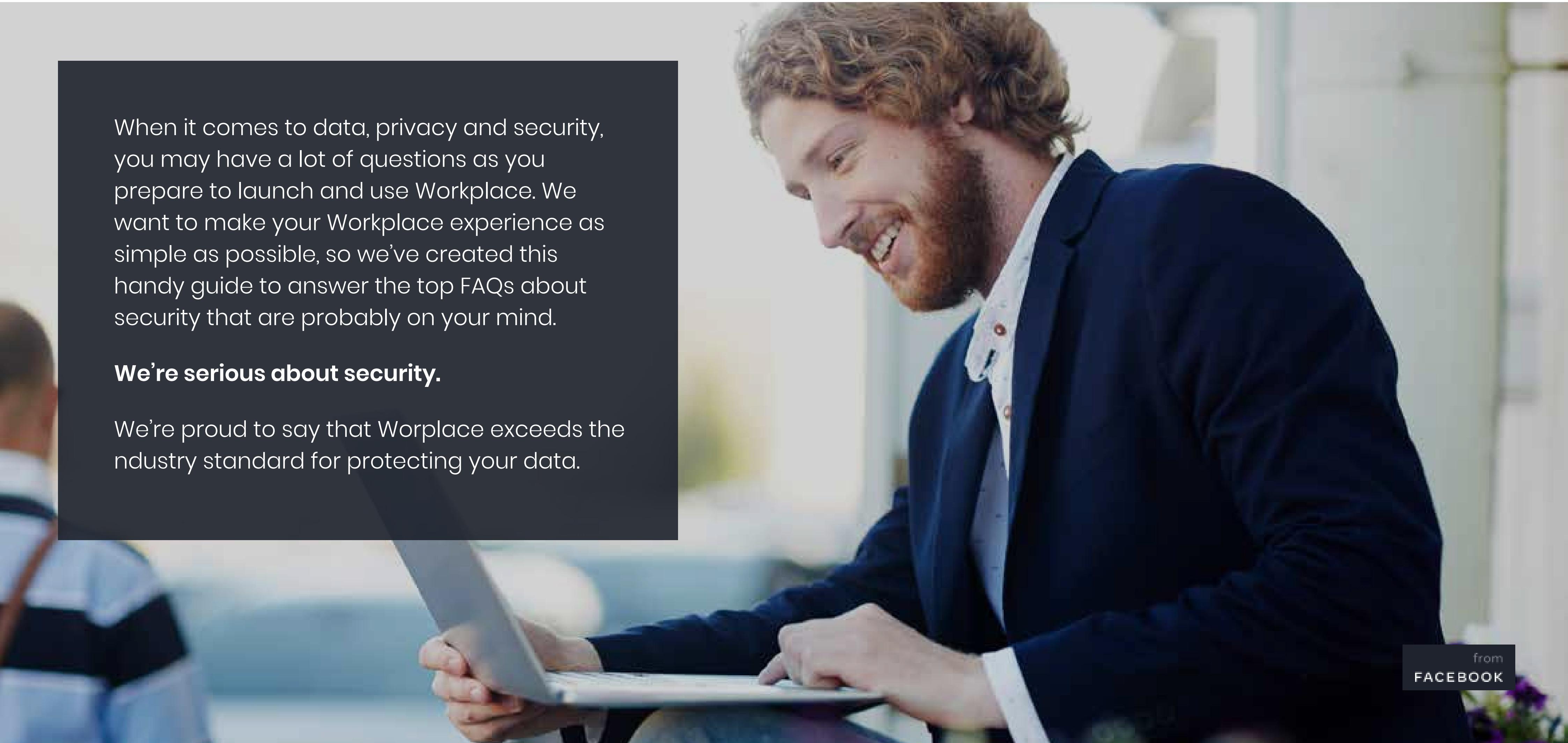
ACL Digital
an ALTEN group company

Workplace

Security Simplified



When it comes to data, privacy and security, you may have a lot of questions as you prepare to launch and use Workplace. We want to make your Workplace experience as simple as possible, so we've created this handy guide to answer the top FAQs about security that are probably on your mind.

We're serious about security.

We're proud to say that Worplace exceeds the ndustry standard for protecting your data.

from
FACEBOOK

Workplace is built on four principles of trust

1. Workplace accounts are separate from personal Facebook accounts

Workplace is built on Facebook's infrastructure, but it is a separate platform. And the same goes for data. For Workplace, data is segregated via what we call "logical boundaries."

What does this mean? Well, when you sign up for Workplace, we create a unique enterprise ID for you and your Workplace community. All data that is created within this community - or by any account associated with it - is then contained within the boundaries of your community. These boundaries restrict the ability for anyone outside of your authorized community to access or view content within it. None of your content is publicly accessible.

Workplace and Facebook accounts are also separate, with separate profiles and login credentials for each account. Content is never shared between your Workplace and personal Facebook account.

2. Workplace meets the highest data safety standards

Workplace is ISO 27001 and 27018 certified, and our security practices are regularly audited by independent third-party auditors with an industry standard SOC report.

For Advanced and Enterprise customers, a SOC3 and more detailed SOC2 reports are available from the Workplace Admin panel. Both reports are also available upon request with an NDA. Check out the FAQs below for a more detailed description of what these mean for your organization.

The Workplace Online Terms provide customers with various contractual protections when it comes to the handling of customer data, including, in particular, those set out in the Data Processing Addendum and the Data Security Addendum of the Workplace Online Terms. For our EU clients or their subsidiaries, Workplace offers an additional addendum with standard contractual clauses (SCCs) to assist them, as data controllers, in ensuring compliance with their obligations under General Data Protection Regulation (GDPR).

3. Security is our top priority

We have built Workplace in collaboration with our security experts. We regularly evaluate and test Workplace with full source code reviews, penetration tests, security audits by independent third parties and more. Customers on Advanced or Enterprise can access these resources in their Workplace Admin Panel. Alternatively, we will happily share these reports and results upon request.

4. You're in control of your data and privacy

In Workplace Essential, Advanced and Enterprise, your organization owns and administers the account data - you can modify, delete or export it at any time. Our industry standard APIs allow for real-time activity monitoring and content exports. If we receive a request for your data, we will redirect the request to you. If you would like to use third party tools for eDiscovery and compliance, we provide integrations with several industry-leading providers.

Got a question? Here are the top security FAQs

Who owns and controls the information my employees create?

For Workplace Essential, Advanced and Enterprise customers, the data your employees put into Workplace belongs to your organization. You control it. Your administrators can modify, delete or export it at any time via an API or the Admin Panel. What's more, to create a Workplace account, the only mandatory information a user needs to provide is their first and last names and their email address or an employee identifier.

Where's the data stored?

To protect your data and provide unprecedented performance and availability within our platform, data on Workplace is stored globally across Facebook's data centers, currently located in the US and the EU.

How does Workplace keep my information secure?

Workplace is hosted on Facebook's infrastructure, protected by a combination of advanced security systems, world-renowned security teams, firm security policies and processes focused on customer privacy and safety. Physical access to our data centers is restricted to authorized individuals, and we own or directly lease all of our facilities, so we have end-to-end control over the grounds, buildings, servers, operations and maintenance for each center.

Admins can leverage our Security Center to monitor unusual security events and view a company security health score. They can also use our APIs, and we have partnered with a variety of industry standard compliance service providers for policy enforcement and to receive security alerts.

Do you have a way for admins to filter content that gets posted in Workplace?

We don't offer any content filtering capabilities within Workplace. However, we have integrations with third-party Cloud Access Security Brokers solutions that perform content inspection and monitoring. If you prefer to build your own custom content monitoring solution, we provide a rich API that allows for real-time content inspection and remediation. When a user reports a post, it goes to the content monitors (admins designated by your organization) for review.

Is content shared on Workplace also visible in my personal Facebook account?

No. Posts made on Workplace are not visible on your personal Facebook account. Workplace and Facebook are separate products, with separate profiles and logins. This distinction is clear in the design, so you can easily identify whether you're in your work or a personal account. A separate application is also required to access Workplace from your mobile device. This keeps personal and work discussions distinct. What's more, you don't need a personal Facebook account to sign up for Workplace.

Who can access Workplace customer data within Facebook, and how is that access reviewed?

On a need-to-know basis, engineers or teams supporting Workplace products may access Workplace data e.g. resolving a support ticket raised by the customer. Access to customer data is logged by our internal abuse monitoring system, is closely monitored, and any suspicious behavior is thoroughly investigated. All requests to access Workplace customer data are logged and analyzed. This includes requests for content within a customer's Workplace community, like user profiles or posts. The abuse monitoring system uses a rules engine to determine what action to take when such a request is made, based on several factors including what type of data is being accessed, who is accessing it and for what reason.

Facebook has a zero-tolerance approach to abuse, and improper behavior results in termination. Moreover, Facebook employees 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.

Got a question?
Here are the top security FAQs

What happens when an employee leaves the organization?

If you're using Workplace Essential, Advanced or Enterprise, admins can disable an account, but only those using Workplace Advance and Enterprise can raise a request to permanently delete it or build custom API integrations to anonymize the profile data. We have integrations with cloud identity providers to allow automated user management in Workplace, so your Workplace user accounts get automatically deactivated once your organization's identity management system gets updated.

Will you fill out our Security Questionnaire?

We focus our efforts on making sure that Workplace is enterprise-grade, safe and secure for all of our customers rather than on demonstrating this to a few upon request. However, this doesn't mean we aren't committed. We've packaged all the necessary information to deliver to customers in a scaled way through our security questionnaire (CAIQ), SOC 2/3 and penetration testing reports and ISO certifications. A full package containing these resources can be provided upon request (under NDA), while the reports are available for Advanced and Enterprise customers directly within the admin site.

What security certifications does Workplace hold?

ISO 27001
This certification demonstrates security best practice and provides an independent validation of the design and operational effectiveness of our security management program and information security management system.

ISO 27018
This certification covers the control objectives, controls and guidelines for implementing measures to protect personally identifiable information (PII) in accordance with the privacy principles in ISO/IEC 29100 for the Workplace from Facebook service and all related supporting technology.

SOC Certifications

- SOC 2 - is an extensive independent audit of how we host and operate Workplace from Facebook, which is performed annually by an independent third party auditor and covers the 12 month period from the previous calendar year. The assessment covers everything from how we secure and protect the application and our data centers, to how we verify the identity and background of our employees. This is available upon request, subject to an NDA.
- SOC 3 - this report provides a summary of the SOC 2 report.

NCC
The result of source code review and penetration test by one of the world's top security consultancies, NCC Group.

Got a question? Here are the top security FAQs

Do you support eDiscovery?

Most customers that ask about the eDiscovery capabilities are interested in the extent to which Workplace data can be extracted from a customer instance, and the format in which the data is pulled via the API. Workplace provides a robust REST-based API that allows for the extraction of virtually all content in Workplace, including Workplace Chat conversations, as of a point in time. This can be filtered across a number of factors including time range, groups, author and keywords. However, content deleted from Workplace or Workplace Chat is not available through the API, and for any content that has been edited, only the current version of such content will be available.

We offer native integrations with several security and compliance providers to help you meet enterprise-grade requirements for eDiscovery, regulatory compliance and system activity monitoring. Workplace customers on Advanced and Enterprise can also design their own custom integrations to internal tools.

Facebook is blocked in my organization. Will Workplace still be accessible?

Workplace won't work reliably if your company blocks consumer Facebook. Any workarounds would be unsupported, and we cannot guarantee that it will work going forward. More information is available in our Domain Whitelisting documentation.

Does Workplace encrypt data at rest?

All data transmitted over public networks is secured via best-in-class encryption standards. To provide our consumers with unmatched performance and better service at scale, we have taken an informed decision not to encrypt the data at rest. Instead, we use compensating security controls. These include:

- Controls to prevent compromise of networks with access to data (custom perimeter devices)
- Controls to prevent compromise of systems with access to data (stringent access controls)
- Controls to prevent loss of control of storage media (data center security, physical security, controls on recycling of media and data cleansing).
- Loss of backup media: Workplace data is continuously replicated across multiple servers for high availability and streamed to a backup tier for recoverability. No portable backup media is utilized for this purpose, hence preventing the risk from loss of backup media.

ACL Digital - Reseller Partner of Workplace

Any questions?

Contact us by clicking here.

ACL Digital is a design-led Digital Experience, Product Innovation, Engineering and Enterprise IT offerings leader. From strategy, to design, implementation and management we help accelerate innovation and transform businesses. ACL Digital is a part of ALTEN group, a leader in technology consulting and engineering services.

business@acldigital.com | www.acldigital.com

USA | UK | France | India