Data privacy and security by design on the WhatsApp Business Platform

The WhatsApp Business Platform powers communication with people all over the world, so businesses can connect with their customers on WhatsApp in a simple, secure and reliable way. The WhatsApp Business Platform enables businesses to have conversations with their customers across the customer journey, from initial discovery through post-purchase support. We highly value the data privacy and security of both businesses and their customers, and this document is intended to provide transparency on the security and compliance practices of the Cloud API, hosted by Meta.

Contents

Data privacy

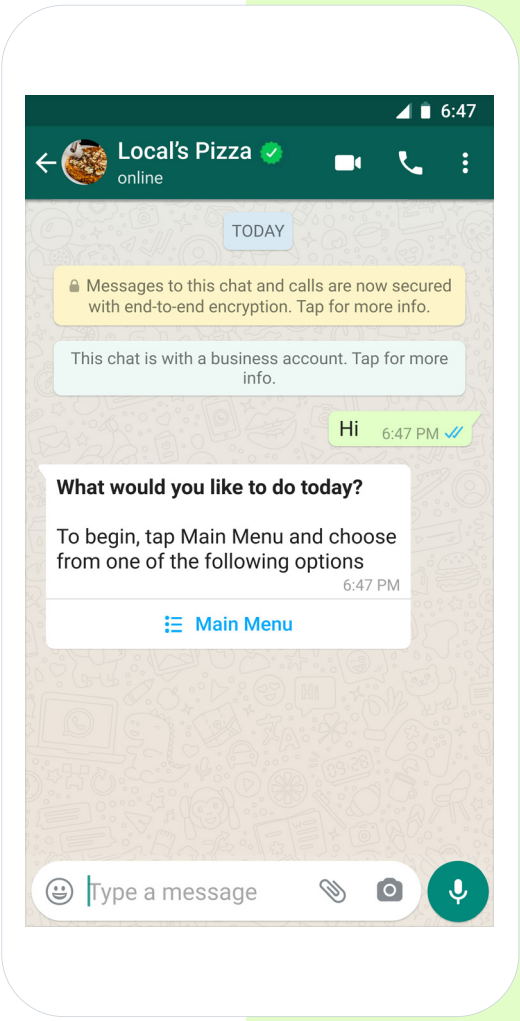
Security by design

Compliance and security standards

Data privacy

Businesses now have the option to use a Cloud API, hosted by Meta, to manage communication with their customers on WhatsApp, as well as the existing On-premises API. When businesses choose to use Meta hosting services, Meta acts as a service provider and will have access to the messages between consumers and businesses using this integration. Meta will use the messages it processes on behalf of and at the instruction of the business. This is an industry standard practice among many companies that offer hosting solutions. While Meta will not automatically use messages to inform the ads that a user sees, as is always the case, businesses will be able to use messages they receive for their own marketing purposes, which may include advertising on Meta, or via other channels, like email or TV.

Note: There are optional services that a business or you can choose to use where Meta receives limited information. For example, you can choose to start a chat with a business after interacting with their ad on Facebook and Instagram or interact with offers and announcements a business may send you on WhatsApp. We're rolling out the >> icon at the top of the chat bar for these services, which you'll be able to tap to learn more about how this works.



Encryption

Every WhatsApp message, including messages between people and businesses, is protected by the same industry-leading, signal encryption protocol that protects messages from before they're sent until they're delivered to the intended recipient.

Messages with businesses that use the WhatsApp Business app or directly integrate with the On-premises API are end-to-end encrypted. When a business chooses to use a WhatsApp Business solution provider, or Meta, to operate the Business API on its behalf, we do not consider that to be end-to-end encrypted since the business has chosen to give an intermediary access to those messages. If a business chooses to use the Cloud API, as stated above, Meta will use the messages it processes on behalf of and at the instruction of the business.

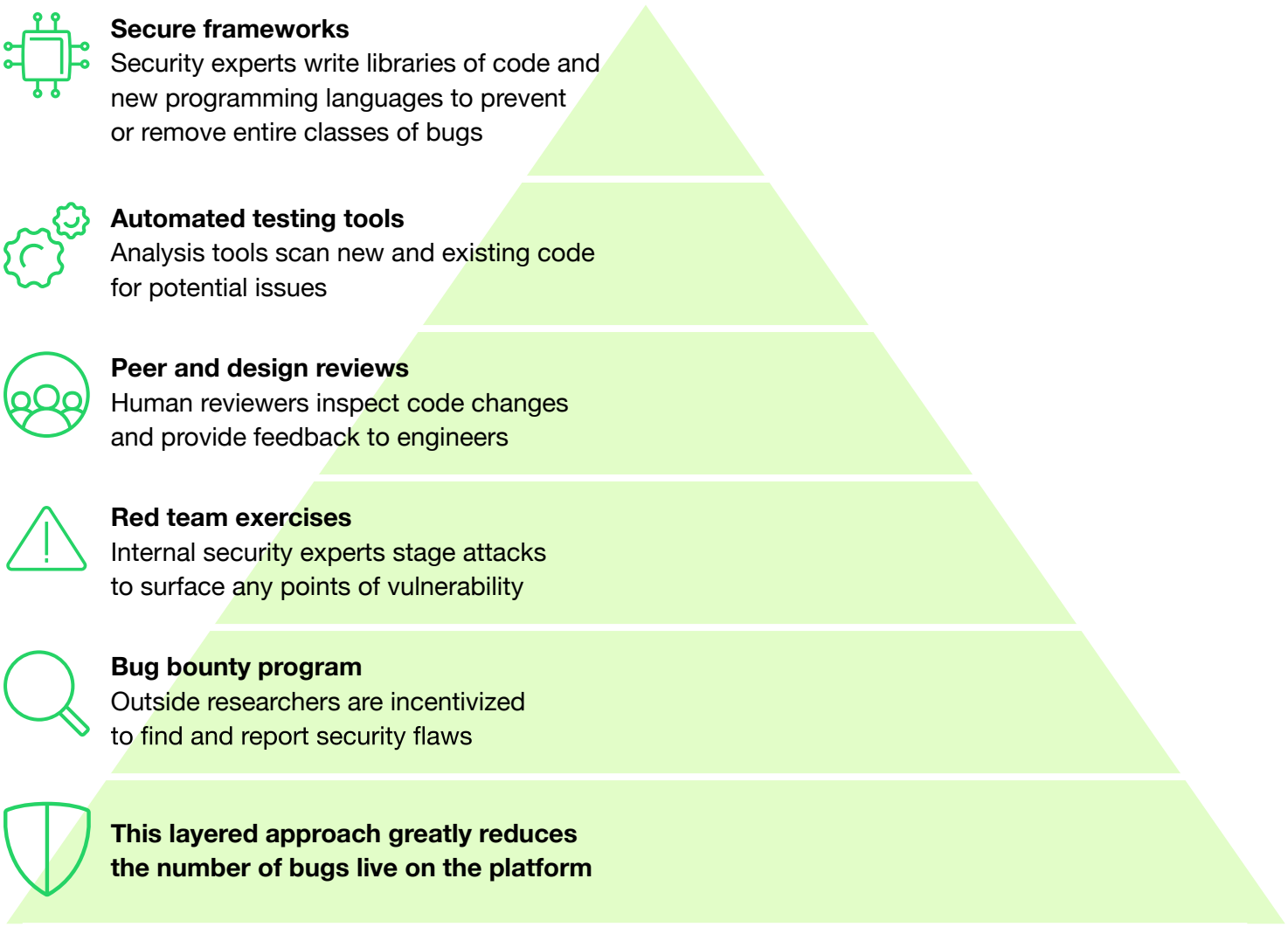
To ensure people know how a business chooses to manage their messages with customers, we make it clear within the chat whether businesses have chosen Meta or another company to help manage their messages.

Security by design

The WhatsApp Business Platform is protected by a combination of people, processes and technology security systems that keeps customer data private and secure. Meta uses defense in depth, meaning we layer a number of protections to make sure we prevent and address vulnerabilities in our code from multiple angles. We care deeply about protecting customer data and we have built the Cloud API with security in mind.

Defense in depth

Keeping Meta safe requires a multi-layered approach to security.



Product security

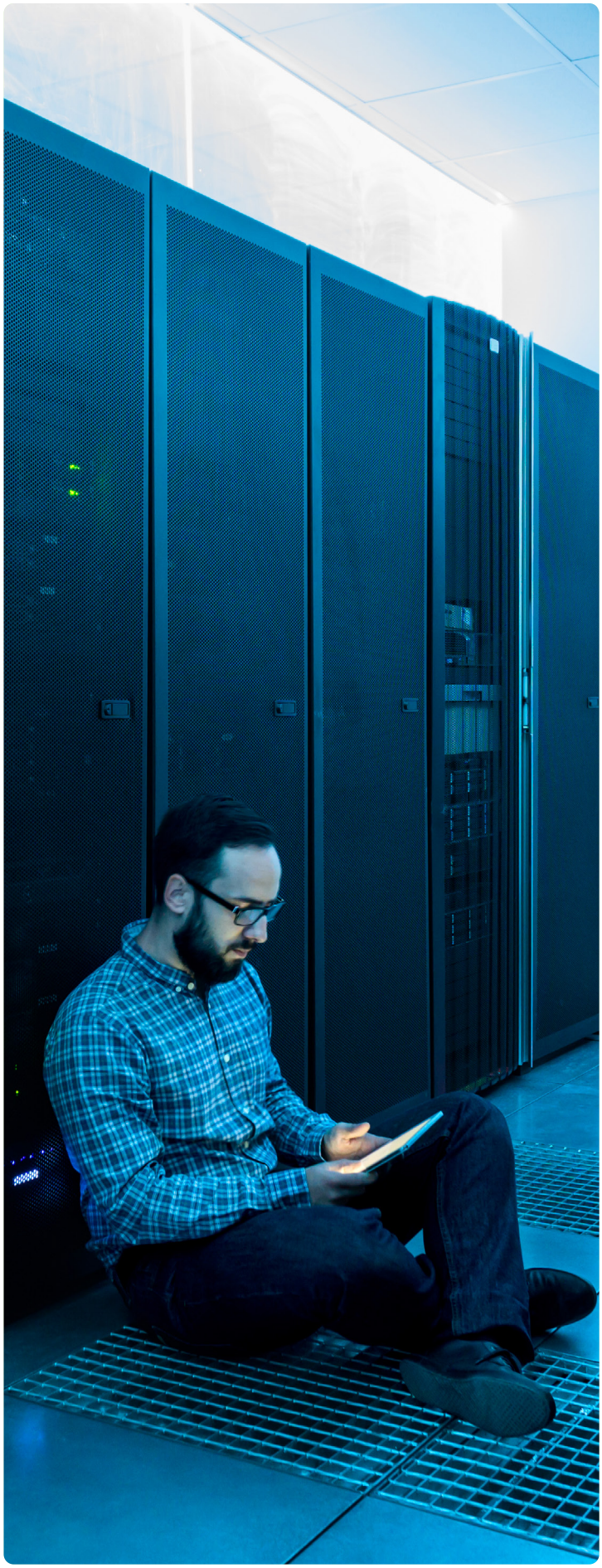
Application security: Meta has multiple layers of security controls built into its software development lifecycle designed to prevent vulnerabilities from being introduced into Meta code. Meta uses third-party security experts to perform detailed penetration tests on our applications.

White hat program: Meta operates a white hat bug bounty program which creates incentives for external users to report security vulnerabilities on Meta's platform. Meta has a designated on-call team that manages the review and validation of white hat reports. Validated reports are resolved based on severity level, and progress is tracked in an internal system.

Vulnerability management: Meta operates a vulnerability management program to identify, track and remediate known security vulnerabilities across Meta's infrastructure.

Data security: Meta implements state-of-the-art mechanisms to ensure security of data (at rest or in transit) and security of software and hardware components (which are used to implement the Meta-hosted WhatsApp Business API service). Traffic in and out of Meta data centers is encrypted (HTTPS). Traffic within Meta data centers is encrypted using Transport Layer Security (TLS). Traffic between WhatsApp Business API service and WhatsApp servers is encrypted using the Noise protocol. WhatsApp Business API message content (including text, template, and media messages) is stored in an encrypted state on Meta's data stores.

Meta policies define sensitive data types and require that appropriate security and access controls be implemented, taking into account data type, business need, the nature and purpose of processing, data privacy laws and roles and responsibilities of accessing parties.



Change management

Code changes are tracked through an internal tracking system and go through the following change management process:

- To initiate a change, the change author first creates a differential, or “diff,” which serves as documentation of the proposed change, the test plan for the proposed change, the results of automated testing of the change, and review and approval of the change.
- Each diff represents a change to the code base that a developer has proposed for use in production.
- Developers check out the code base from a central repository and load it into a testing environment in order to test the proposed change.
- Diffs are run through automated tools that check for common errors or deviations from best coding practices and for known code patterns that raise security or privacy concerns. These testing tools include features designed to help the author locate the documentation or resources needed to resolve any identified issues.
- Testing and approval of the diff are logged by the system to support the change.

Availability and continuity

Disaster recovery: We maintain a disaster recovery program to ensure services remain available or are easily recoverable in the case of a disaster. Developers can stay up-to-date on service outages through a publicly available status page.

Resiliency: Meta maintains a resiliency program for preparing Meta personnel to effectively respond to and recover from an emergency or crisis. Meta has a designated team to lead company-wide efforts to enhance preparedness, with attention to critical areas of business continuity, crisis management, data center resiliency and workplace resiliency, as well as competencies within business units. Meta has DDoS detection and mitigation mechanisms in place to protect the network from denial of service attacks. Meta regularly conducts disaster recovery tests and, based on the learning from these tests, works to update and improve its disaster recovery processes and automated technologies.

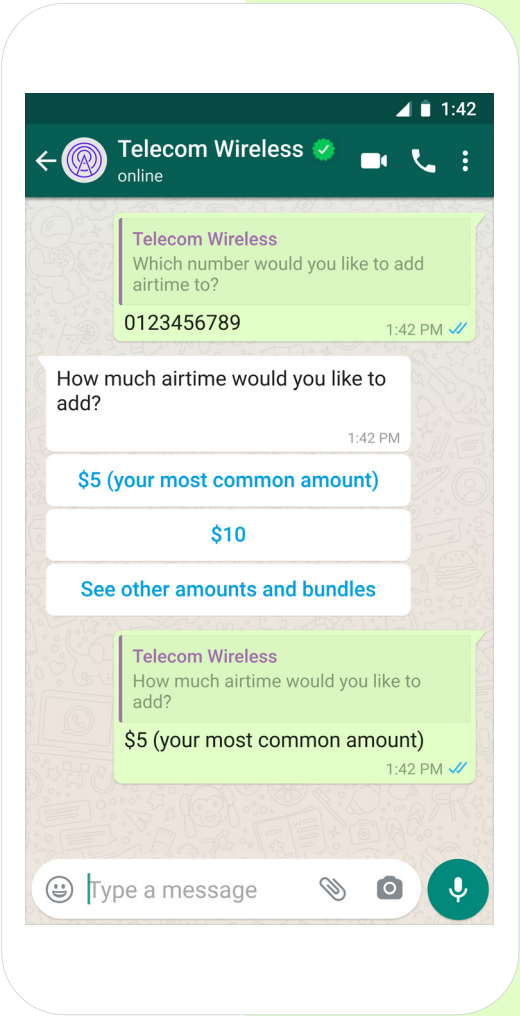
Compliance and security standards

SOC 2

SOC 2 is an extensive independent audit of how Meta hosts and operates the Cloud API, which is performed annually by third-party auditors. It evaluates the processes in place to ensure the security, confidentiality and availability of customer data on our platforms, covering everything from how we secure and protect our data centers to how we verify the identity and background of our employees. This is available upon request, subject to an NDA.

Penetration testing

Meta works with external auditors to conduct regular penetration tests. Features are tested and reviewed by an independent security consulting firm. This is available upon request, subject to an NDA.



Security questionnaire

We have completed the Cloud Security Alliance Consensus Assessments Initiative Questionnaire, which is available upon request, subject to an NDA. It offers an industry-accepted way to document what security controls exist in the Cloud API providing security control transparency. It provides a set of questions that the Cloud Security Alliance anticipates a cloud consumer or auditor would ask a cloud provider. We document WhatsApp's answers to the questionnaire, which should provide a basis for security, control and process review.

GDPR

Meta takes data protection and people's privacy very seriously and we are committed to continuing to comply with data protection laws. The Cloud API allows our customers to continue to meet their obligations under General Data Protection Regulation (GDPR). Meta complies with applicable legal, industry and regulatory requirements, as well as industry best practices. See more.