

# VMware Workspace ONE Privacy Disclosure

Effective Date: October 2023

## Introduction

This Privacy Disclosure covers VMware Workspace ONE Unified Endpoint Management (UEM), VMware Workspace ONE Access, VMware Workspace ONE Intelligence as well as the additional VMware Workspace ONE components described below (collectively, the “Software”). The purpose of this Privacy Disclosure is to inform customers who purchase the Software (“Customers”) and those individuals whose devices are being managed by the Software (“Users”) regarding the types of information collected by the Software about Users and their devices.

Users should be aware that the data collected by the Software depends on how the Customer configures the Software. Users should review the Customer’s privacy policies or notices. Additionally, VMware and its service providers may collect data when the Software is used, as well as Customer relationship data. VMware uses this data in accordance with VMware’s [Privacy Notice](#) and VMware’s [End User Terms and Conditions](#). The Customer is responsible for providing any necessary notices to its Users, and obtaining any legally required authorizations or consents from Users regarding use of the Software.

This Privacy Disclosure may be updated from time to time as new features and functionality are added. We encourage Customers and Users to periodically review this page. VMware is constantly updating and improving the Software to include new features and functionality. It is the responsibility of the Customer to ensure it uses the Software in accordance with its internal policies and legal requirements, including providing any required notice to Users and obtaining any required consents.

Below sections provide details of these components that are part of the Software:

- Workspace ONE UEM and VMware mobile applications
- Workspace ONE Access

- Workspace ONE Hub Services
- Workspace ONE Mobile Flows
- Workspace ONE Experience Workflows
- Workspace ONE Mobile Threat Defense
- Workspace ONE Intelligence

## **PART I: Workspace ONE UEM and VMware Mobile Applications**

This section covers VMware's unified endpoint management software, Workspace ONE UEM, including the related VMware mobile applications.

### **a. Overview of the Workspace ONE UEM**

Workspace ONE UEM ("UEM") enables Customers to protect the confidentiality, security and integrity of Customer systems and information that are accessed by Users from corporate-owned and User-owned devices. UEM provides the Customer with controls which enable them to manage the access and security of its User's devices. UEM consists of a Customer-specific console, which enables the Customer to manage its Users' devices ("Console") and software that is installed on a User's device, which (i) facilitates communication between the User's device and the Console, as well as other third-party endpoints (e.g. Apple or Google API) depending on Customer's configuration, and (ii) provides the User with various productivity applications (i.e. an email client, a web browser, etc.). The specific features available to a Customer or a Customer's Users will depend on the specific version/bundle purchased, how the Customer configures UEM, and which devices/platforms (i.e., iOS, Android, Windows, etc.) and mobile applications are used by the Users. The Console may be hosted by the Customer in its own IT environment ("On-Prem") or may be hosted by VMware ("Hosted Service").

### **b. Console Controls**

The Console provides Customers with controls to assist them in complying with their legal obligations and internal compliance programs and requirements. The specific features available to a Customer or a Customer's Users will depend on the specific version/bundle purchased, how the Customer configures UEM, and which devices/platforms (i.e., iOS, Android, Windows, etc.) and mobile applications are used by the Users. For example, the Customer can set password complexity, password expiration, and the timing for screen lockouts through the Console for the User's device. Customer can also choose to enable

different settings for corporate-owned devices and User-owned devices. Some of the other options available to Customers are outlined below:

**i. Infrastructure.** The Customer chooses whether to host the Console On-Prem or whether to have the Console hosted by VMware through the Hosted Service. If a Customer wants to maintain greater control over the environment hosting the Console, including the security thereof, the Customer can choose to host the Console On-Prem rather than having the Console hosted by VMware. The collected data is available to the Customer via the Console. If the Customer has chosen the Hosted Service, then VMware will also have access to the data collected through the Console; however, VMware only uses that data as stated in VMware's [Terms of Service](#) and [Privacy Notice](#).

**ii. Data Collection.** Using the Console, the Customer has the ability to control the types of information they collect about Users' devices. Additionally, the Console gives the Customer the ability to have different data collection practices for corporate-dedicated, corporate-shared, and User-owned devices. For example, through the Console, the Customer can enable or disable the collection of the following data:

- GPS Data
- Carrier/Country Code
- Roaming Status
- Cellular Usage Data
- Call Usage
- SMS Usage
- Device Phone Number
- Personal Applications
- Unmanaged Profiles
- Public IP Address

**iii. Device Commands.** Using the Console, the Customer can elect to allow/prevent certain commands and can decide whether the execution of a command requires the User's permission:

- Device Wipe
- Clear Device Passcode/Lock Device
- File Manager Access

- Remote Control
- Registry Manager
- Request Device Log
- Command Line/Remote Shell Access

**iv. Display of User Data.** The Console also contains settings that enable the Customer to decide what User data should be visible to its IT administrators via the Console. For example, the Customer can decide whether the following User data is visible to its IT administrators in the Console:

- First Name
- Last Name
- Phone Number
- Email Accounts
- User name

### **c. Collection of User and Device Data Through the UEM**

User data that may be collected by UEM varies depending on the specific version/bundle purchased by the Customer, how the Customer configures UEM, and which devices/platforms (i.e., iOS, Android, Windows, etc.) and mobile applications are used by the Users. Examples of the data that may be collected by UEM are provided below.

#### **i. General User and Device Data Collected by UEM**

In connection with its core enterprise mobility management functions, UEM collects user and device data such as the following:

##### ***Identity and Authentication Information***

- Identity details (including name, email address, phone number, etc.)
- Login credentials and security authentication data (including certificates, domain information, login and logout dates and times, usernames, enrollment IDs, etc.)

##### ***Employment Information***

- Employer, job title, work address, employee number
- Information maintained in the Customer's Active Directory

##### ***Device Information***

- Device type, name, make, model, manufacturer, and device identifiers such as universal unique identifier (“UUID”), International Mobile Station Equipment Identity (“IMEI”), mobile equipment identifier (“MEID”), serial number, International Mobile Subscriber Identity (“IMSI”) number, Internet Protocol (“IP”) address and Media Access Control (“MAC”) address
- Last seen information (i.e., when the device last connected to the Console), log data
- Information about the device’s operating system (including operating system build, version, firmware/kernel versions, etc.)
- Battery capacity and availability, memory capacity and availability, storage capacity and availability
- Installed profiles on the device, including configuration data of Users’ devices and compliance status concerning requirements defined by the Customer in its Console settings
- Information about the device’s file manager and registry manager (Android/Windows devices)

UEM also may collect user and device data in connection with the following:

#### ***Data about Customer-Managed Applications***

“Customer-Managed Applications” are Customer approved applications that are either pushed to User devices by the Customer or made available for download through the Workspace ONE Intelligent Hub app (formerly the AirWatch Agent), Workspace ONE App Catalog, or Customer application catalogues. These mobile applications may be public applications or internally-created applications. Information collected in connection with Customer-Managed Applications may include:

- Names and details of Customer-Managed Applications installed on the device, such as application name, version number, file size, configuration settings, installation progress status, app failure error codes, etc.
- Technical data generated from the use of Customer-Managed Applications, such as launch activities, clickstream data, crash reports and log files, which may contain personal data about the User.

***Data about Personal Applications:*** “Personal Applications” are the applications Users purchase or download from a public app store (e.g. the Apple App Store, the Google Play Store) to their devices. They are not automatically pushed to the User’s devices by Customer and are not managed via UEM. Depending on how the Customer has configured UEM, UEM may collect limited details about Personal Applications to assist the Customer in knowing/verifying that its Users do not download Personal Applications which may pose a security threat. UEM does not collect or have access to any data inside

any Personal Applications. The information collected about Personal Applications may include:

- Name, version, identifier, and total size of Personal Applications installed on the device

***File Manager Access:*** File manager access is functionality that allows read only access to a device's internal and external storage. Certain mobile applications (such as Workspace ONE Content, formerly known as VMware Content Locker) may request file manager access from a User so that data may be synced between the User's device and the Customer's systems, files could be attached to emails that the User wants to send, etc. When enabled, UEM may collect the contents of the device storage, including the SD card and locally stored files. Depending on how the Customer has configured UEM, certain applications like Workspace ONE Assist may have read and write access to the device file system based on the platform type and the permissions granted by the User.

***Telecom and Network Information:*** UEM may collect certain telecom data, such as carrier information, roaming status, and networks being used. This information helps the Customer know how the device is connected, to communicate with the device, and to enforce any restrictions implemented by Customer in its use of UEM, such as preventing large applications from automatically being pushed to a device that is roaming. Depending on how the Customer has configured UEM, this telecom and network information may include the following:

- Carrier information (including carrier settings versions, phone number, signal strength, roaming status, current and subscriber mobile country code and country location, current and subscriber mobile network code, SIM Carrier Network information, etc.)
- Information about the device's cellular technology (such as its Global System for Mobile Communications Standard ("GSM") and Code Division Multiple Access ("CDMA"))
- SSID, Internet Protocol ("IP") and Media Access Control ("MAC") addresses for the Wi-Fi network being used
- Amount of data used by the network connections, cellular data usage, and aggregated information about Wi-Fi bandwidth consumption (excluding content)

***Communication Data:*** The Customer may configure UEM to collect usage information, such as the number of calls and text messages sent or received. This information may assist the Customer in managing SMS limits on the Customer's cellular plan. UEM does

not collect or have access to the contents of text messages, phone calls, or personal email accounts. Depending on how the Customer has configured UEM, this communications data may include:

- The amount of data used, the number of SMS sent or received, phone call usage statistics (number of calls sent or received, duration of calls), broken down on an enrolled device phone number basis
- Name of sender, name of recipient, date, time

***Geo-location Data:*** Depending on how the Customer has configured UEM, UEM may collect geo-location data. By default, it does not collect geo-location data. UEM enables the Customer to collect geo-location data as it may enable a Customer to locate lost devices or to distribute functionality and content based on certain geo-fenced locations. Depending on the operating system and platform of the device, the User may be presented with an operating system notice, asking for the User's consent to collect geo-location data. The User can change their selection by going into their device settings and revoking the geo-location permission.

***Data via Remote Access:*** The Customer can use UEM to establish remote control access, which allows a Customer's IT administrators to assist in troubleshooting a User's device issue by remotely taking control of the device. A remote-control application must be installed on the device and, depending on platform and configuration, remote control may need to be approved by the User at the time when remote control is to be taken. This functionality enables the Customer to remotely access or control the device, including the use of remote locks, screen capture, remote device reboots or remote restart (for the device or applications).

## **ii. Additional Data for Specialized VMware Mobile App Functionality**

VMware provides various mobile applications in connection with UEM ("VMware Mobile Apps"). Some of these VMware Mobile Apps collect or share additional data in order to support their specialized functionality. For example, VMware Mobile Apps that provide VPN or internet browsing functionality (such as Boxer and Web) collect the URLs visited through those VMware Mobile Apps. The data collected and shared will vary depending on the functionality provided by the mobile application, as detailed further in the product documentation. Below are some examples of this additional data collected by specific VMware Mobile Apps:

- **VMware Workspace ONE Boxer.** Workspace ONE Boxer provides access to enterprise email, calendar and contacts. Boxer does not host the email or calendar content; instead, Boxer provides direct communication between the Customer's backend email system and the User's device. To operate, Boxer collects certain email header information (such as sender/recipient name, date, time, subject line, etc.) If configured to do so, Boxer has access to User device calendars to overlay the User's corporate calendar and access to User device contacts to display them in Boxer as well as to write corporate contacts to the device contact app for call identification purposes. Boxer may also be configured to collect header information and snippets of the email body in order to generate a contextual notification and send to a User's mobile device to deliver updates of incoming messages. The User can enable/disable these features via the UEM Console and mobile device operating system settings. Workspace ONE Boxer's use and transfer to any other app of information received from Google Accounts will adhere to Google API Services User Data Policy, including the Limited Use requirements.
- **VMware Workspace ONE Web.** Workspace ONE Web provides Users with secure VPN access to internet and intranet sites. It may also provide single sign-on capabilities allowing Users with access to the Customer designated web sites and web apps without the need to enter credentials. Web enables direct communication between Web on the User's device and Customer's backend systems. To operate, Web collects certain additional information such as the browser information and browsing history on the User's device. Web records the URLs of websites and web pages viewed using Web but Web does not give VMware access to the content viewed using Web. (For clarity, UEM may have access to that content to the extent the Customer maintains the content in VMware Hosted Services.)
- **VMware Workspace ONE Content.** Workspace ONE Content allows Customer content to be uploaded, stored, edited, shared and accessed from a User's device. The content is stored in a corporate container on the User's device or in a managed server-side repository, which the Customer may host using UEM (either On-Prem or in the Hosted Service, depending on the Customer's deployment) or which the Customer may maintain in third-party services. The Content mobile app allows the User to securely access, distribute and collaborate on content from their device. The Customer may configure Content to allow or limit access to certain content. If Content is used, UEM will have access to data such as the date and times when files are accessed and shared, file size, file names, a history of User actions inside the Content, and details regarding with whom the User interacts through Content. Content has a geo-fencing feature that allows the Customer's IT administrators to place geo-fencing restrictions on access to content stored in Content. The geo-fencing feature does not transmit the User's geo-location data to the Console; instead, the Content mobile application uses the geo-location data locally on the device to perform the geo-fencing.
- **VMware Workspace ONE Assist.** The Workspace ONE Assist application provides Customer's IT and support personnel with the ability to remotely view and control the device screen and applications, managed files and run commands with the User's permission. Assist also provides the ability to capture screenshots and record the device screen for troubleshooting and training purposes. The level of access is configurable by the Customer.
- **OEM Supplements to Agent App.** For certain Customers, VMware operates customized OEM (Original Equipment Manufacturer referring to the hardware or platform manufacturer) mobile applications that accompany its standard Workspace ONE Intelligent Hub, used for mobile device management. These OEM mobile applications may offer additional functionality and collect additional data points based on the Customer's and/or device's specifications.



For example, this may include information about carrier codes, battery health, and other data related to the Customer's device or product specifications.

**iii. Software Development Kit (SDK).** The Workspace ONE Software Development Kit ("Workspace ONE SDK") is a code library that mobile app developers can use to build security, configurations and management capabilities into their own, non-VMware mobile applications. Apps that use the Workspace ONE SDK collect and transmit certain data back to VMware, such as identity and authentication information and device information as described above, as well as crash reporting data and analytics data as described below. When an app uses the Workspace ONE SDK to provide tunneling functionality, the app also transmits to VMware's systems the URLs of the sites accessed using that tunneling functionality. Developers of third-party apps that use the Workspace ONE SDK also may configure the Workspace ONE SDK to collect other custom data points as they determine in their discretion. This Privacy Disclosure describes only VMware's collection of user data from the Workspace ONE SDK; it does not address the practices of third-party developers that may incorporate the Workspace ONE SDK into their non-VMware mobile apps.

#### **d. Intel Device Health and Chip to Cloud**

This section covers Intel Device Health and Chip to Cloud, which are optional add-on features powered by Intel and available for select Workspace ONE SKUs.

**i. Overview of the Intel Device Health Service.** Intel Device Health (IDH) helps Customers to protect the confidentiality, security and integrity of Customer systems and information that are accessed by Users from corporate-owned and User-owned laptops. IDH does this by helping to detect threats to the security of those laptops, particularly firmware-related threats. IDH threat analysis information is fed back to the Workspace ONE console where Customers can see and evaluate potential vulnerabilities of enrolled laptops. Customers may use this information to respond to threats by, for example, requiring end users to update their OS.

**ii. IDH Data Collection.** If IDH is enabled, enrolled laptops send data directly to Intel. Collected data includes information about installed operating system, Intel-based applications, drivers and BIOS; information about the device such as manufacturer, model number, serial number, SKU, and motherboard and CPU details; and country. Intel sends threat analysis results to VMware for display in the Workspace ONE console.

iii. **Use of IDH Data by Intel.** Intel uses the data collected not only to deliver the IDH threat analysis service, but also to enhance its own threat intelligence and threat detection capabilities. For information about how Intel will use that data, see the [Intel Privacy Notice](#).

iv. **Chip to Cloud.** Chip to Cloud functionality enables administrators to remotely perform power actions on Intel Active Management Technology (AMT)-enabled managed devices such as Power On, Power Off, Reset, and Power Cycle. Administrators may also remotely access the device to assume KVM (keyboard, video, mouse) control, including seeing the end user's screen, if the end user provides consent to such remote access at that time.

#### e. Device Wiping

UEM allows for two different types of device wiping:

- *Enterprise Wipe* – An Enterprise Wipe deletes all Customer-Managed Applications and any information stored in the Customer-Managed Applications. Enterprise Wipes will not remove Personal Applications or photos, videos, text messages, or personal email stored in Personal Applications.
- *Full Device Wipe* – A Full Device Wipe is a complete full factory reset. Full Device Wipes will remove all data and applications from the device.

The Customer's IT administrator may select which device wiping feature is enabled and can perform these wipes from the Console, either manually or via an automated compliance action. The ability to perform a Full Device Wipe for a device cannot be turned on for a particular device after enrollment, meaning if the setting is off when the User enrolls the device, the Customer cannot perform a Full Device Wipe on a User's device even if the Customer enables the Full Device Wipe setting in the Console. Depending on the Customer's configuration, Users may be able to choose to perform an Enterprise Wipe on their devices from the self-service portal.

## PART II: VMware Workspace ONE Access

This section covers Workspace ONE Access (formerly VMware Identity Manager, "Access"), which enables identity and access management as part of the Workspace ONE platform. Workspace ONE Access use cases include but are not limited to single sign on, multifactor authentication, conditional access, and identity security.

#### a. Overview of the Workspace ONE Access

Workspace ONE Access combines the User's identity with factors such as device and network information to make intelligence driven, conditional access decisions for applications delivered by Workspace ONE. Access acts as a broker to other identity stores and providers (such as Active Directory (AD), Active Directory Federation Services (ADFS), Azure AD, Okta and Ping Identity) that Customers may already be using to enable authentication across on-premises, SaaS, web and native applications without the need to rearchitect the identity environment.

## **b. Collection of User and Device Data Through the Access**

**i. User Data.** Workspace ONE Access collects data about Users who are using the Workspace ONE platform. Typically, the data is synced from Customer's directory with certain required attributes, as well as optional attributes that Customers can configure. Required User data that is synced with Access:

- Username
- Email
- First and last name

Customers can customize additional attributes to sync to Access for the purposes of policy creation or application entitlements.

**ii. Authentication Data.** When Users log in to the Workspace ONE platform using their username and password credentials, VMware does not store credentials in Access, but validates Users' input by reaching out to Customer's directory that Access has been integrated with, and validating the credentials.

In some cases, Access may cache credentials for the duration of User sessions on a User's device to enable features such as integration with other applications like VMware Horizon® or Citrix Virtual Apps and Desktops to prevent double prompting when Users launch virtual resources. This functionality can be configured or disabled by Customer's IT admin using Access.

Customers can also enable other authentication methods that do not involve credentials such as certificate-based authentication. To use certificate authentication, Customer IT administrators must upload root certificates and intermediate certificates to the Workspace ONE Access connector. The certificates are copied to the local certificate

store on the User device. These certificates are not replicated in the Workspace ONE Access database.

iii. **Logging Data.** Workspace ONE Access will also generate audit logs for all User activity. For instance, what applications User is launching, time of the launch, authentication methods used, etc. These logs can be retained within Workspace ONE Access, or they can be sent to Workspace ONE Intelligence for analytical purposes. For example, User login activity data can be used in Intelligence to identify user behavior anomalies and notify the Customer IT administrator. Sending logs to Intelligence is configurable and optional functionality.

## PART III: VMware Workspace ONE Hub Services

This section covers Workspace ONE Hub Services (“Hub Services”), which provide Users with a single destination to access, discover, and connect with corporate resources, applications, teams, and workflows via the Workspace ONE Intelligent Hub application.

### a. Overview of Workspace ONE Hub Services

Hub Services provide a collection of services that are co-located with Workspace ONE Access and can be deployed On-Prem or as a Hosted Service. Customers can choose to enable one or more Hub Services capabilities:

- **Hub Catalog.** Provides a branded and customized enterprise app store for native, web and virtual Customer apps for discovery and Single-Sign-On access by Users.
- **Notifications.** Provides personalized push and in-app notifications to Users of Customer communications including system downtimes, survey participation, and updates around enrollments.
- **People.** Provides employee directory for quick lookup of colleague information along with an organization chart.
- **Custom Tab.** Provides access to Customer resources through embeddable intranet or company portal within a customizable tab.
- **Support.** Provides self-service capability for Users to access helpful links and manage their devices.
- **Virtual Assistant.** Provides Users the ability to find answers to common Customer questions, troubleshoot issues and complete workflows like ordering a new device through a chatbot style interaction.

### b. Collection of User and Device Data Through Hub Services

i. **Authentication.** Hub Services relies on UEM or Access for user authentication as defined by Customer's IT administrator in the UEM Console as part of source of authentication configuration.

ii. **User Data.** Customers can use Hub Service admin console to create and send push notifications to Users. In addition, notifications can be generated based on changes in third party business systems when integrated via Workspace ONE Mobile Flows. Notification related data generated through Hub Services admin console or Mobile Flows is stored in Hub Services data store. In addition to the notification content, Hub Service collects individual notification acted on state, and target User device identifiers including UUID.

Customers can turn on the app rating feature to collect User feedback. When enabled, Hub Services collects User's external Id and app Id. Customer IT administrators can download a report of aggregated app ratings with following data points: App Name, App ID, Platform, App Version, App Type, Catalog Provider, Likes and Dislikes. Hub Services does not disclose individual User ratings for different apps to Customer's IT administrator.

When User favorites/unfavorites an app, Hub Services stores app Id favorited/unfavorited by User along with the device type to indicate the platform from which User has favorited/unfavorited the app from.

When User searches for a colleague using People tab, Hub Services stores the most recent search result for that User.

iii. **Logging Data.** Workspace ONE Hub Services generates audit logs for User activity. Hub Services logs the source of authentication (UEM or Access), username, external Id and app Id. For instance, app Id is logged: 1) when Users favorites or unfavorites an app; 2) when Users change the order of apps in favorites tab; 3) when install action is invoked on an app; or 4) when apps are launched from Hub Services app.

## PART IV: VMware Workspace ONE Mobile Flows

This section covers Workspace ONE Mobile Flows, ("Mobile Flows"), which is a Hosted Service built for the VMware Workspace ONE platform that provides contextual workflows and integrations to third-party systems or applications all within the digital workspace.

## **a. Overview of the Workspace ONE mobile flows**

Mobile Flows integrates with third-party systems or applications (e.g. Salesforce, Concur, Coupa, etc .) and presents standardized notifications within Workspace ONE applications (e.g. Workspace ONE Intelligent Hub or Workspace ONE Boxer). Mobile Flows allows Customers to leverage VMware out-of-the-box (“OOTB”) connectors or build their own custom connectors and configure them in the Workspace ONE UEM Console so their Users can complete tasks and/or take actions across third party systems or applications without leaving Workspace ONE applications.

## **b. Collection of User and Device Data Through the Workspace ONE Mobile Flows Software**

**i. Authentication Data.** Users are authenticated to the third-party systems or applications to see contextual information and take actions in those systems via VMware Workspace ONE Access by providing a signed token to identify the User, which is used to exchange User access tokens with federated third-party systems. These access tokens are encrypted and cached for rapid retrieval, and are deleted on expiration within the Mobile Flows service. Mobile Flows supports multiple authentication types for third-party systems so the exact token exchange flow may vary depending on the system.

**ii. Stateless Connectors to Backend Systems.** If Customers choose to use the OOTB connectors, Mobile Flows will process information from third-party systems and send it in a structure format to the Workspace ONE applications. All connectors deployed as out-of-the-box are stateless, holding no data about the request and response, completing all work in a single call, and logging no personally identifiable information to logs.

## **PART V: VMware Workspace ONE Experience Workflows**

This section covers Experience Workflows powered by Boomi, which is an optional feature add-on available for Hub Services.

## **a. Overview of the Workspace ONE Experience Workflows**

Experience Workflows is powered by Boomi and enables integration with third-party systems or applications (e.g., Salesforce, Concur, Coupa, etc.) to present standardized notifications within Workspace ONE Intelligent Hub. Experience Workflows allows

Customers to leverage VMware out-of-the-box (“OOTB”) integration packs or build their own custom integrations and configure them in Workspace ONE Hub Services and Boom! AtomSphere so their Users can complete tasks and/or take actions across third party systems or applications without leaving Workspace ONE Intelligent Hub.

## **b. Collection of User and Device Data Through the Workspace ONE Experience Workflows Software**

**i. Stateless Integrations to Backend Systems.** If Customers choose to use the OOTB integration packs, Experience Workflows will process information from third-party systems and send it in a structure format to the Workspace ONE Intelligent Hub. All integration packs deployed as out-of-the-box are stateless, holding no data about the request and response, completing all work in a single call, and logging no personally identifiable information to logs. The information sent by Workspace ONE through Experience Workflows will depend on the use case and nature of the third party system being integrated. Please check with your third party vendor(s) for information about their applicable privacy policies and disclosures.

## **PART VI: VMware Workspace ONE Mobile Threat Defense and Mobile Applications Powered by Lookout**

This section covers Workspace ONE Mobile Threat Defense service (“MTD”), which is an optional feature add-on available for Hub Services and is a Hosted Service powered by Lookout, Inc., including the related mobile applications.

### **a. Overview of the Workspace ONE Mobile Threat Defense Service**

The Workspace ONE Mobile Threat Defense service helps Customers to protect the confidentiality, security and integrity of Customer systems and information that are accessed by Users from corporate-owned and User-owned devices by helping to detect and protect against threats to the security of those devices. MTD provides the Customer with controls which enable them to respond to threats to enrolled mobile devices. MTD consists of a Customer-specific console, which enables the Customer to monitor threats to its Users’ devices (“Console”), and software that is installed on a User’s device. The specific features available, and the applicable on-device software application, will depend on the specific version/bundle purchased, how the Customer configures MTD, and which

devices/platforms (i.e., iOS, Android, Windows, etc.) are used by the Users. The Console is hosted by VMware's service provider, Lookout, Inc.

## **b. Console Controls**

The specific features and settings available through the Console will depend on the specific version/bundle purchased and which devices/platforms (i.e., iOS, Android, Windows, etc.) are used by the Users. Customer can also choose to enable different settings for corporate-owned devices and User-owned devices. In the Console, Customers can customize threat classifications and set their own threat response policies accordingly (e.g., Alert, Warn, Block, etc.). Some of the other options available to Customers are outlined below:

### **i. Data Collection**

Customer may elect for the Console to maintain a username and email address for each enrolled device, or may elect for the Console to rely solely on a pseudonymized Device ID provided by the UEM platform. With the latter option, Customers' administrators would need access to the UEM platform to make the association between the device threat data within the Console and the individual User.

### **ii. Display of User Data**

Customers may elect to redact certain fields within threat data from administrators' view within the Console. Fields that may be redacted include IP address and resultant geolocation, SSID of suspect networks, name of suspect apps, and suspect or blocked URLs and domains.

## **c. Collection of User and Device Data for MTD**

User data that may be collected by MTD varies depending on the specific version/bundle purchased by the Customer, how the Customer configures MTD, and which devices/platforms (i.e., iOS, Android, Windows, etc.) and mobile applications are used by the Users. Examples of data collected by MTD are provided below.

### ***Device and User Identifiers***



- Device type, name, make, model and manufacturer
- Username, email address, IP address

### *Firmware / OS / Configuration Data*

- Information about the device's operating system (including operating system build, version, firmware/kernel versions, configurations, etc.)
- Various security hygiene details such as developer mode status, whether storage encrypted, whether side loading of apps allowed, whether Bluetooth is enabled, whether lock screen is enabled

### *Application Data*

- No user-generated data from within applications is processed or collected (e.g., messages within a messaging app are not processed or collected)
- For Android devices, a list of installed apps and version details are collected for analysis. If the device is managed using Android's 'Work Profile,' the analyzed apps may be limited to those in the Work Profile.
- For iOS devices, the list of installed apps is only collected if Customer configures Workspace ONE UEM to provide such information. Customer may configure Workspace ONE UEM to limit the list to work apps.
- The name of an app installed on a specific User's device is only available to the Customer if the app is suspected of posing a threat and if the Customers' privacy controls permit administrators to see names of suspect apps.
- App data collected includes SHA-1 hash, Package name, APK file, Bundle ID & Team ID, app/file name, app bundle/package names, application metadata

### *Network Data*

- Network name (SSID) and network analysis details are collected for suspect WiFi networks only. Whether the suspect SSID is visible to Customer administrators depends on the Customer's privacy controls.

### *Phishing and Content Protection (PCP) Data*

- Data collected includes blocked and suspect URLs and domains, number of URLs and domains checked and number of URLs and domains blocked or detected as suspect
- URLs and domains that Users click on are processed against lists of suspect and blocked URLs and domains. URLs and domains clicked on are not recorded by MTD unless flagged as suspect or blocked. Block lists are established by Customers.
- The fact that a User tried to access a blocked or suspect URL or domain, and why the URL or domain was flagged as suspect or blocked, is visible to

the Customer Administrators, but the specific blocked or suspect URL or domain is not visible to Customer Administrators.

- For Android devices, Customers may configure PCP to apply only to URLs and domains clicked on from apps in the 'Work Profile.'
- For iOS devices, no apps bypass PCP; all URLs and domains clicked on are analyzed.

## **PART VII: VMware Workspace ONE Intelligence Software**

This section covers Workspace ONE Intelligence ("Intelligence"), which is a Hosted Service built for the VMware Workspace ONE platform that provides insights, analytics and automation for the entire digital workspace.

### **a. Overview of the Workspace ONE Intelligence**

Workspace ONE Intelligence Software provides insights into a Customer's digital workspace by aggregating and correlating device, application and User data together from multiple data sources in one place to give Customer's IT administrators a complete view of their entire digital workspace environment. Customers can use reports and dashboards to monitor trends and take actions using the automation feature to mitigate issues. Customers opt-in for Workspace ONE Intelligence using the UEM console to access the Intelligence console and configure the data sources that Customer wishes to use. Workspace ONE Intelligence is able to ingest data from the following sources:

- Workspace ONE UEM
- Workspace ONE Access
- Common Vulnerabilities and Exposure (CVE) data from its database
- App Analytics data from Workspace ONE Intelligence SDK
- Workspace ONE Trust Network data from technology partners

### **b. Collection of User and Device Data Through the Workspace ONE Intelligence Software**

**i. Data Collection from UEM.** UEM data flows to Intelligence only after Customer has opted in. The type of data collected from UEM depend on the privacy controls that the Customer has configured. Refer to the UEM section for details on privacy controls.

The Workspace ONE Intelligent Hub app also sends app health, and device health data from corporate-dedicated and corporate-shared Windows devices directly to Intelligence

once Customer opts in to this feature in the UEM console. This data may include app crashes, app hang, OS crashes, boot time, logon/shutdown time, windows service start/stop events, sleep and wake events, and device performance monitoring data. This feature is not available for User-owned devices (BYOD).

Customers can use this data set to create dashboards and reports to monitor different key performance indices (KPIs) for maintenance and visibility. Customers can also use the automation feature to take actions on devices, and issue notifications.

**ii. Data Collection from Access.** Customers configure Access integration in Intelligence to allow data from Access to flow into Intelligence platform. The type of data may include app logon and logout events. Please refer to Access section for details.

For example, Customers can use this data set to check User login trend, unique User logins, login failure by authentication method and top 5 apps launched in last week.

**iii. Data Collection from CVE.** Intelligence retrieves list of common vulnerabilities and exposure entries from the CVE database. This list includes publicly known cybersecurity vulnerabilities. Customers can use this data to measure security threats to their digital workspace and take actions to mitigate issues. Details of these integration and data collection are also provided in Workspace ONE Intelligence documentation which can be reviewed [here](#).

**iv. Data Collection from Trust Network Technology Partners.** The type of data collected by Intelligence depends upon the privacy settings and terms of agreement between Customer and Trust Network technology partners. Workspace ONE Intelligence can integrate with Trust Network technology partners by configuring technology partner's APIs in Intelligence to ingest data or allowing Customer to create credentials for technology partner to use Intelligence APIs to send data to Intelligence. The type of integration is determined by the Customer.

Sample data available in Intelligence from Trust Network technology partners may include but is not limited to:

- Device Unique IDs – UDID, IP, MAC, Serial Number
- End user's name
- Email address

- Apps details
- Network information
- Apps usage data
- Security health of devices

Customers can use this data set to improve visibility across their organization for security threats and take actions using the automation feature to take actions to mitigate the risks.

**v. Data collection from Intelligence SDK.** By integrating the Workspace ONE Intelligence Software Development Kit (the “Intelligence SDK”), Customers can analyze and interact with data about app engagement, app failures, network insights, and user flows. Sample of data may include:

- App Start
- Crashes
- Handled Exceptions
- Network Errors
- Latency

VMware mobile applications also use Intelligence SDK. Please visit UEM section for details.

Customers use this data set to find the root cause of crashes and other application errors quickly, and to prioritize which crashes need to be fixed in order to improve application engagement and usage.

Details of this integration and data collection are also provided in Workspace ONE Intelligence documentation [here](#).

## **PART VIII: Crash Reporting**

The Software can collect crash reports, including those from the VMware Mobile Apps (“Crash Reports”). A Customer IT administrator can disable the collection of Crash Reports via the Console settings. Crash Reports may contain User data, such as IP/MAC address, device Information (including unique identifiers, device type, carrier, operating system, model, system, etc.), and geo-location information. Crash Reports are provided to the Customer via the Software to enable the Customer to troubleshoot User issues. VMware

may also use Crash Reports to improve our products and services and troubleshoot and provide support to our Customers.

## **PART IX: Analytics Data**

VMware collects certain configuration, performance, usage and other analytics data from our Customers and our Customer's Users for a variety of purposes including to improve our products and services, fix problems, help us understand better how our Customers use our products and services, and advise our Customers on how best to deploy and use our products and services. There are several different data collection programs that a Customer/User may participate in when using the Workspace ONE branded products and services. Please see the [VMware Trust & Assurance](#) page for more information.

## **PART X: Operational Data**

VMware may monitor and collect configuration, performance, usage, and consumption data relating to Customer's and its Users' use of the Software to facilitate the delivery and operation of the products and services (collectively, "Operational Data") as described in the [VMware Privacy Notice](#).

## **PART XI: User Transparency**

As part of the device enrollment process, the Software pushes a privacy dialog to the User's mobile device, which enables the User to review a summary of the settings enabled for the Software on their device. In some cases, the User may also have the ability to control the enablement of certain features of the Software, via the self-service portal and/or their device settings. Most VMware Mobile Apps made available by VMware have a privacy dialog that includes (i) an overview of the data collected by the mobile application, (ii) the permissions that the mobile application will request, and (iii) an option to send analytics data to VMware (unless the Customer has disabled the sending of analytics data for all Users). The Software also provides functionality that Customers can use through the Console to provide Users with a link to their privacy notice via the privacy dialog.

The portions of the Software that allow devices to be monitored by the Console run in the background of the devices, and may not provide additional notice when these functions are occurring in real time.

## **PART XII: Data Subject Access Requests**

VMware has no direct relationship with the Users whose data it processes in connection with providing the Software and any related services. A User who seeks access, or who seeks to correct, amend, or delete inaccurate data should direct their query to the Customer. If the Customer requests VMware to modify or remove the data, we will respond to the Customer's request in accordance with our agreement with the applicable Customer or as may otherwise be required by applicable law.

## **PART XIII: Contact Us**

If you have any questions or concerns regarding this Privacy Disclosure, you may write to us at [privacy@vmware.com](mailto:privacy@vmware.com) or by mail to: Office of the General Counsel of VMware, Inc., 3401 Hillview Ave, Palo Alto, California, 94304, USA.