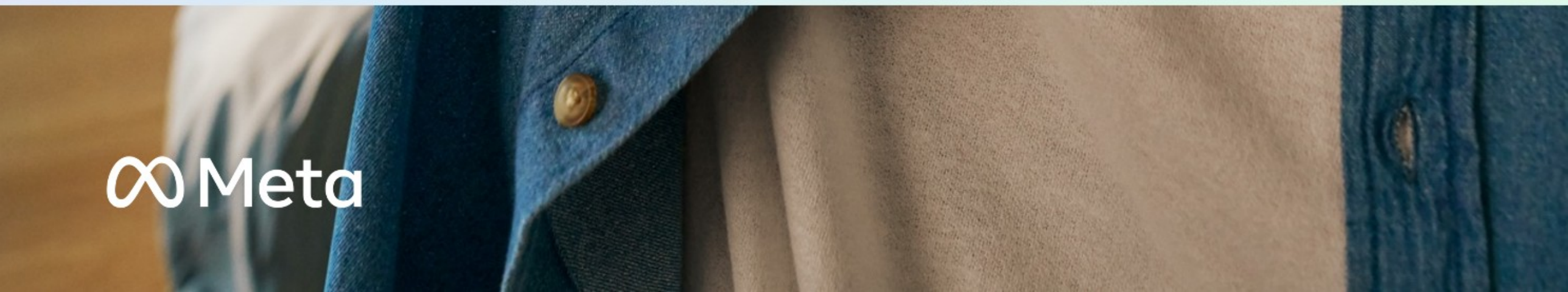
Meta Quest for Business

Security and Privacy Whitepaper



Contents

Introduction

Meta Quest for Business allows your organization to experience the full potential of immersive and blended reality with Meta Quest. It makes it easy to scale the power of Meta Quest across your organization, unlock new work solutions, and empower new ways of working.

With essential features like user management, device management, app management, and customer support, Quest for Business makes your Meta Quest 2, Meta Quest 3, and Meta Quest Pro devices work-ready.

Protecting data across Meta Quest devices and Meta Quest for Business is our top priority. Your Customer Data* will only be used for stated purposes. Meta does not sell Customer Data or use it for any other purpose, including personalizing consumer Meta Products or advertising.

This whitepaper provides an overview of the security and privacy investments made by Meta to protect your data.

“Customer Data“ is the data and content submitted by Customer or by its authorized Users (including user and device configuration information) while using the following web tools: Meta Admin Center and the managed Accounts Center.However, Customer Data excludes:(i) data shared with the Meta Quest operating system that is utilized to perform necessary functions, such as downloading and running applications, network connections, device configurations and third-party device management configurations;(ii) data that you permit to share with other apps, and that may be subject to other terms and policies; and(iii) the content you or your authorized users provide when providing feedback or reporting bugs, and communications with technical support, through Admin Center.

How Meta Quest for Business makes Meta Quest devices more secure

Quest for Business includes a number of management controls and security features designed to meet common IT requirements and help your organization adopt Meta Quest devices.

Configure security settings with Quest for Business

Through Quest for Business, you can control and monitor your fleet of Meta Quest devices and configure them to meet the security standards and requirements of your organization using the below features:

Network configuration (VPN support, Wi-Fi)
Admin Center offers VPN support for vendors, including Cisco and VMware. It also supports EAP-TLS for certificate-based Wi-Fi in enterprise environments. This allows people in an organization to connect their Meta Quest devices to their corporate Wi-Fi networks.

OS update controls
Admins can control whether OS updates are automatically applied to Meta Quest devices, delayed up to 30 days or set to a defined time to minimize work disruption. This can help maintain a balance between device security and productivity of people in an organization.

PIN requirements
Admins can ensure that the Meta Quest device is only used by its assigned person, enforcing a PIN code to unlock a device each time it's accessed. Admins can also specify the complexity requirements of the device PIN.

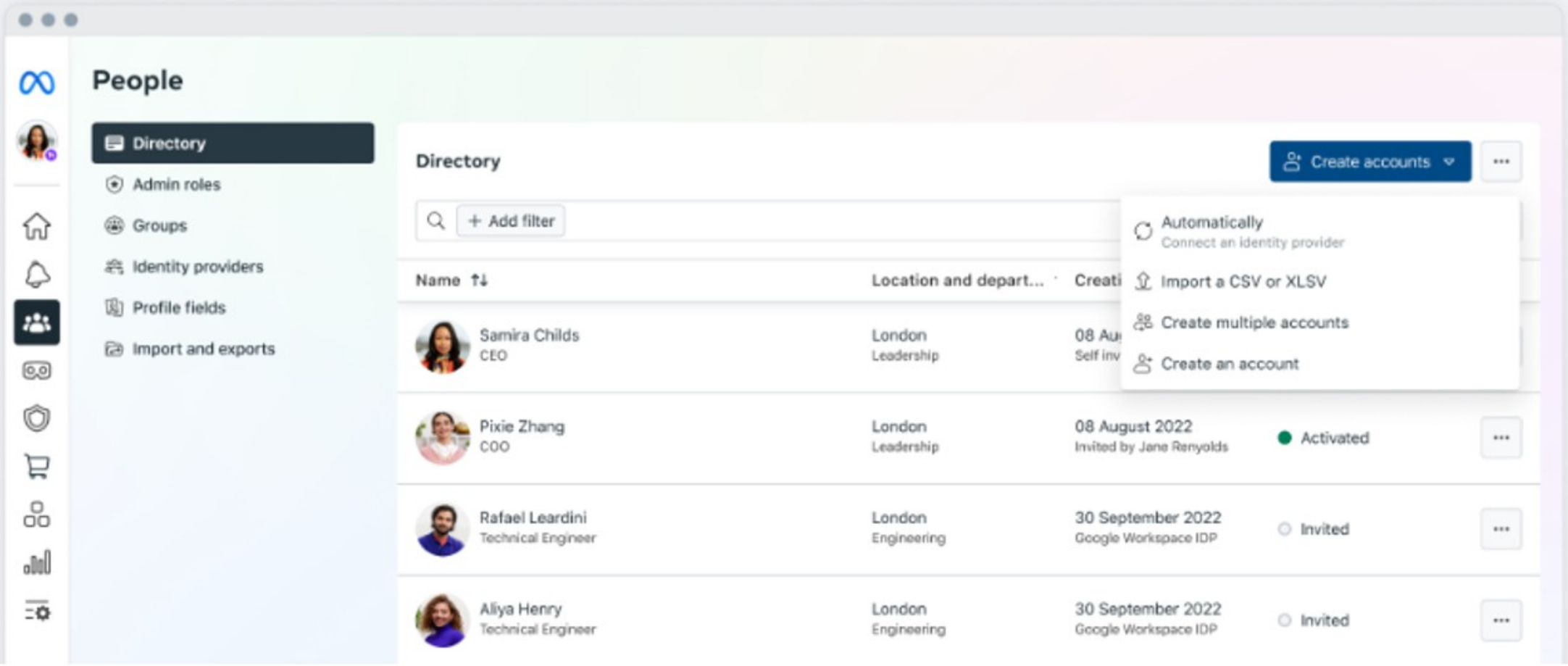
Quest for Business also enables your organization to monitor changes in your Meta Quest device security status, and provides:

On-device root detection
Admins can detect Meta Quest devices that have root access - a common pre-condition to malware attacks - and set security rules to trigger actions based on root potential (note: currently only available with Admin Center device manager). These actions include automatic remote wipe and admin notifications (security alert and email) for compromised devices. Admins can also detect if the device bootloader has been unlocked without permission or has been tampered with.

Security rules and alerts
Admins can receive prompt alerts about detected anomalous or malicious activity, and review historical security events in the Admin Center.

Security logs
Admins can review security events such as provisioning actions or password changes in the Security Log tab.

Remote wipe
Meta Quest devices can be wiped of user and on-device data via the Admin Center remotely or it can be configured to automatically wipe in certain situations, like when root access is detected.



Enable secure access and authentication with Meta Quest for Business[1]

Through Quest for Business, admins can manage access to Meta Quest headsets through the Admin Center and manage and provision accounts for the organization through automated provisioning and integration with major identity providers.

Meta accounts managed by your organization

When you deploy Quest for Business, your organization's admin can create Meta accounts for people using managed Meta Quest devices. These accounts—which this document will refer to as managed Meta accounts—allow access to the full ecosystem of Meta Quest applications.

Single sign-on (SSO)

Quest for Business helps organizations streamline user access by enabling single sign-on on Meta Quest devices. People in your organization can then leverage their corporate credentials to sign in.

Identity integrations

Quest for Business currently integrates with several identity providers (IdP), including Microsoft Azure AD, Google Workspace Directory and Okta, which offer native app connectors to make SSO and automated provisioning easier. Quest for Business supports SAML 2.0 for authentication and offers a SCIM 2.0 API for automated provisioning, allowing admins to develop custom connectors for account management if the existing identity provider doesn't have a built-in integration. Admins can also implement SAML 2.0 single logout (SLO) to improve security by ensuring people within the organization are fully logged out from all sessions, depending on the IdP session - reducing the risk of session hijacking.

[1] Features discussed in this section apply to headsets configured in Individual Mode. They do not apply to headsets configured in Shared Mode. See below for more information about these configurations.

Two-factor authentication

Two-factor authentication (2FA) adds an extra layer of security by requiring people within the organization to input a one-time code along with their password during login, reducing the risk of unauthorized access even if the attacker knows their password. Quest for Business 2FA supports various methods like SMS based, TOTP and admin-issued codes. Once people in the organization have successfully logged in, they have the option to save the device to their managed Meta account as a trusted device so that they don't have to repeat the process each time they log in from the same device. People using passwords are protected with 2FA default on, with the option to turn it off if desired.

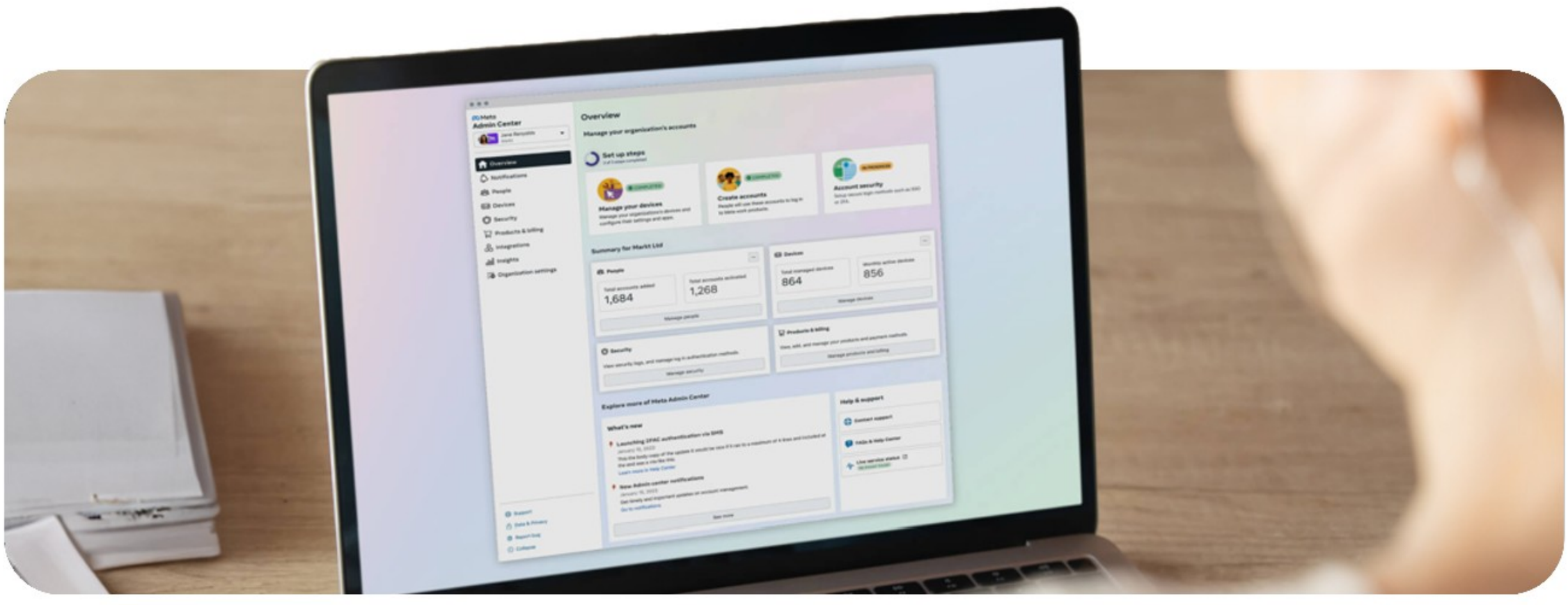
Step-Up authentication

For particular high-risk actions involving sensitive information and transactions, we have added an extra layer of protection via challenges which require the person to provide additional information to authenticate their identity. This helps to ensure only the legitimate person is requesting the action. Examples of high-risk actions are adding or removing admins or changing a company's authentication settings.

Account and device security

Meta uses a combination of proprietary and open source tools to detect unintended and/or suspicious IP addresses and devices exposed on the internet. As soon as we suspect an account has been compromised, it is locked. When a managed Meta account is locked, we send an email to both the admin and the affected person within the organization with steps to recover the account.

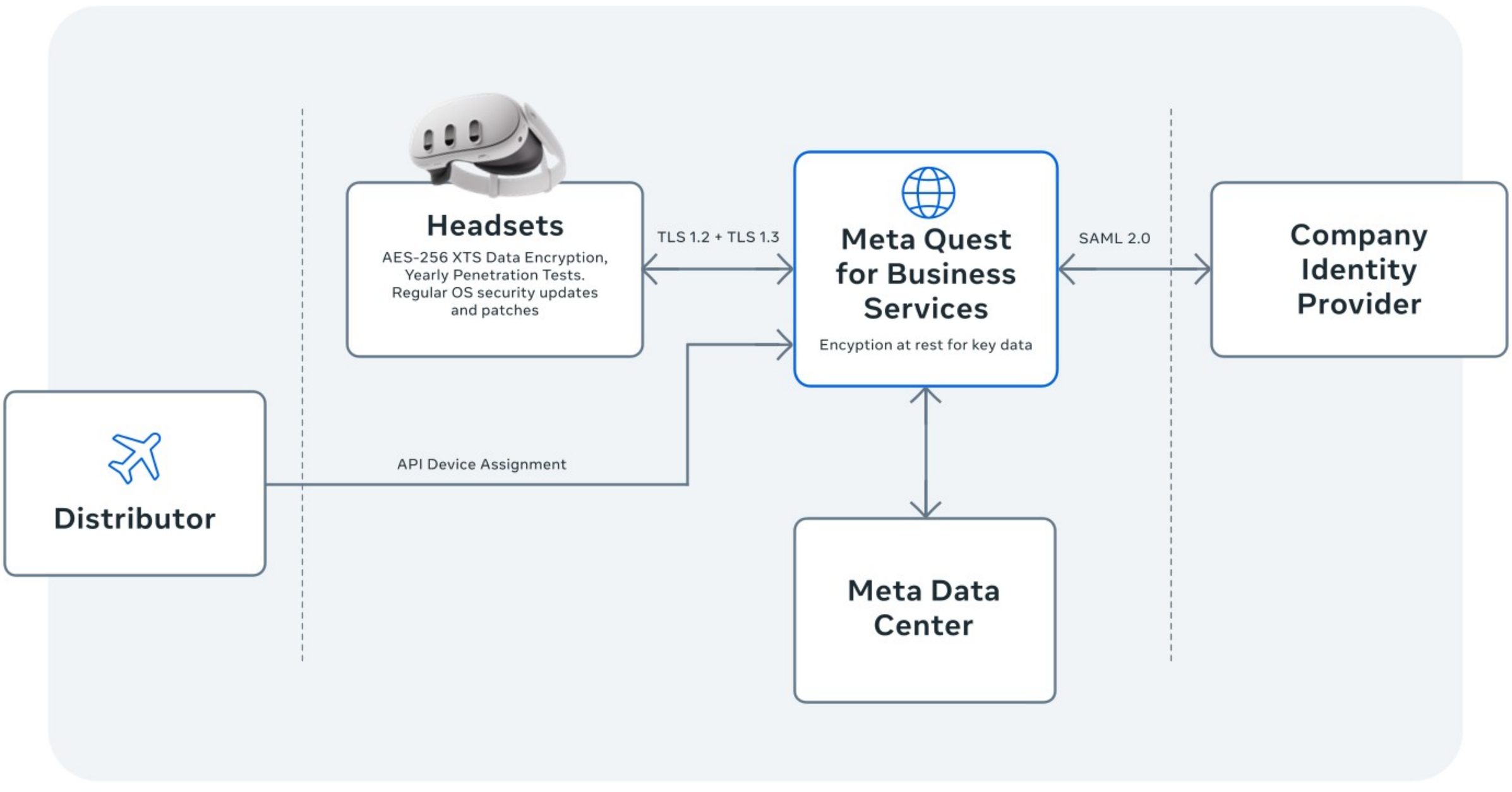
When a device is associated with your organization, the device cannot be set up for use outside of the management of your organization. If the device is stolen, and a factory reset is initiated, anyone using the device would need to reconnect to Quest for Business in order to complete the device setup. This makes the device unusable to anyone, except authorized people in your organization.



We take a multilayered approach to security

We want you to be confident in the security of your Meta Quest devices, and trust the way we process and store your proprietary and sensitive data. In addition to the security capabilities we've built in Quest for Business, we provide multiple layers of security, from application security to vulnerability management.

Figure 1 below illustrates various security elements that come into play in a Quest for Business deployment.



We follow stringent security practices to protect data across our ecosystem, whether it is stored or in transit.

Security is core to how we build our products. This section describes our multilayered approach to security across our software, hardware, applications and operating system. Our security measures include vulnerability management, penetration testing, or encryption.

Encrypted headset to server transmission

Data transmitted between the headsets and backend servers is encrypted with the industry-standard TLS 1.2 and TLS 1.3 protocols. Certificate pinning on devices and HTTP Strict Transport Security (HSTS) on traditional endpoints where possible is also used. Beyond the headsets' built-in security capabilities, Quest for Business has created core device security management capabilities as detailed in Meta Quest for Business security features above.

Encryption at rest

By default, Meta Quest for Business encrypts your organization's key data when it is stored at rest, except as used by Meta (i) to promote safety, integrity and security, (ii) for billing, or (iii) to comply with applicable law.

Specifically, this data is encrypted at rest using strong symmetric encryption algorithms such as ChaCha20-Poly1305 (XChaPoly) and AES-GCM. The encryption keys are created and managed by a dedicated service in a secured environment. All access to the encryption keys is logged, ensuring that only entities and systems that need to access your encrypted data stored at rest are able to do so.

Application security

For users installing apps through the Meta Quest Store, the first line of defense is preventing Meta Quest users from installing malicious and vulnerable apps. Each submitted app must go through the Meta malware detection and vulnerability scanning system automatically. We block apps where we identify potentially malicious behavior.

Meta Quest Store apps are scanned for vulnerabilities through Meta Quest App Static Analysis. The static analysis inspects existing known vulnerability types as well as vulnerable third-party libraries. Submitted apps are inspected for potential vulnerabilities that may cause the app to be exploited by malicious actors or malware. For example, it detects if apps are missing certain security checks or using vulnerable versions of third-party libraries. Based on the detection result, the system provides suggestions for developers to fix the issue in their apps. Meta runs security programs to keep malware and app vulnerability detections up to date.

All users of the Meta Quest Browser have their URLs scanned by the Safe Browsing system, which is based on Google Chromium Safe Browsing. Meta Quest users will be alerted for potentially harmful URLs which are deceptive or can conduct phishing attacks. People can opt out of this feature in Meta Quest Browser settings.

Secure Operating System

Meta's Virtual Reality Operating System (VROS) is built on top of the Android Open Source Project (AOSP) and inherits its capabilities. This allows Meta to leverage the security features found in the Android platform. These features include:

- **App sandboxing**
- **App signing**
- **Authentication**
- **Encryption**
- **Keystore**
- **SE Linux**
- **Trusty Trusted Execution Environment (TEE)**
- **Verified Boot**

Meta patches security vulnerabilities in Android OS on a regular basis. Meta Quest Browser patches are also made on a regular basis to help protect the web browsing experience.

Hardware and Firmware Security

Meta Quest devices are designed with state-of-the-art hardware and backed by stringent security practices. These devices use the Qualcomm Snapdragon XR2 platform, which contains a separate cryptographic module that supports hardware-backed cryptographic keys. In addition, Meta patches security vulnerabilities in the firmware on a regular basis.

Meta Quest devices follow industry standards in securing devices running Android, including but not limited to:

- Secure Boot which ensures a chain of trust, established in the factory, that all following stacks require.
- Device Identity provides uniqueness established in the factory, allowing strong identity for communication with Meta backend services.
- Enforcement mode SELinux implementation locks down critical API access to specific applications.
- Sensitive data stored on device, including user account information and all user generated content is encrypted with industry-standard AES-256 XTS encryption, with optional operating system formatting capabilities if encryption is maliciously disabled.

Penetration testing

Meta Quest hardware is penetration tested by third party vendors to ensure no security vulnerabilities escape internal review. New-to-market Meta Quest hardware is tested at least twice. First, for Meta Quest hardware early in development, Meta tests hardware and firmware level security features and implementations including secure boot, anti-rollback, trustzone (TZ) and factory reset/restore. Secondly, later in development, Meta Quest hardware is tested for OS level security and application level security features including privilege escalations, secure pairing (accessories), and Out-of-Box-Experience (OoBE) device provisioning. In-market Meta Quest devices are penetration tested periodically to determine if any new features or product updates introduce new security risks and, if they do, we take measures to patch them

Vulnerability management

Meta performs regular security and vulnerability testing to assess whether key controls are implemented properly and are effective. Meta has a vulnerability management program for Quest for Business that includes definition of roles and responsibilities, dedicated ownership of vulnerability monitoring, vulnerability risk assessment and patch deployment.

Meta's security team is responsible for the detection, triage, and remediation of vulnerabilities in Meta Quest hardware and software. Meta leverages various tools to detect security bugs in its code base, as well as in open-source and third party code, in order to mitigate or fix security bugs before they make it into shipped Meta Quest devices and impact our customers.

Meta Quest for Business benefits from Meta's investments in security

When crafting the Quest for Business security strategy, we tapped into the knowledge available within Meta, including the expertise gained from Workplace from Meta, a trusted enterprise collaboration tool used by millions of paid users.

Meta is a trusted partner to some of the largest organizations in the world, such as Accenture and Microsoft. Our customers trust us because Quest for Business and Workplace benefit from Meta's heavy investments in security technology, resilient infrastructure, policies and processes - investments necessary to protect the data of Meta's billions of worldwide users.

Building security-conscious teams

We understand the commitment to the security of your data starts with hiring the right people and raising their awareness on the importance of data security.

For example, Meta performs background checks on personnel working with your Customer instance for Quest for Business in accordance with Meta policies, where legally permissible.
Meta also ensures all employees with access to Customer Data undergo security training.

Forming resilient security protocols

Our commitment to the security of your data also manifests through the monitoring, controls and measures we have in place to pre-empt or respond to security risks.
Meta maintains a business continuity plan for responding to emergency or other critical situations that could damage the Quest for Business service, and formally reviews the plan at least once a year.

Meta's security measures also include controls designed to provide reasonable assurance that access to physical processing facilities is limited to authorized persons and that environmental controls are established to detect, prevent and control destruction due to environmental hazard. The controls include:

- Protocols requiring personal ID cards for entry to all Meta facilities for all personnel working on the Quest for Business service.
- Logging and auditing of all physical access to the data processing facility by employees and contractors.
- Camera surveillance systems at critical entry points to the data processing facility.
- Systems that monitor and control the temperature and humidity for the computer equipment.
- Power supply and backup generators.

Managing the security lifecycle

Quest for Business benefits from the focused security Meta has created.
Finally, Meta has established and will maintain an Information Security Management System (ISMS) designed to implement industry-standard information security practices applicable to Quest for Business. Meta's ISMS is designed to protect against unauthorized access, disclosure, use, loss or alteration of Customer Data.

Meta has a security incident response plan for monitoring, detecting and handling possible incidents affecting Quest for Business. The security incident response plan includes the definition of roles and responsibilities, communication protocols and post mortem reviews, including root cause analysis and remediation plans. Meta monitors the Quest for Business service for any security breaches and malicious activity. The monitoring process and detection techniques are designed to enable detection of security incidents affecting Quest for Business according to relevant threats and ongoing threat intelligence.

A privacy-first approach for our products and services

Our responsible innovation principles serve as the foundation for all our work. These principles are specifically crafted to protect people's privacy, so your organization feels empowered to explore, connect and engage with our products.

We provide controls that matter on Meta Quest devices

Quest for Business is compatible with Meta Quest 2, Meta Quest Pro and Meta Quest 3, with many core privacy features included on all three headsets. Meta Quest Pro and Meta Quest 3 have some unique features for which we offer additional privacy controls over data collection specific to these devices.

Privacy Features Common Across Meta Quest 2, Meta Quest Pro, and Meta Quest 3
Several privacy and security features are common to all three headsets. Some examples of common privacy features include:

- Ability to control who sees your information
- Control what data you share with Meta
- Protecting users from visiting websites that are suspected to be potentially dangerous
- The ability to report a bad user
- Information we collect from an end user

There are other features and you can learn more about them in our help center on Privacy Information and Settings.

Unique Sensors and privacy controls for Quest Pro
Released in 2022, Meta Quest Pro was the first Meta Quest headset featuring Natural Facial Expressions (NFE) sensors, and Eye-tracking (ET) sensors. These sensors help power the effect of social presence, which enables people to be their authentic self in immersive experiences. Along with the introduction of these sensors, we have also introduced additional privacy protections.

For example, **eye tracking** and **natural facial expressions** are off by default and, if turned on, can be paused at any time in the 'Quick Settings' menu. These sensors turn off automatically when the headset is in standby mode. Raw images of people's eyes and face never leave the device, are deleted after processing and are never shared with Meta or third-party apps. Additionally, people have control over which apps can access ET or NFE sensor data. If the features are not enabled for the device, they cannot be enabled for any app. You can read more details about these sensors in the Eye Tracking Privacy Notice and Natural Facial Expressions Privacy Notice.

Enhanced Mixed Reality Experiences with Quest 3

Meta Quest 3 ushers in more mixed reality (MR) use cases, apps and experiences. Mixed reality changes the way users interact with digital content by enabling them to enhance their surroundings without having to leave their environment behind. Mixed reality experiences are powered by spatial data which is collected by the headset and can be used by the device and apps to create unique and sophisticated MR experiences. Meta published a whitepaper on spatial data, which provides details on the different types of data the Meta Quest 3 collects. It also describes how we applied our responsible innovation principles to minimize any impact to people's privacy when creating MR experiences for Meta Quest 3.

We protect Customer Data

We limit access to your Customer Data
"Customer Data" is the data and content your organization or authorized users submit while using Admin Center and the Managed Accounts Center for Quest for Business. "Customer Data" excludes (i) data shared with the Meta Quest operating system that is utilized to perform necessary functions, such as downloading and running applications, network connections, device configurations and third-party MDM configurations; (ii) data that you permit to share with other apps, and that may be subject to other terms and policies; and (iii) the content you or your authorized users provide when providing feedback or reporting bugs, and communications with technical support, through Admin Center.

Meta products serve both organizations and consumers. We know it's important to our Quest for Business customers to have their data separated from end user consumer data, so we've logically separated Customer Data from consumer data. "Logical separation" refers to a data separation technique used by Meta that applies logic and data tagging in order to separate one or more identifiable data sets from other data sets.

We only use your Customer Data for stated purposes
Your Customer Data will only be used by Meta to provide and improve Quest for Business, to promote safety, integrity and security, and to comply with applicable law. Meta does not sell Customer Data or use it for any other purpose, including personalizing consumer Meta Products or advertising.

We set standards for apps on the Meta Quest Store

Third-party apps available on the Meta Quest Store are governed by their own terms and privacy policies. We require that developers of those third-party apps abide by the Meta Platform Terms and the Developer Policies, and reserve the right to remove developers or apps that do not fully comply.

We understand that you may share sensitive and proprietary information with VR apps on Meta Quest devices.

All the data processed at the app layer of any third-party VR application is not shared with Meta. The treatment of that data is handled in accordance with the applicable terms of the third-party developer.

We enable different use modes for Meta Quest devices to meet your organization's needs

Meta Quest devices can be configured through Quest for Business to either Individual Mode or Shared Mode to enable the configurations and controls that best support your organization's needs. Each mode provides organizations with distinct user experiences and data privacy models that support different use cases.

Shared Mode
Shared Mode enables multiple people to share Meta Quest devices for easy access to organization-curated apps. Shared Mode gives your organization the ability to determine the app experiences available in a headset through configurations made in Admin Center. Apps in Shared Mode are accessible by anyone using the device.

In Shared Mode, access to the Meta Quest Store and Meta platform-enabled social experiences, such as messaging, are disabled. This ensures your organization is in full control of the apps and experiences available in the headset.

Individual Mode
Individual Mode enables organizations to issue a Meta Quest headset to a single person, similar to device setups for work phones and laptops. In addition, Individual Mode offers admins control over which experiences a person can access, allowing flexibility in leveraging the full ecosystem or limiting access to a core set of apps and functionality. Individual Mode utilizes Meta accounts managed by your organization and respects the SSO settings to ensure secure access.

Meta accounts managed by your organization and Meta Horizon profiles
When a person logs into a Meta Quest device for the first time in Individual Mode, the managed Meta account will be used to authenticate the person and enroll the device into the appropriate mobile device management software. Unlike a consumer Meta account, a person cannot link the managed Meta account to other Meta social accounts (such as Facebook or Instagram) in the Account Center.

Managed Meta account information for an organization is not public and is only visible to people within the same organization. Admins also have the ability to delete a managed Meta account.
On first login in Individual Mode, people in an organization will be asked to create a Meta Horizon profile. They choose their own username, name, avatar, and profile picture.
The Meta Horizon profile defines how people appear in immersive and blended experiences. Meta will have access to the Meta Horizon profile username, name, profile picture, avatar, interactions with games and apps, and list of followers, among other data. This data helps us continue to improve immersive and blended experiences, to enable app functionality, and to use for other purposes as stated in the Meta Terms of Service the Meta Platform Technologies Supplemental Terms of Service, the Meta Privacy Policy, and the Supplemental Meta Platform Technologies Privacy Policy.

People in an organization can download the data associated with their Meta Horizon profile or delete their Meta Horizon profile entirely. When a Horizon profile is deleted, Customer Data associated with the corresponding managed Meta account will not be deleted, nor will the managed Meta account.

Individual Mode specific device management controls

Meta Quest Devices in Individual Mode have additional device management controls that empower admins to customize experiences based on their organization's needs and constraints.

- Admins can choose to allow people in your organization to add a personal Meta account on the Meta Quest device. This may enable them to switch between their personal Meta account and managed Meta account when navigating different experiences on the Meta Quest device.
- Admins can also enable or disable access to the Meta Quest Store for people in their organization. This gives the admin control over the apps people can download and use on the Meta Quest device.
- Admins can also decide whether people in their organization have access to Meta platform enabled social experiences, including the Horizon Worlds app, messaging and more, based on your organization's policies.

Meta partners with and serves some of the most respected businesses in the world.

accenture
Nanome
Adobe
Arkio
ARTHUR
BadVR
Mortenson construction
shapes xr
Pfizer
precisionos
gravity sketch
AUTODESK
FLOW IMMERSIVE
glue
PURINA
UCL SCHOOL OF PHARMACY
SkillsVR
TALESPIN
RESOLVE
SENTIO VR
mural
Microsoft
MESMERISE
SketchUp Viewer A Trimble Product

Contact Us

For more information about security or anything else related to Quest for Business, please contact us.