workplace
from Meta

Workplace Security Whitepaper

Contents

Introduction

Business is better when people are connected. That's what we do.

At Workplace, we're committed to your privacy and security, with world-class infrastructure and enterprise-grade security features to keep your Workplace community safe.

Workplace is a communication tool that connects everyone in your company using familiar features like Groups, Chat, and live video broadcasting. It integrates with the business tools you already use to provide a simple, secure and more productive way for people to share knowledge, work together and build community.

A combination of systems, capabilities and features ensures that Workplace keeps your information secure. These include advanced defense-in-depth security systems, world-renowned security teams working 24/7, and strict security policies and processes. This is all validated by trusted security and compliance certifications.

More than 7 million paid subscribers worldwide use Workplace.

"We're now a more secure organisation thanks to Workplace."

Paul Jones

Head of Emerging Technologies & UK Innovation Lab, AstraZeneca

The three principles of Workplace security

Your security is our top priority. The following three principles underlie our approach to security and protection of customer data:

You own your data

As the data controller, you choose what to do with your data, including whether to modify, delete or export it. The data that your users put on Workplace belongs to your organization and can't be accessed publicly. We take extensive steps to protect customer data in our systems as well. Our internal multi-layer data access, intrusion, account privilege and abuse monitoring systems log and analyze all requests to access customer data.

Strict controls on data access

Our tools and technology process the data you create and put onto Workplace to ensure you and your company have the best possible experience with Workplace. We don't show third-party advertising to your users on Workplace. Also, we don't use your data to provide or target advertising to your users or to personalize your users' experience on their personal Facebook accounts.

Workplace and Facebook are separate platforms

Workplace benefits from Facebook's investments in security, infrastructure, scalability, high availability and technical innovation. However, Workplace and Facebook are separate platforms with different accounts and profiles. Content is never shared between your Workplace and personal Facebook account.

Organizational security

Workplace benefits from the dedicated security culture Facebook has created. This is evident throughout our hiring process, employee onboarding, security training and dedicated engineering practices.

People security

Facebook's Human Resources team understands the commitment to your security starts with the people they hire. Facebook finds, develops and retains the best people aligned with our organizational security culture.

Subject to applicable law and regulations, all Facebook employees and contingent workers are required to complete background checks during their onboarding process. Facebook monitors and reviews progress reports to ensure completion of background checks before being granted access to worksites and Information Systems, including company-issued devices or physical access tokens (e.g., ID badges, hardware-based multi-factor authentication tokens.) If Facebook identifies a candidate who has not completed the background checks, notification and escalation procedures are enforced per the Facebook Background Check Policy.

Facebook employees and contingent workers are required to sign a confidentiality statement upon hire agreeing to the terms outlined in Facebook's Confidentiality Information Agreement, which includes information regarding disciplinary actions for non-compliance. Additionally, employees are shown the security policies and procedures as part of the onboarding process.

Facebook employees and contingent workers are encouraged to report known and suspected violations to their managers or managers in the Legal, HR or Internal Audit teams.

This includes violations of the following:

a. Laws, governmental rules and regulations

b. Accounting, internal accounting controls and auditing matters

c. Facebook's Code of Conduct or other policies

Security training

New and existing Facebook employees and contingent workers are required to complete training focusing on confidentiality and security. Topics covered in this training include the following: Facebook's policies and key privacy principles, privacy laws and regulations, vendor security audits, privacy and security by design, data security and access, as well as general practices relating to security awareness.

Teams such as Engineering, Sales, and User Operations have specific onboarding training programs for new hires. For engineers and product managers, there is a four to six-week program called Bootcamp, which includes all-day classes, coding tasks, mentoring sessions and training on common security issues in code.

The Security team conducts several company-wide security awareness activities, including National Cyber Security Awareness Month and periodic security awareness campaigns. The results are communicated to employees to increase their awareness and responsiveness to threats and vulnerabilities.

Security engineering

Facebook's Security Engineering organization is centralized into four pillars:

1. Prevention
2. Detection & response
3. Measurement & validation
4. Program & operations

Our prevention pillar proactively reduces a potential attacker's ability to compromise our data or systems. Our detection and response pillar focuses on identifying and responding to threats. The measurement and validation pillar independently evaluates our prevention, detection, and response efforts to ensure they are in line with our risk and avoid regression. Lastly, our program and operations pillar streamlines communication, drives engagement, and optimizes processes for both internal and external security initiatives.

From security engineers and data scientists to penetration testers and forensics engineers, our team comprises people with diverse backgrounds and skill sets. All of our Security team works to create a safe and secure community. Dispersed across Facebook's offices around the world—London, Seattle, New York, Singapore, and Washington DC— our Security team ensures we approach every challenge with a global view and can make a global impact around the clock.

Vendor management

The Security team has a process for conducting due diligence on third parties who may receive user data. As part of the due diligence process, Facebook assesses whether the third party meets Facebook's functional security requirements to protect the privacy and confidentiality of user data.

Resilience

Workplace is designed to stay up and running no matter what, thanks to our globally distributed infrastructure. This includes physical security safeguards for our data centers and offices, mitigations against denial of service attacks or local disasters, advanced threat intelligence, and automated detection using machine learning. This is backed up by 24/7 monitoring by dedicated teams.

Infrastructure

Workplace utilizes Facebook's systems and networks, which are maintained by highly resilient infrastructure. This infrastructure is built to provide maximum performance and to ensure protection against catastrophic events. Facebook either owns or leases and operates multiple data center facilities in multiple geographical regions. Workplace utilizes these locations along with our edge Content Delivery Network (CDN) to deliver our service. You can see a list of the data centers in our ISO 27018 certificate.

Data center facilities have all the appropriate capabilities to ensure continuity of service including fire suppression systems, redundant secondary power (UPS/CPS), backup generator units and telecommunications connections. Facebook uses configuration management tools to manage and monitor its systems. The tools automatically push standard policies to servers to help ensure consistency and compliance with the configuration.

Furthermore, Facebook has Distributed Denial of Service (DDoS) detection and mitigation mechanisms in place to protect the network from denial of service attacks. In addition to redundancy built into the edge network. Facebook uses a cutting-edge Berkeley Packet Filter (BPF) based DDoS mitigation capability.

Workplace uses Facebook's proprietary Domain Name System (DNS) architecture that takes various sources of information like capacity, resolvers and latency, routing and health information to make a decision as to which globally distributed Point of Presence (PoP) and/or Data Center to connect a user for maximum performance.

Physical security

Layers of security processes and measures restrict access to Facebook facilities. These measures include badge access, monitoring through the use of CCTV cameras and 24/7 guard staff. On-premise guard staff are responsible for patrolling and monitoring facilities and responding to physical security alerts. Badges issued to Facebook personnel control their access to Facebook premises. Facebook personnel includes employees, interns, contingent workers and vendors.

Facebook maintains a dedicated mechanism to troubleshoot issues related to badge access. When higher security is required based on increased risk, badge access privileges are limited to employees on a need-to-access basis. Access to higher-risk areas is monitored through enhanced physical and electronic means. Facebook uses a combination of owned and leased third-party data centers to support its products. Owned and third-party data center locations use badge readers and/or biometric fingerprint devices.

All visitors must register with Facebook, present a valid ID and sign a non-disclosure agreement - or get an approved exception. Visitors must be escorted while on premises at all times. Visitors must also visibly wear a visitor lanyard at all times and return the lanyard before leaving Facebook premises.

Disaster response and business continuity

Facebook has a dedicated team to improve Disaster Recovery (DR) capabilities. This team makes infrastructure and software systems resilient to failures. The DR team provides tools and performs tests to ensure Facebook and its family of apps stay resilient despite site outages.

To limit exposure from a business continuity event, Facebook writes or replicates data across multiple data center regions for performance and resiliency. Facebook automatically routes and load balances network traffic based on latency and network health checks.

Facebook conducts Disaster Recovery exercises to verify it can safely and fully disconnect a region with minimal impact to users. Various same-day unannounced tests are performed to monitor and learn how products and services react in a catastrophic scenario. Based on the learning, runbooks are updated and automation opportunities are identified to recover from such scenarios.

Facebook has a Resiliency program that supplements Facebook's Disaster Recovery efforts. This program focuses on the resiliency of the Company's network, IT and engineering assets. The Resiliency Team conducts periodic training and exercises ranging from geographic-specific crisis simulations to preparing data center teams to respond to a crisis and continue operations following a disruption.

Service availability and support

Workplace customers can monitor the current health of the service via our dedicated status page and subscribe to receive any notifications or updates.

Our dedicated support teams are available at all times through a variety of channels.

Protection

Workplace uses Facebook's investments in security, infrastructure, scalability, high availability and technical innovation to keep your data safe.

Secure by design

Workplace keeps your information secured with a defense-in-depth strategy of advanced security systems, world-renowned security teams and secure development processes focused on customer privacy and safety. A dedicated Security team validates, prioritizes and tracks identified vulnerabilities to resolution. In addition to these protections built into our design and testing methods, we also recognize the value that the external security research community provides. We reward eligible reports of potential vulnerabilities via the bug bounty program.

Encryption

Facebook uses Transport Layer Security (TLS) to encrypt all user interactions – including Workplace customers – ensuring that all traffic is encrypted in transit. The digital certificates used to provide the TLS encrypted connection between Facebook and the user are by a trusted Certificate Authority and kept current through internal validation processes. Facebook also encrypts sensitive network traffic between data centers and uses key-based encryption to ensure information can't be intercepted by unauthorized parties.

Facebook's Content Delivery Network (CDN) infrastructure, housed in third-party data centers, has encryption-at-rest implemented.

In first-party environments, Facebook takes a risk-informed approach that uses deep defense-in-depth investments and compensating security measures as outlined in this whitepaper. Facebook's ongoing security reviews and compliance audits regularly evaluate these measures and controls.

Additionally, objects associated with static content such as images, videos, etc., get encrypted using a unique per object encryption key. These objects are stored in Facebook's primary blob storage system, Everstore.

Vulnerability management

Facebook has a Vulnerability Management Team in place that is responsible for evaluating threats and prioritizing them by appropriate owners.

Scoped systems have external scanning performed at least every quarter. These systems also have internal scanning and detection performed continuously. The results are validated internally and tracked to resolution. Penetration testing is performed as needed by designated security engineers or external service providers who specialize in attack and penetration testing. To find the latest version of the Workplace penetration testing report, head to the Admin Panel or make a request.

Endpoint devices have malware defense solutions installed. Additionally, a configuration management tool manages the environment, so once the tool fixes a vulnerability, the corrective action or relevant update is pushed out to all in-scope devices.

Monitoring

Facebook's Logging and Monitoring policies and procedures support the detection and investigation of suspicious events in production and corporate systems. These policies include having security tools to prevent and detect unauthorized access by internal and external users.

Configuration management tools monitor systems and security settings. These tools continually update security settings and configurations on production servers with master settings to ensure systems are consistent with expected security standards.

Facebook's intrusion detection system collects and monitors logs from production and corporate systems. Facebook also utilizes endpoint-monitoring software to log and monitor activity on Facebook-managed IT assets, such as employee devices.

Facebook configures all employee and third-party tools to have consistent security settings. A central tool monitors these settings and authorized employees review any alerts.

Incident management

Facebook has dedicated teams to monitor and resolve security incidents based on company policies and ensure that action is taken within an appropriate time. These security incidents include (but are not limited to) external threat actors, internal threat actors, lost or stolen devices, service disruptions, incidents involving regulated data and incidents requiring coordination with law enforcement.

The Facebook incident management system tracks and assigns incidents based on severity level. On-call teams evaluate each incident and determine a resolution timing prioritized based on the severity. Policies and procedures for handling security and privacy incidents are documented and published internally. Responsible teams include:

- Internal Detection & Response (IDR): Responsible for managing security incidents related to employees, contractors and external threats. The Internal Detection & Response Team has the authority to investigate cases of internal abuse and insider threats. This investigation may also lead to collecting evidence of employee activity on corporate networks or devices.
- Global Legal Privacy Incident Management (GLPIM): Responsible for the legal analysis to determine notification requirements to regulators and/or impacted data subject(s), and where applicable, to communicate with relevant regulatory authorities.
- Cybersecurity Law & Investigations: Responsible for investigating information security incidents, making law enforcement referrals and for information sharing with other entities.

Facebook maintains an Incident Management Framework (IMF) that outlines how to assess and respond to data incidents and facilitate data subject protection and notification.

Once declaring an incident that requires external communication, GLPIM team members perform a risk assessment and analysis of data subjects and determine requirements for regulatory notification.

Access to customer data

Facebook designs its systems to limit the number of Facebook employees that have access to customer data. Facebook's system then tracks the activities of those employees. Only when necessary and on a case-by-case basis do engineers or teams supporting Workplace get access to Workplace data.

Facebook's internal abuse monitoring system logs and analyzes all requests to access customer data. It is then closely reviewed and any suspicious behavior is thoroughly investigated. Such access requests include content within a customer's Workplace community, such as user profiles or posts. Facebook has a zero-tolerance approach to abuse and improper behavior results in termination. Additionally, Facebook requires all new employees to sign a confidentiality statement. Signing this means employees have agreed to the terms outlined in Facebook's Confidentiality Information Agreement. This includes information about disciplinary actions for non-compliance.

Malicious content protection

Facebook has implemented numerous automated systems which protect users from harmful content and Workplace inherits many of these capabilities including anti-malware scanning and link inspection.

Files uploaded to your Workplace are scanned using our anti-virus/anti-malware service and checked against our repository of internal and industry-sourced malware signatures. If we detect a user uploading malware, we will inform the user and create a security log for an admin. At Workplace, we collect, store, and rely on our threat intelligence systems to improve the security of our services.

Malicious links are another significant concern. We implement both initial blocking and click-time checks to ensure that users aren't directed to malicious or spam sites. All links to non-Workplace URLs, both in-platform and in email notifications, are rewritten to first go through the link protection system. In addition to our internal list and integration with external blacklists, this system uses advanced machine learning classifiers to check the authenticity of the destination along with a slew of other inputs.

Data Loss Prevention (DLP) features

Keeping your content safe means being able to trust that it is only accessible by authorized users. Workplace includes DLP capabilities that help protect your sensitive corporate data.

On mobile apps (iOS and Android) admins can use either Enterprise Mobility Management (EMM) or Workplace native Mobile Application Management (MAM) features to enforce certain restrictions on what staff can do with Workplace content. These include:

- Block copy and paste
- Block file downloads
- Block screenshots and screen recordings

Workplace also offers integrated Video Rights Management (VRM) capabilities to encrypt livestreams and Video on Demand uploaded to Workplace. Videos with this encryption can only be watched by authorized, currently logged in users, and download or retransmission of the video can be restricted.

Identity and access

We make it easy to get the right people into your Workplace community while keeping it safe from unauthorised access or misuse.

Account lifecycle management

While Workplace allows you to manage accounts manually or in bulk via spreadsheets, we recommend that you automate your account provisioning. With automation, a user account will be automatically created, updated or deactivated in Workplace when taking the same action in your organization's directory. Automation ensures an easy joining and leaving process for employees and also ensures that no former employees will retain an active account after their departure.

Single Sign-On (SSO)

Single Sign-On (SSO) gives users access to Workplace through an Identity Provider (IdP) that you control, providing an additional security and governance layer. Users can sign in to Workplace using the same SSO credentials as other systems (e.g. laptop or internal apps). This means that users can access Workplace without having to remember another password. Additionally, no credentials are stored outside of your company's controlled systems or transmitted over your network.

Read more about your options for allowing users access to Workplace.

Identity integrations

Workplace is directly supported by several identity providers, including Azure AD, G Suite, Okta, OneLogin and Ping Identity, which offer native app connectors to make SSO and automated provisioning easier. Workplace supports SAML 2.0 for authentication and offers a SCIM API for automated provisioning, which is supported by most Identity Providers. Workplace customers can also choose to create a custom provisioning integration.

Read how you can create, update and deactivate user accounts on Workplace.

Secure identities for all staff

For accounts not using SSO, Workplace offers secure local accounts with email and password authentication with length and retry policies enforced. Passwords are managed and stored by Workplace and set by users upon verifying their identity during their first access.

We recognize that not every employee has a company email address, so we created access codes. With access codes, employees can activate their accounts without the need for a company email address.

Read more about creating an account without an email address.

Two-Factor Authentication

Two-Factor Authentication, also known as 2FA, is an extra security check that requires a user to enter an additional identifier that only they can access. A user with 2FA activated in Workplace will be asked for this extra identifier each time they try to log in to their Workplace account or app from a new device. Once they've entered this identifier, they have the option to save the device to their account as a trusted device so that they don't have to repeat the process each time when logging in from the same device.

Read more about Two-Factor Authentication.

Device management and access

Customers can control which devices can access their Workplace environment and whether users are subject to Conditional Access when doing so. If you choose to integrate with your IdP for SSO, then you can enforce the same Conditional Access checks during authentication, including device compliance via certificate exchange.

For customers using a Mobile Device Management (MDM) solution - also known as Enterprise Mobility Management (EMM) - the Workplace mobile app can be pushed as a company-managed app and supports additional configurations via following the specifications defined by the AppConfig Community. This includes periodically requiring secondary (biometric) authentication when opening the app, as well as enforcing the use of a MDM-aware minimum version of the Workplace app.

Customers who do not use an EMM/MDM solution or who have staff with unmanaged devices can still use these features via Workplace's native Mobile Application Management layer.

Read more about device management and access.

Governance

Workplace offers your company's admins tools, logs and policies to protect your community. We also offer technical controls to modify, delete or retrieve your data at any time. We design these tools to help you manage your community and create a great work environment.

Customizable terms and rules of conduct

Workplace admins can require their staff to accept customized terms of use or their organization's internal policies by linking them from the Workplace Admin Panel. These terms are shown when a user claims their account for the first time. Community rules are visible at any time under the Quick Help menu.

Native content reporting and review

Members of your Workplace community can report content, comments, chats and profiles directly to your admins that they deem inappropriate or unsafe for their Workplace. Once a user reports content, an Admin will receive a desktop notification and a mobile push notification for review and then has the option to approve or delete the content.

Workplace has limits in place to prevent abuse of our features and to protect people from spam and harassment. For example, if someone sends out several messages to people they are not connected to, they may be warned or temporarily blocked from sending messages.

Customer logging

Within the Workplace Admin, customers can view event logs related to security, account and key instance configuration activities.

These include:

- Account activities (account status change, email changed, etc.)
- User log in activities (log in, log out, etc.)
- Password-related activities (password changed, etc.)
- Admin activities (admin created, account promoted to admin, etc.)
- Domain activities (domain added, etc.)
- File uploads/downloads activities
- Integrations-related activities (integration added, removed, etc.)
- Multi-company group activities (e.g. multi-company group created, joins, etc.)
- Multi-factor authentication activities (e.g. multi-factor authentication succeeded)
- Malware uploads reporting

For a list of reported events read more here.

These events contribute to a Security Health Score. This score takes into account various pieces of information about your community's security activities. Workplace takes the detailed logs of user actions we provide and puts them into a user-friendly dashboard.

Customers can use our Application Programming Interface (API) to consume these events into a relevant platform (e.g. SIEM) for automated analysis and retention.

Integrations and API access

Workplace provides admins an ability to integrate and configure third-party apps with their Workplace platform. This integration happens by allowing apps access to company data through several APIs.

The three types of integrations provided by Workplace are:

1. First Party - Built by Facebook
2. Third Party - Built by a (verified) Workplace partner
3. Custom Integrations - Built and operated by the customer

Third-Party apps allow Independent Software Vendors (ISVs) to integrate their SaaS andPaaS products with Workplace. Once reviewed and approved by the Workplace team, these apps can be installed by Workplace community admins to deliver valuable automation. Workplace follows a rigorous process of evaluation and annual recertification which includes independent external audits by trusted cybersecurity consultancies. Learn more.

Workplace system admins can control the capabilities offered to each integration by creating apps and granting them specific permissions. Each app can be named to reflect the service it enables. Apps come with unique access tokens and permissions to control what information is allowed to be read or written by that app.

Compliance integrations

Workplace customers can meet their compliance, data security, threat protection and legal eDiscovery requirements by building an integration or using one of our partners' products. Our Third-Party Partner integrations fall into two categories:

1. Cloud Access Security Broker (CASB) Partners: CASB partners deliver systems that extend compliance, data security and threat protection capabilities into the cloud. These products can monitor Workplace in near-real-time, enforce compliance policies that you define and protect your organization against threats like compromised accounts or data loss. Learn more.
2. eDiscovery, Archive and Compliance partners offer products that can archive all of an organization's electronic communications into a single repository. This enables organizations to comply with regulatory retention and oversight or investigative requirements. Learn more.

At a technical level, two main Workplace capabilities support these requirements:

1. Graph API: gives you read access to all user content in your Workplace instance. The integration programmatically reads all content and makes it possible to batch extracts of your Users, Groups, Posts, Comments, Files, Photos, Videos, and Chat conversations
2. Webhooks: Event-driven notifications that Workplace sends you upon user content changes, post-activity, reactions and user/admin events

Data retention and deletion

Facebook servers store all data gathered from Workplace on behalf of customers until the end of the Workplace service contract. Customers can also initiate the process of deleting all their data. Customers may delete user content at any time through the admin functionality of Workplace or via the API.

Once a customer deletes their data, Facebook's deletion framework ensures its appropriate deletion. Deletion scripts run at a defined frequency to ensure data is deleted based on regulatory and compliance requirements.

Facebook has a process for secure destruction (wiping or physical destruction) of decommissioned electronic media containing Workplace product data. Destruction activities are logged, and when conducted by a third party, a "certificate of destruction" is issued by the vendor and retained by Facebook. Electronic media does not leave Facebook's chain of custody without documented proof or wiping or physical destruction.

Compliance and certifications

Workplace builds a security foundation based on industry standards, compliance and regulatory requirements. We always keep ourselves a step ahead by preparing for constantly evolving security challenges.

Independent third-party certifications

Workplace's customers and regulators expect independent verification of our security, privacy and compliance controls. To provide this, we regularly undergo several independent third-party audits. For each one, an independent auditor examines our data centers, infrastructure, and operations. Regular audits certify our compliance with the auditing standards ISO 27001, ISO 27018, and SOC 2. When customers consider Workplace, these certifications can help confirm that our product meets their security, compliance, and data processing needs.

ISO 27001
We manage sensitive company information by applying an information security management process that's consistent with industry standards.

ISO 27018
We augment the ISO27001 standard by providing privacy-focused controls and guidelines to protect personally identifiable information (PII) in public cloud computing environments.

SOC 2 and SOC 3
We ensure the security, confidentiality and availability of enterprise data on our platforms.

General Data Protection Regulation (GDPR)

Since its implementation on May 25, 2018, GDPR has sought to harmonize and clarify EU data protection law, while also imposing new requirements. Data controllers are the organization or party that decides the 'purposes' and 'means' of any processing of personal data, and many GDPR requirements fall on them.

For Workplace, our customers are the data controller in respect of the data on their Workplace product. They appoint Facebook as their data processor under the Workplace agreement and instruct Facebook to process their users' data under the Workplace agreement.

GDPR requires data controllers to engage data processors with appropriate contractual protections in place. This ensures a suitable level of protection for personal data.

Our Workplace Online Terms provide our customers with the contractual commitments required from their data processors under GDPR. In particular, the Data Processing Addendum in these terms addresses the requirements of Article 28 GDPR.

Workplace takes a global approach to our commitments on data processing. The commitments we make under the Data Processing Addendum apply to all customers and we do not differentiatebetween EU customers and those in other territories.

Contact us

For more information about security or anything else related to Workplace, please contact us.

www.workplace.com/security

workplace
from Meta