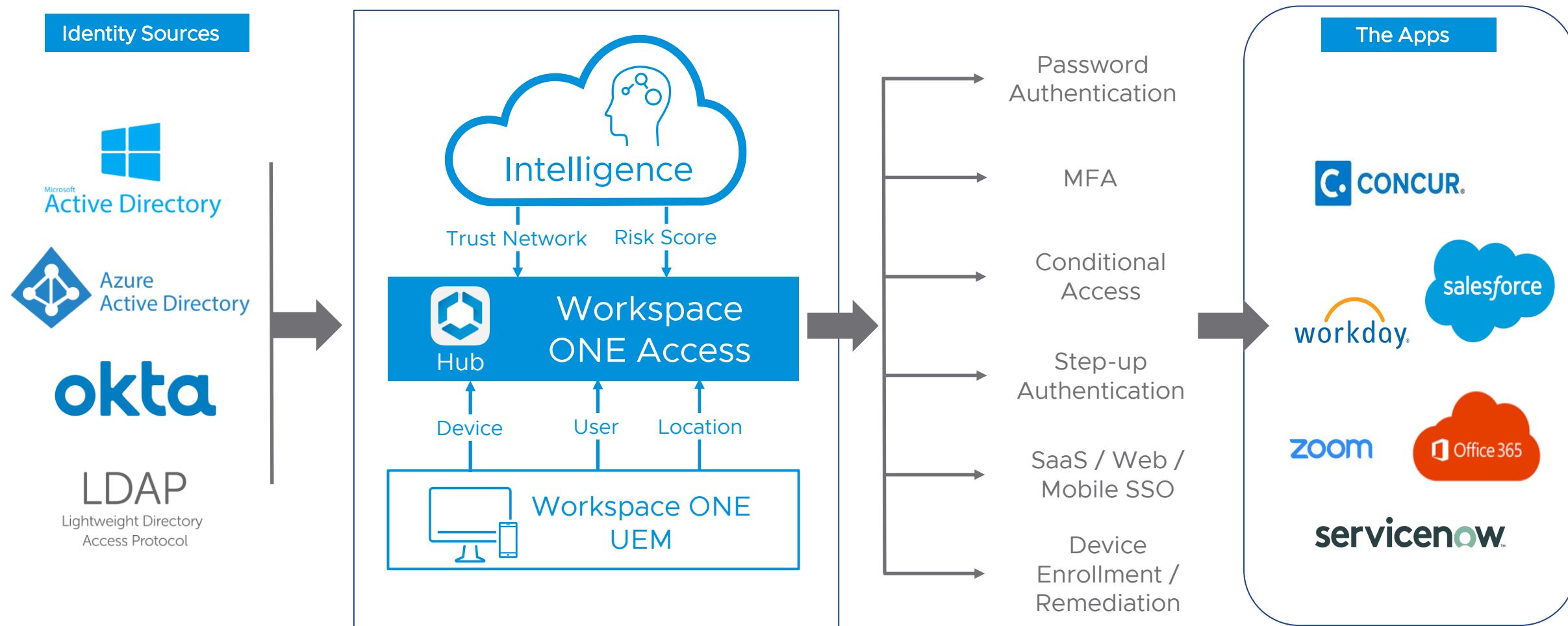
Multi-modal Workstyles Define the Anywhere Organization

Remote Access Today Mostly Based on VPNs



Workspace ONE Access

Enterprise Authentication and Single Sign-On





Creating your

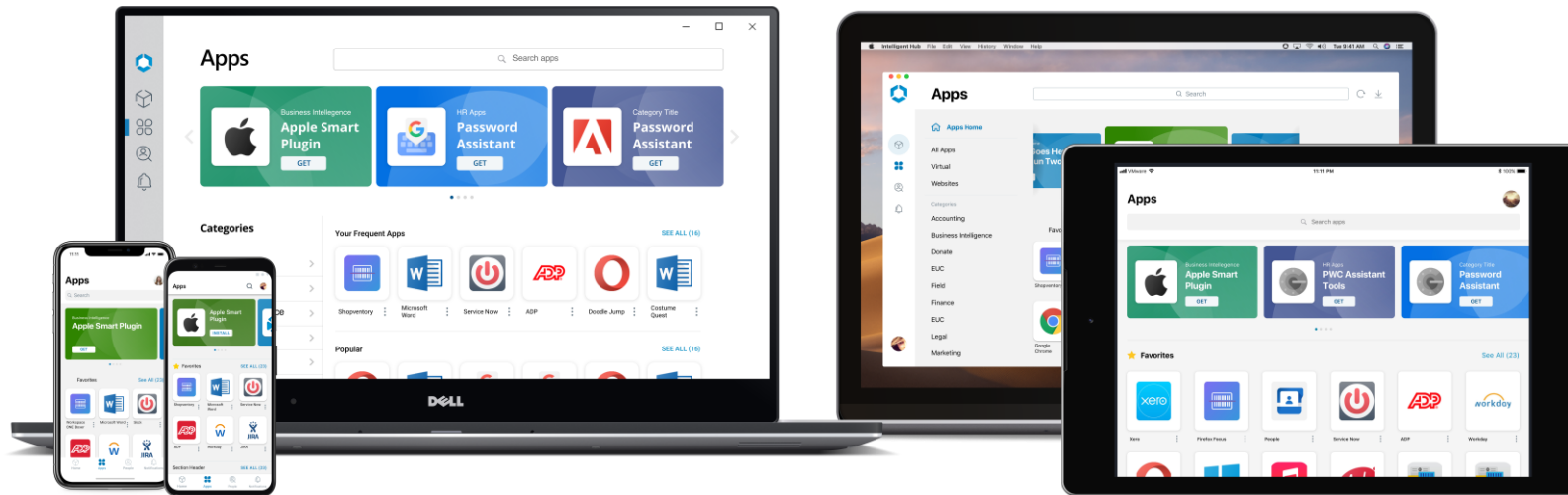
Access Catalog and Single Sign On

Anywhere as ONE



Unified Catalog - Workspace ONE Intelligent Hub

Engaging employees from onboarding to offboarding



Onboarding | Home | App Catalog | People | Notifications | Workflows

Seamless Experience



Single Sign-On (SSO)

Conditional Access

Multi-Factor Auth (MFA)



Native Across Platforms

iOS | Android | Mac

Windows | Web



Corporate Communications

Actionable Notifications



vmware®

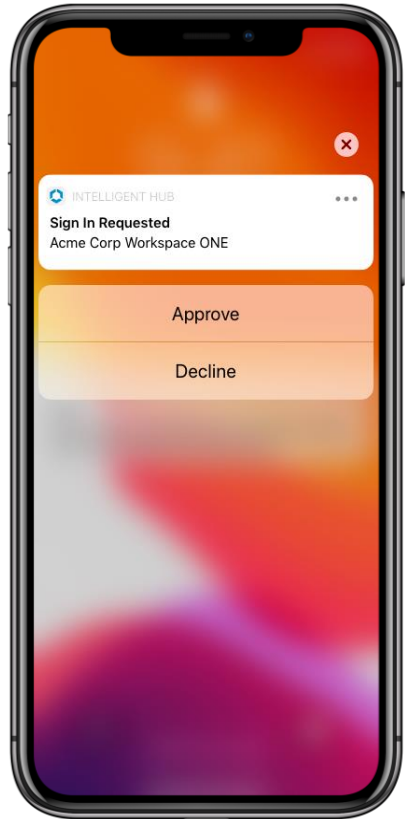
Leveraging

Multi-Factor Authentication

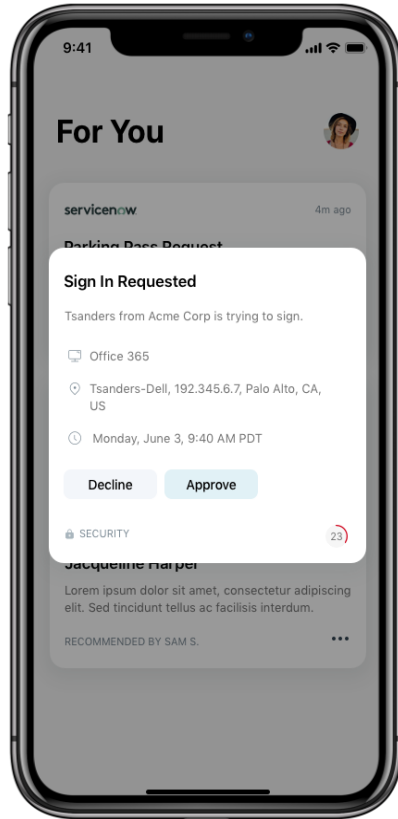
Anywhere as ONE

Verify in Intelligent Hub

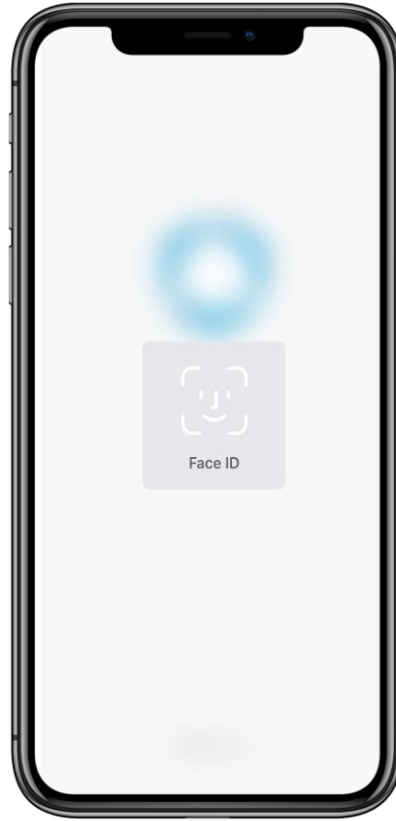
Industry first MFA integration into the Digital Workspace Platform



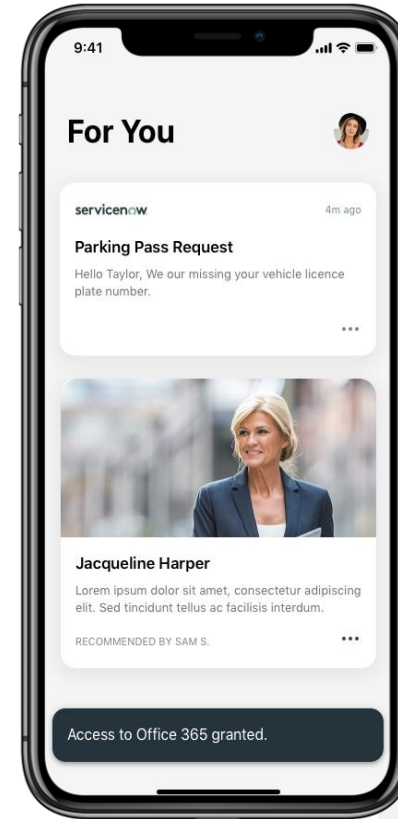
Notify



Authorize



Authenticate



Access

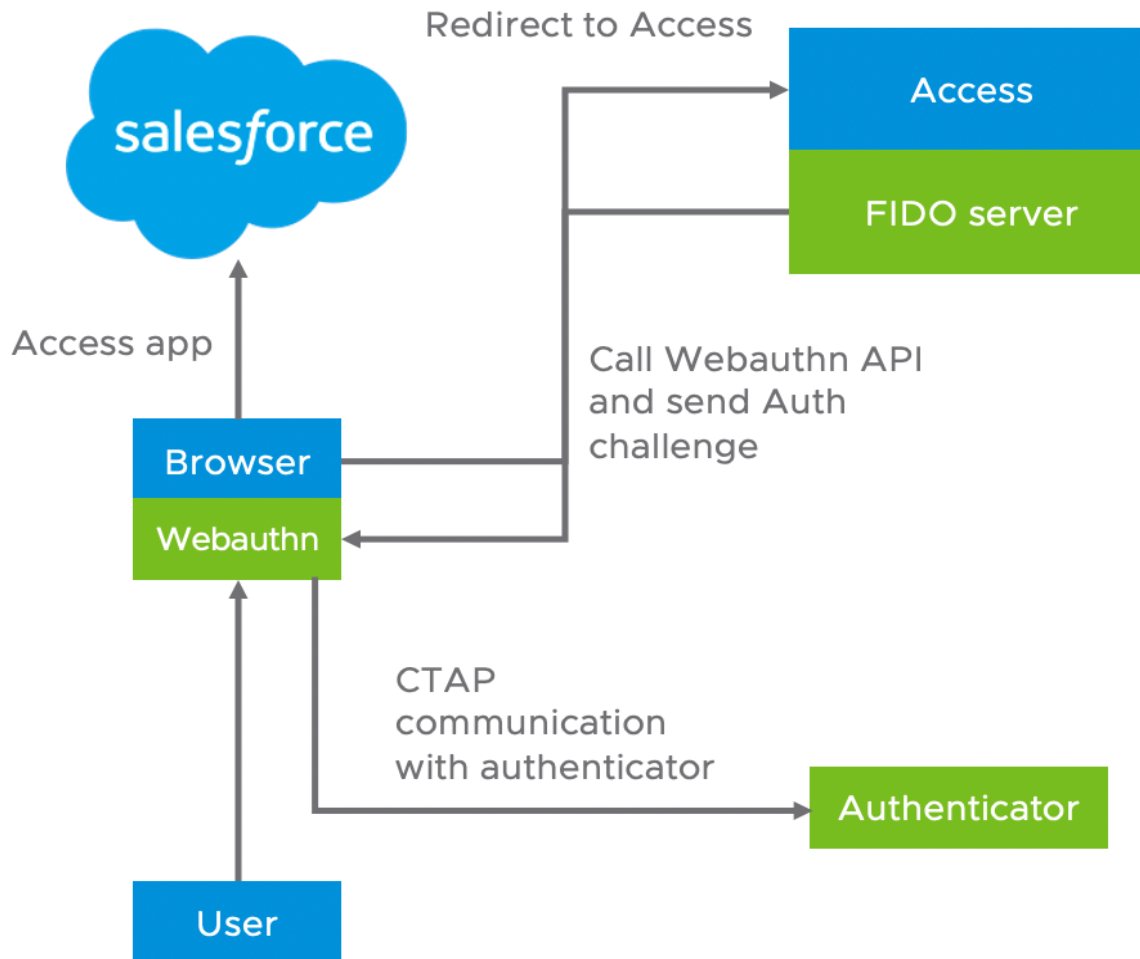
Verify in Intelligent Hub

Industry first integrated experience

No user pre-reg or separate app

Biometric check on approval

FIDO2 and WebAuthn



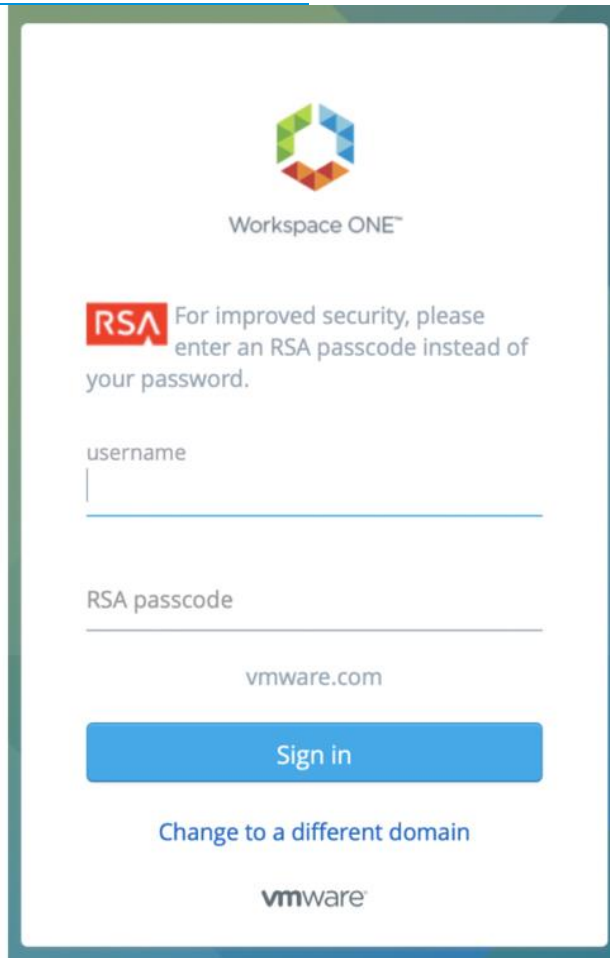
Integration

FIDO stands for Fast identity Online. It is a Consortium that develops secure, open, phishing proof, password less authentication standards.

Webauthn is a global standard for web authentication as of March 2019. it is a browser-based API to trigger FIDO client authentication.

CTAP is a Client to Authenticator Protocol. It is a communication protocol between external authenticator and FIDO client.

3rd Party Integration



Workspace ONE™

RSA For improved security, please enter an RSA passcode instead of your password.

username

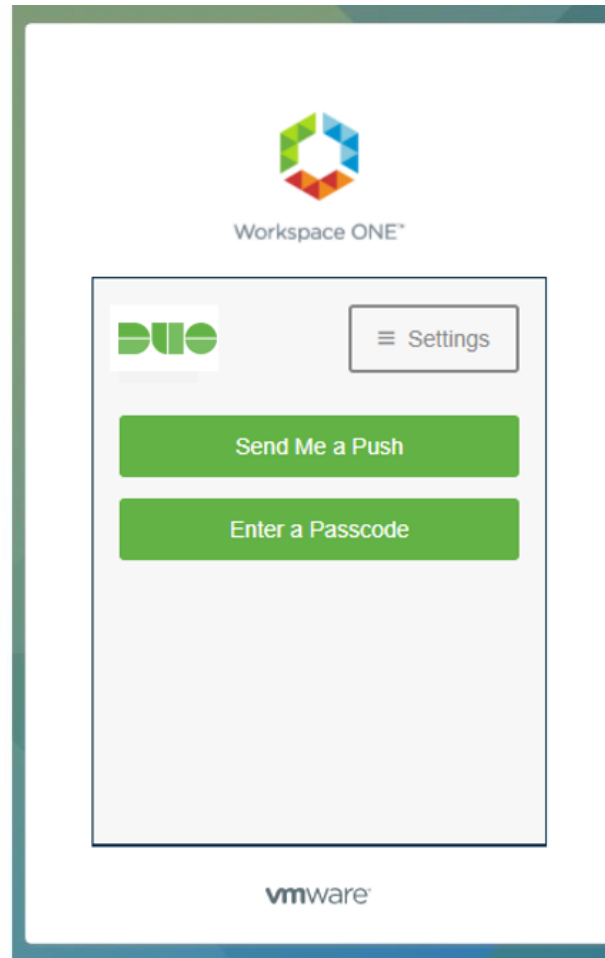
RSA passcode

vmware.com

Sign in

[Change to a different domain](#)

vmware™



Workspace ONE™

Duo ≡ Settings

Send Me a Push

Enter a Passcode

vmware™

Integration

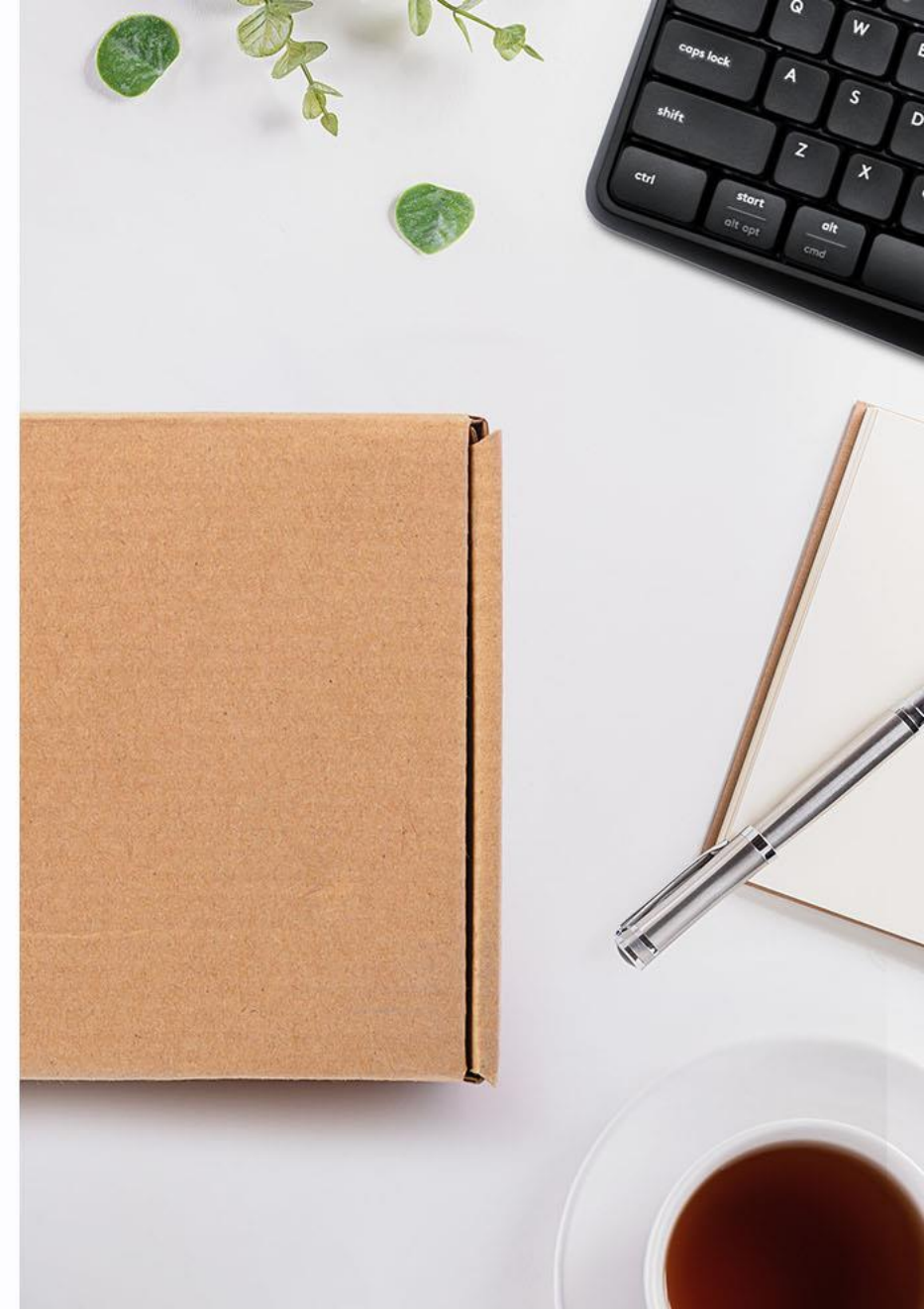
Native Integration with MFA providers – RSA and Duo

RADIUS and SAML/OIDC support for other 3rd party MFA's



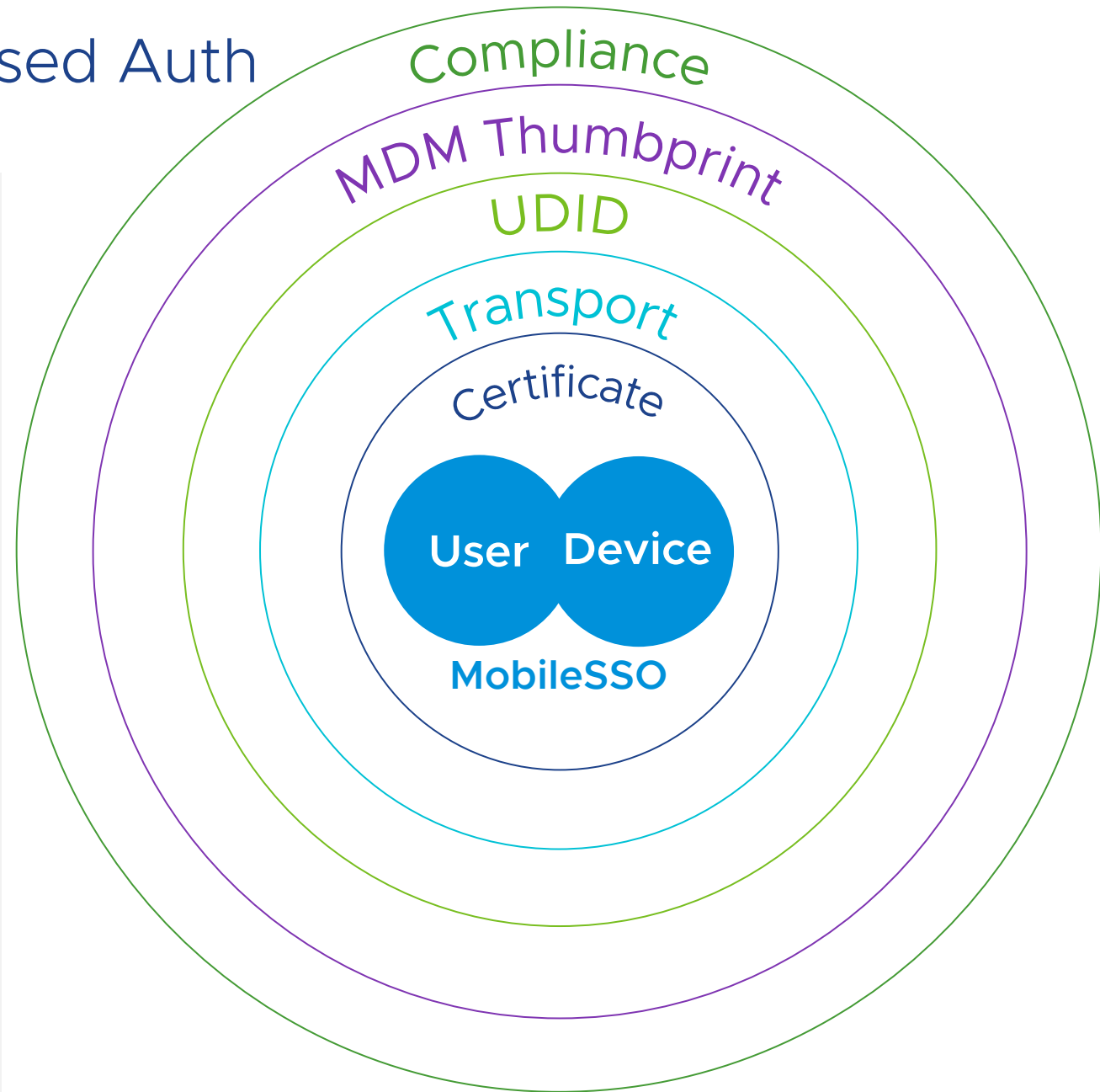
Implementing Seamless SSO

Anywhere as ONE



Workspace ONE Certificate Based Auth

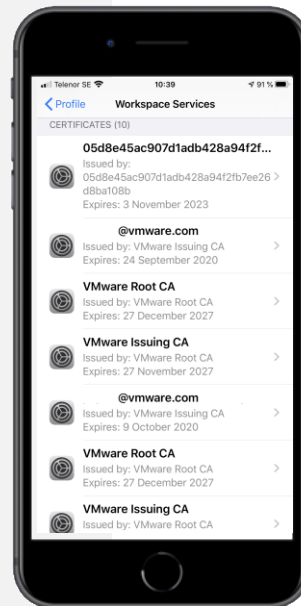
1. Signature, validation of chain, revocation
2. User Authorization
3. Transportation, how certificate is being delivered
4. Extract UDID, hardware ID
5. Enrollment status, MDM thumbprint
6. Compliance status



Mobile Challenges

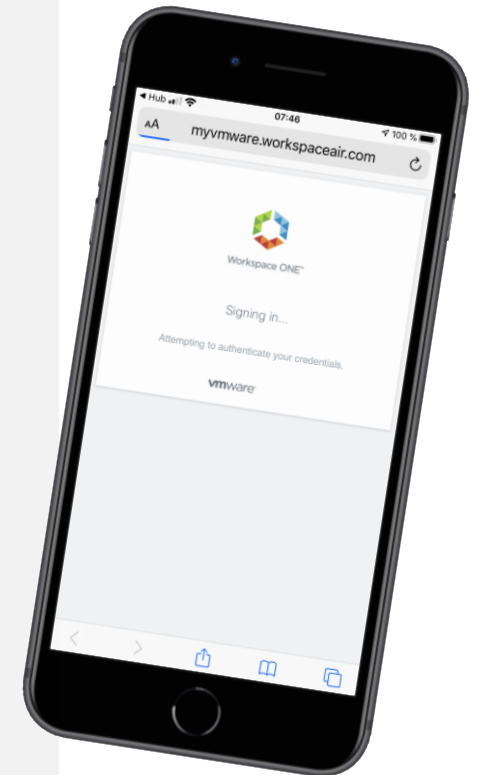
Traditional Mobile Certificate Authentication:

1. Proprietary certificate support
Not scalable
2. Requires local web browser or:
 - Safari view controller
 - Chrome custom tabs



VMware MobileSSO:

1. Universal application support
2. Since authentication flow is decoupled from the application itself, MobileSSO offers a near 100% application support.
3. Requiring no recoding
4. 100% Touchless authentication

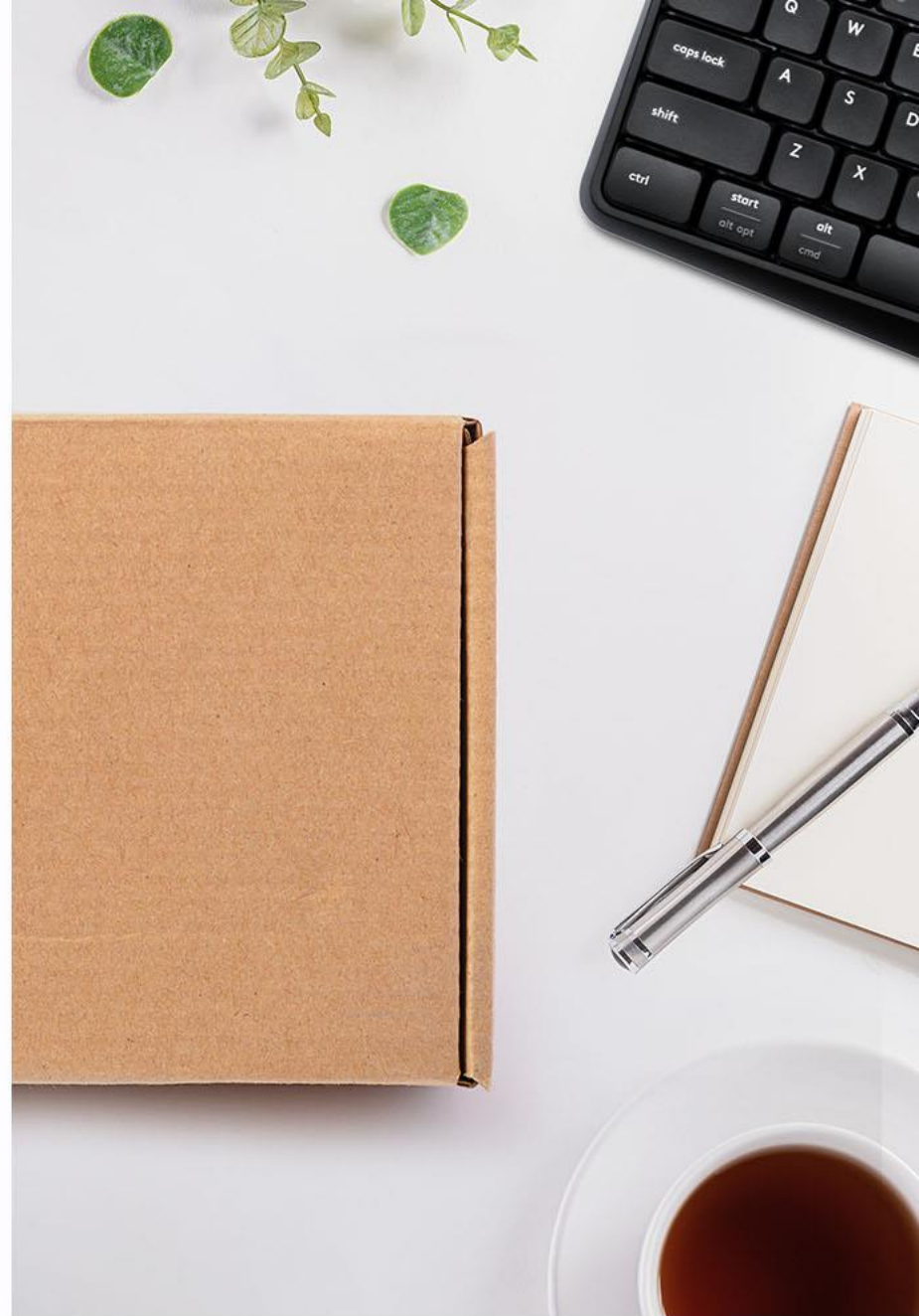


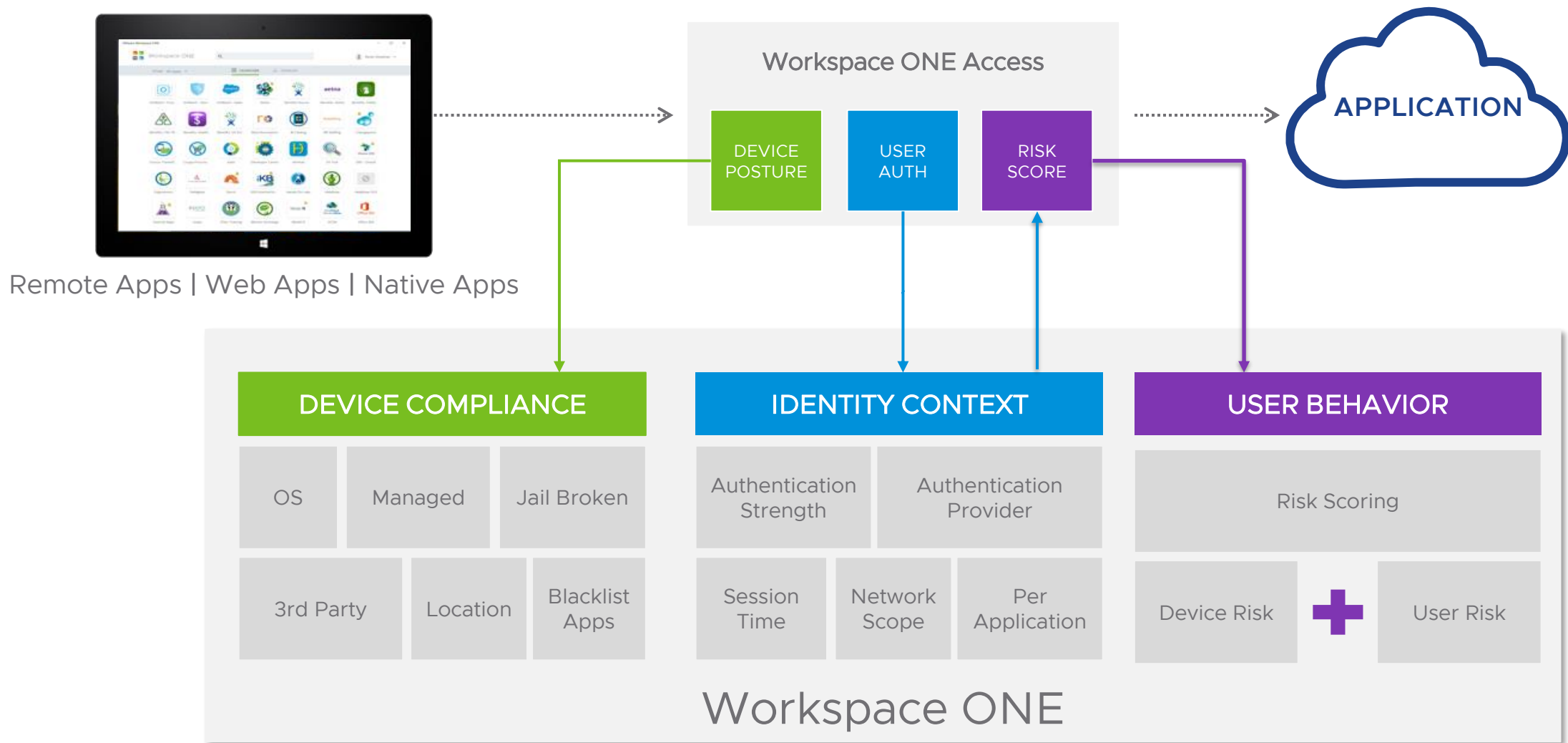


Stepping Up

Contextual & Risk based Access Rules

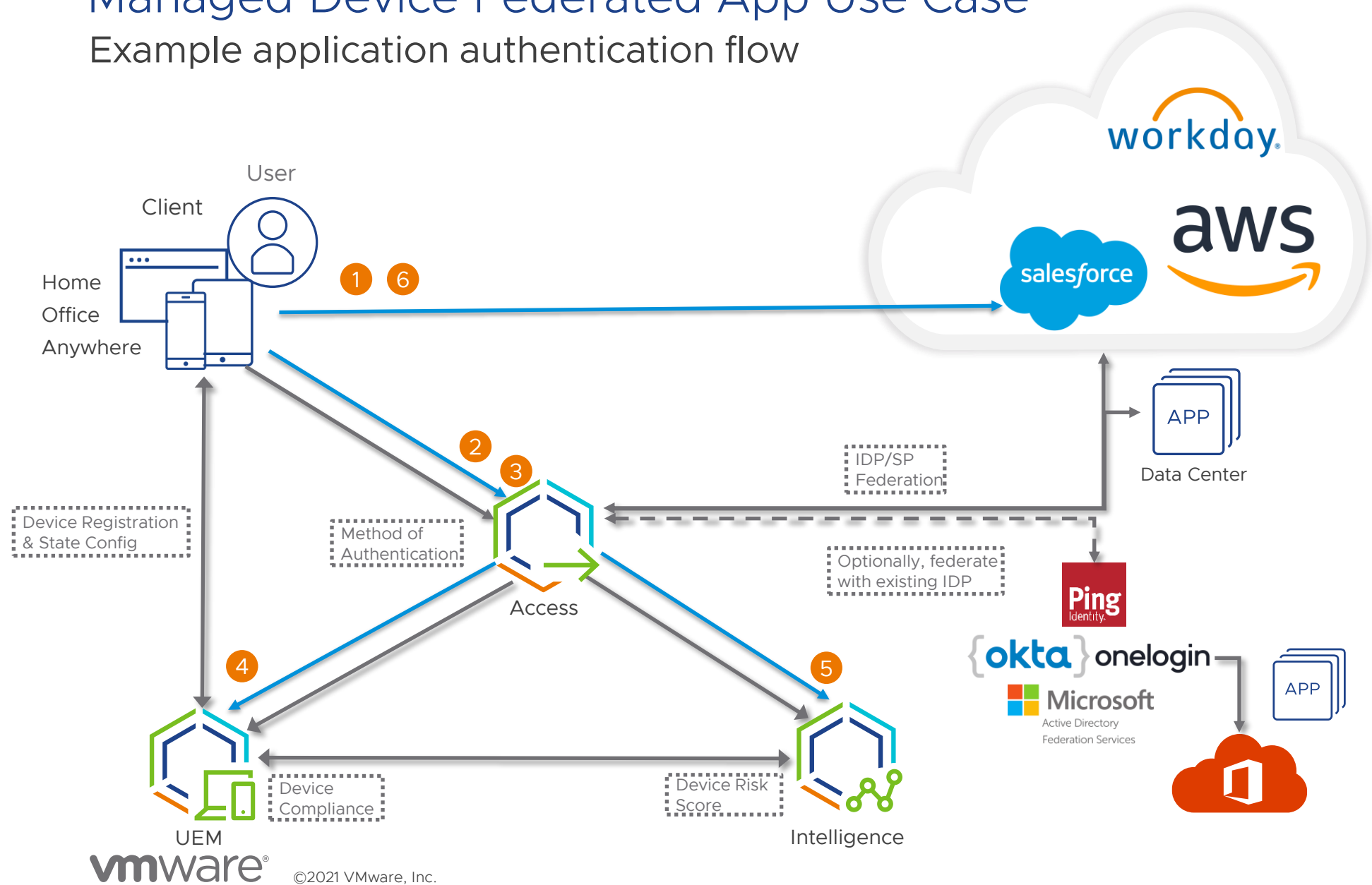
Anywhere as ONE





Managed Device Federated App Use Case

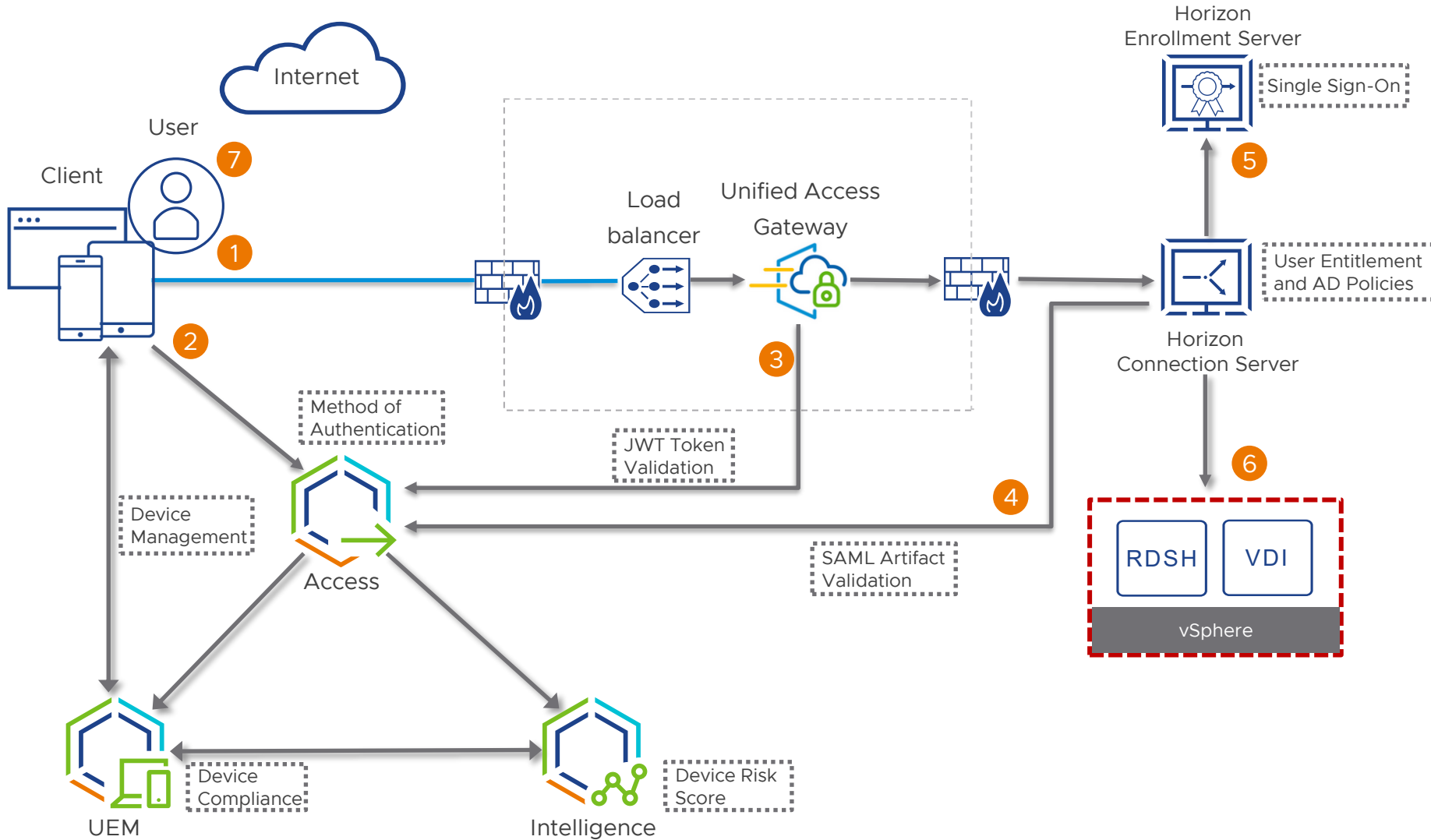
Example application authentication flow



1. Try to access Salesforce
2. Redirect to WSO Access
3. Cert based auth
4. Check Device Compliance
5. Get Login Risk Score
6. Send Assertion/ID Token to app

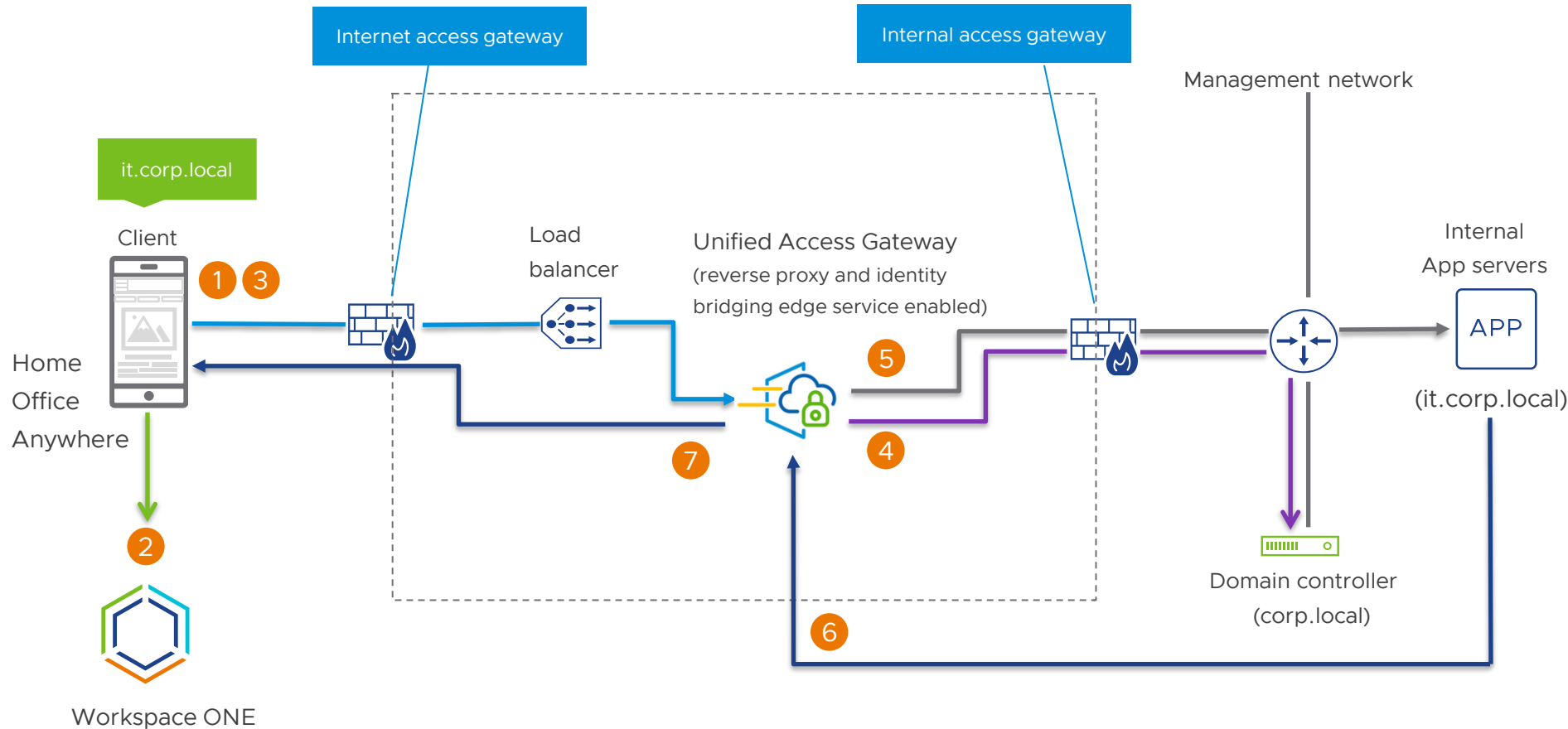
Managed Device VDI Use Case

Single Sign On of the user into their App or Desktop



1. User starts Horizon resource
2. Authenticate against WS1 Access with certificate and checking device compliance/risk
3. SAML Assertion contains JWT which UAG validates with Access
4. Horizon Connection Server uses SAML artifact to get SAML assertion
5. Uses Enrollment server to get short lived user certificate for login
6. User certificate is used with AD domain controller to login and get Kerberos ticket
7. User can start App/VDI

Managed Device Identity Bridging Use Case

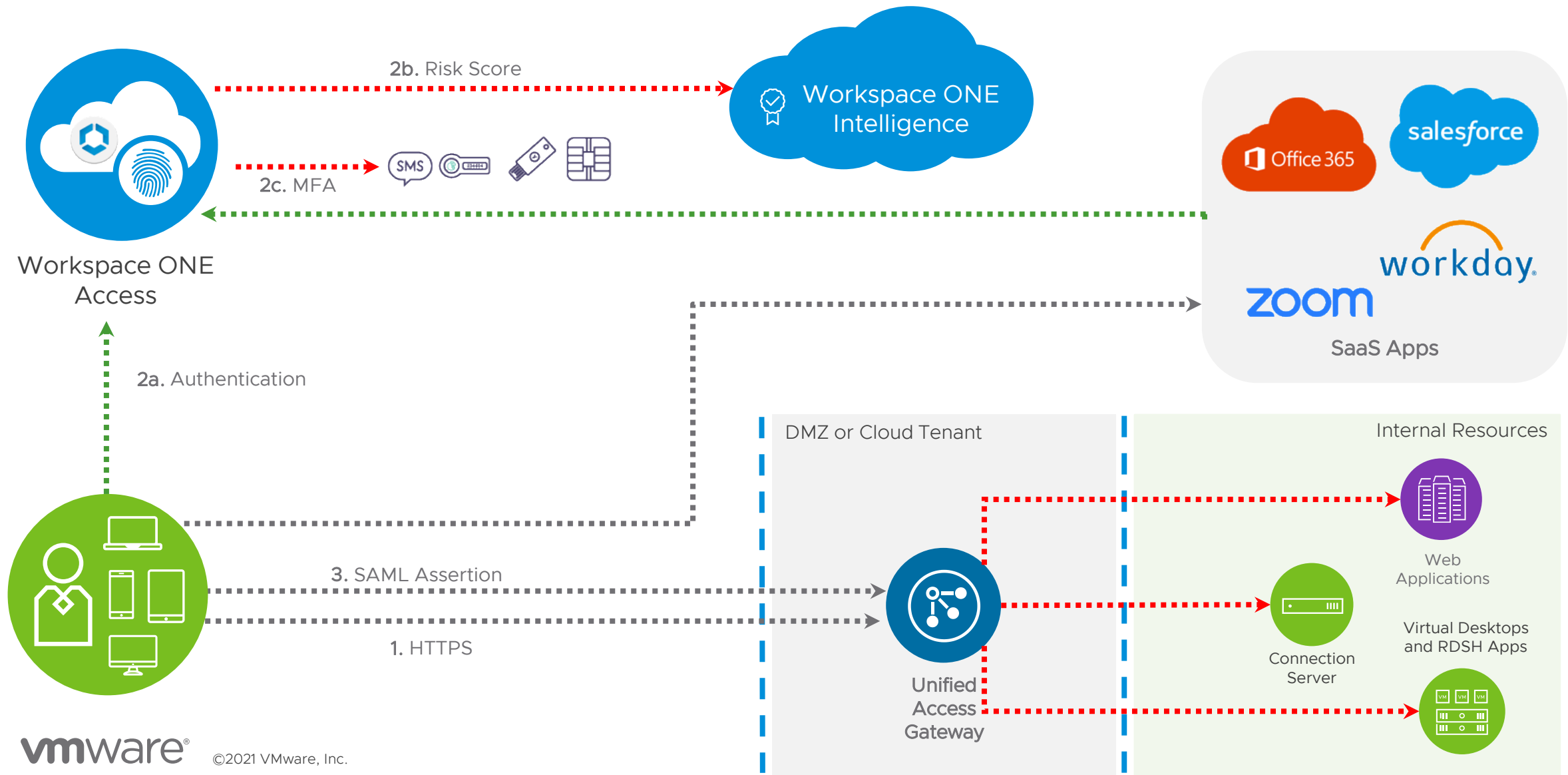


1. Connect in app or browser to uag.airwlab.com/it
2. Redirect to WS1 Access and Authentication
3. Use SAML assertion to ID user
4. UAG uses KCD to get a Kerberos ticket
5. UAG connects to internal app
6. <https://it.corp.local> connects back to UAG
7. uag.airwlab.com/it proxying <https://it.corp.local>

Risk Based Access Policies

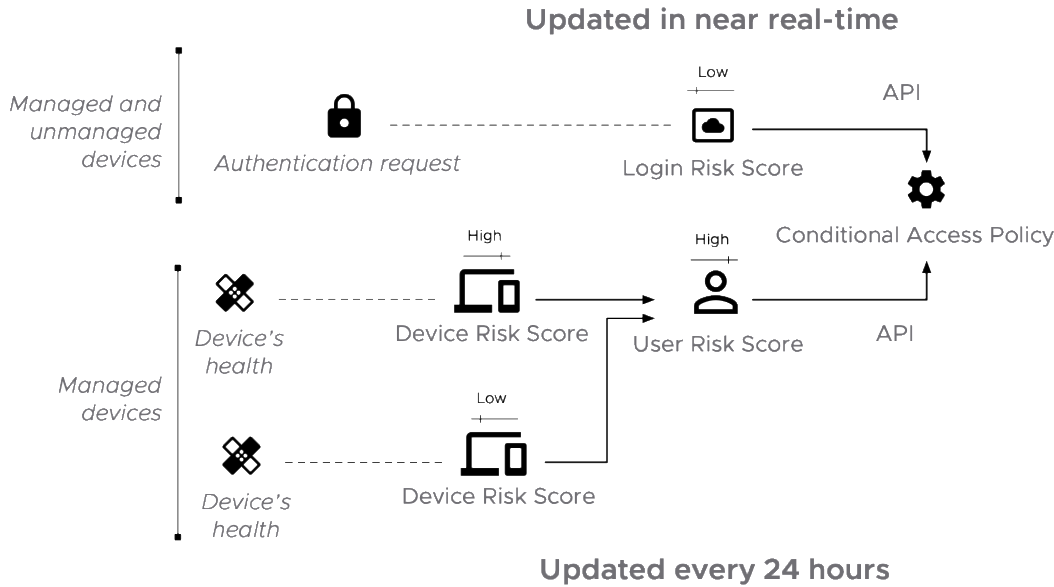
Extending Risk Analytics Across Workspace ONE Use Cases

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

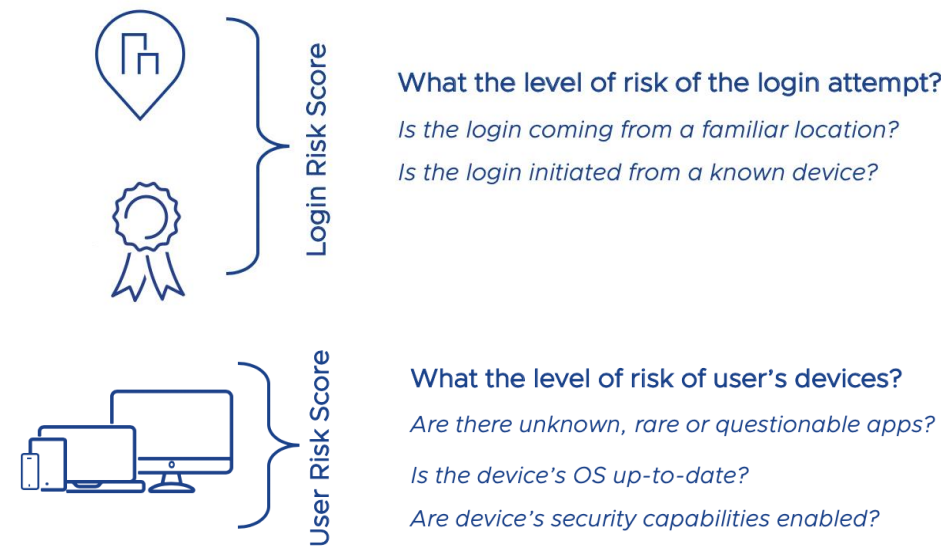


User vs Login Risk Score

Characteristics



Use cases



User/Device Risk Analytics Overview

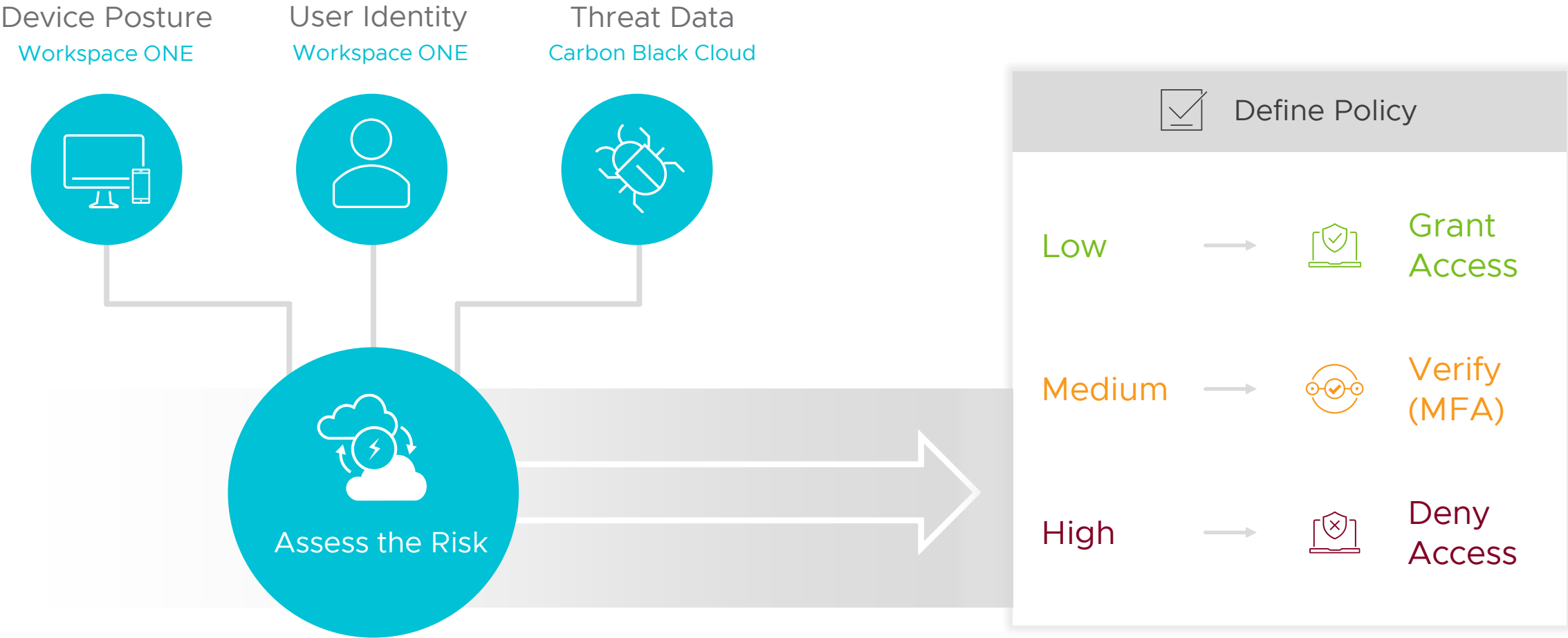
Device Risk Scoring:

- Android
- iOS
- macOS
- Windows

Risk Indicators	Description	Risk
Anomalous Alert Activity	A device that produces an unusual number, type, or severity of Carbon Black alerts.	An unusual number, type, or severity of threat alerts is an indication of a potentially compromised device.
App Collector	A person who installs an unusually large number of apps.	Any app can include known or unpatched vulnerabilities and these vulnerabilities can become attack vectors. The surface area for cyber-attacks increases with the number of apps on the device.
Compulsive App Download	A person who installs an atypical number of apps in a short period of time.	Users frenetically installing unusual apps on their devices have a greater risk of being a victim of malicious activity. Some apps disguise themselves as useful, friendly, or entertaining, when in fact they want to harm the user. Marketplace approaches to filtering unsafe content (malware) vary from vendor to vendor. A careless user can get tracked, hacked, or conned.
Excessive Critical CVEs	A device with an excessive number of unpatched critical CVEs (Common Vulnerability Exposure).	The greater the number of critical CVEs present on a device, the larger the device's attack surface.
Laggard Update	A person who sluggishly updates the device OS or who refuses to update at all.	Ignoring software updates can make a device vulnerable to attack and increases the risk of being compromised.
Persistent Critical CVEs	A device with one or many critical CVEs (Common Vulnerability Exposure) remaining unpatched after the majority of eligible devices in the organization were patched.	The greater the number of critical CVEs present on a device, the larger the device's attack surface.
Rare App Collector	A person who installs an unusually large number of rare apps.	Unlike widely used apps, rare ones are of questionable provenance and have a greater chance of having malware or security vulnerabilities.
Risky Security Setting	A person who owns one or many devices and has explicitly disabled security protection features or has devices explicitly declared lost.	Disabling security measures on a device increases the risk of being compromised.
Unusual App Download	A person who has recently installed unusual apps.	Apps can disguise themselves as useful, friendly, or entertaining, when in fact they want to harm the user. Marketplace approaches to filtering unsafe content (malware) vary from vendor to vendor. A careless user can get tracked, hacked, or conned.

User/Device Risk Based Conditional Access

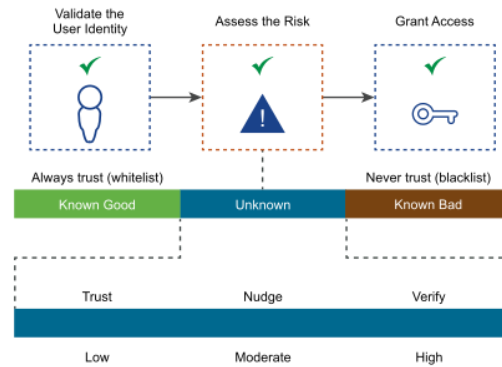
Adaptive policies that don't compromise user experience



Login Risk

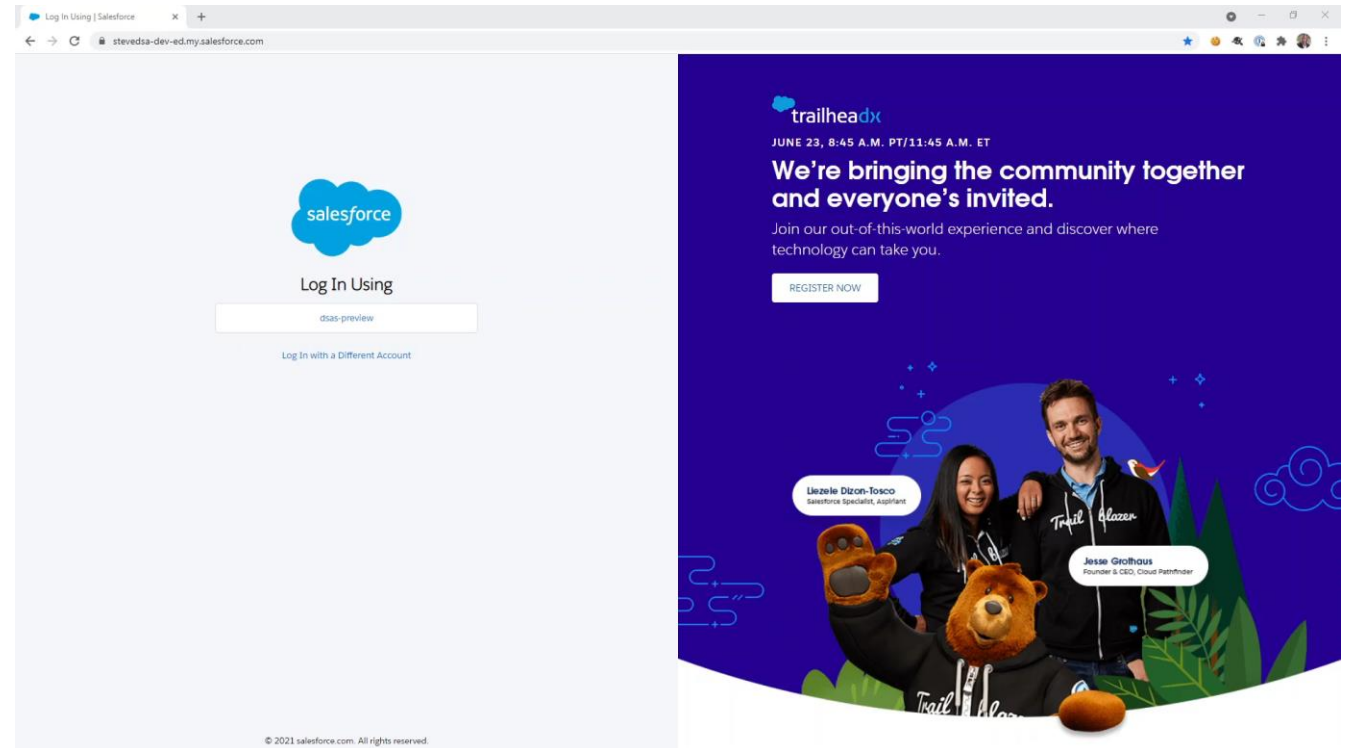
Define Access policies

- LOW Risk – Allow
- MEDIUM Risk – MFA Prompt
- HIGH Risk – Block

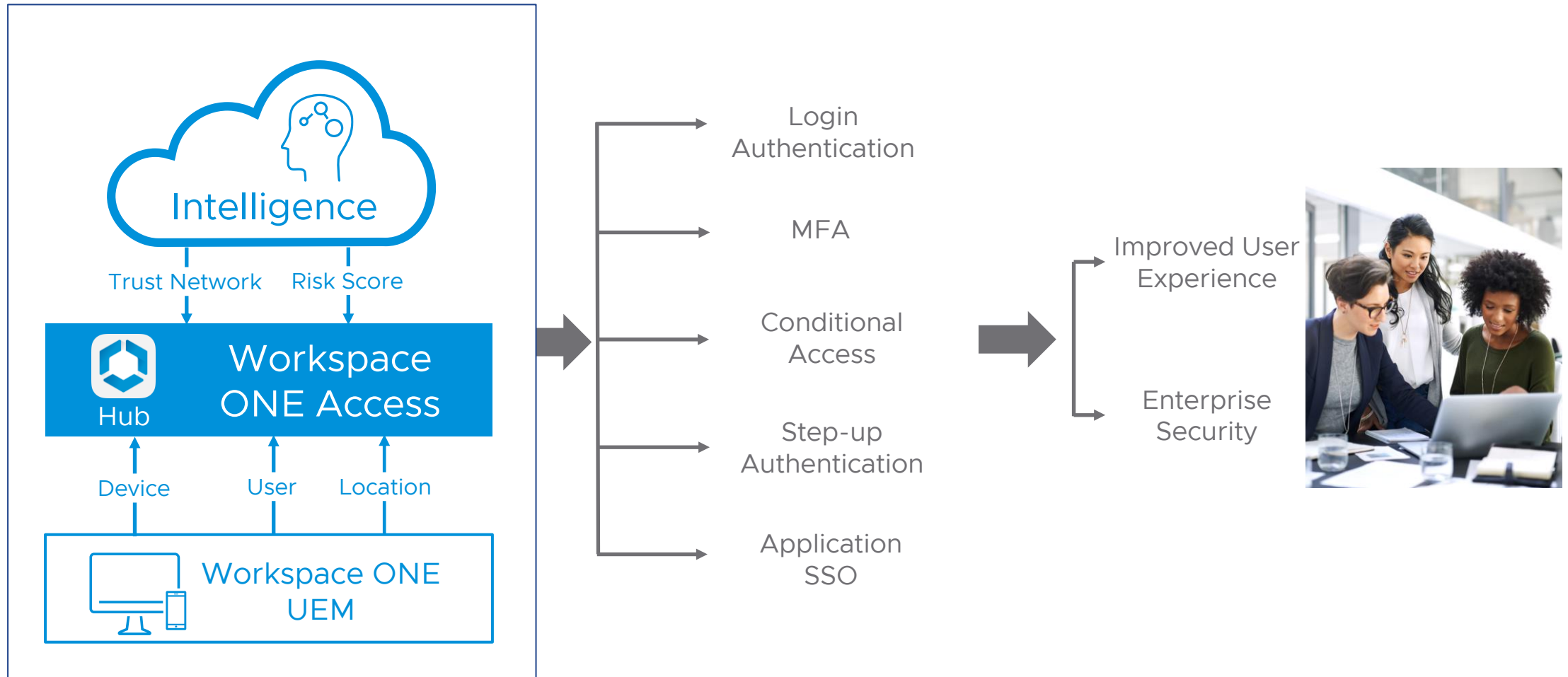


Calculated Realtime based on:

- Account historical login requests
- User location



Workspace ONE Access

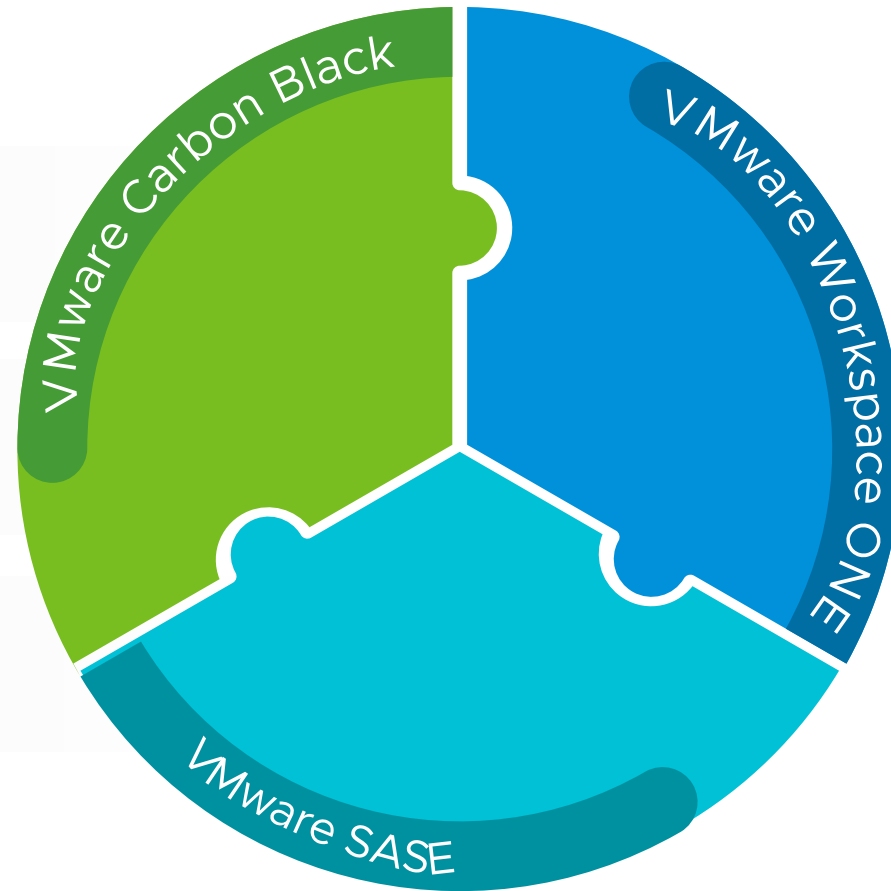


Anywhere Workspace Technologies

Manage Multi-modal
Employee Experience

Secure the
Distributed Edge

Automate the
Workspace



VMware Carbon Black

Cloud-Native | Endpoint Protection

VMware Workspace ONE

Unified Endpoint Management and
Virtual Apps and Desktop delivery

VMware SASE

Zero trust security and network
performance management

Integrated Technologies Across IT, Networking, and Security

Thank you!

vmworld®
IMAGINE
that