remove bg
By Canva

Security Whitepaper

This document describes the security measures for the remove.bg background removal API

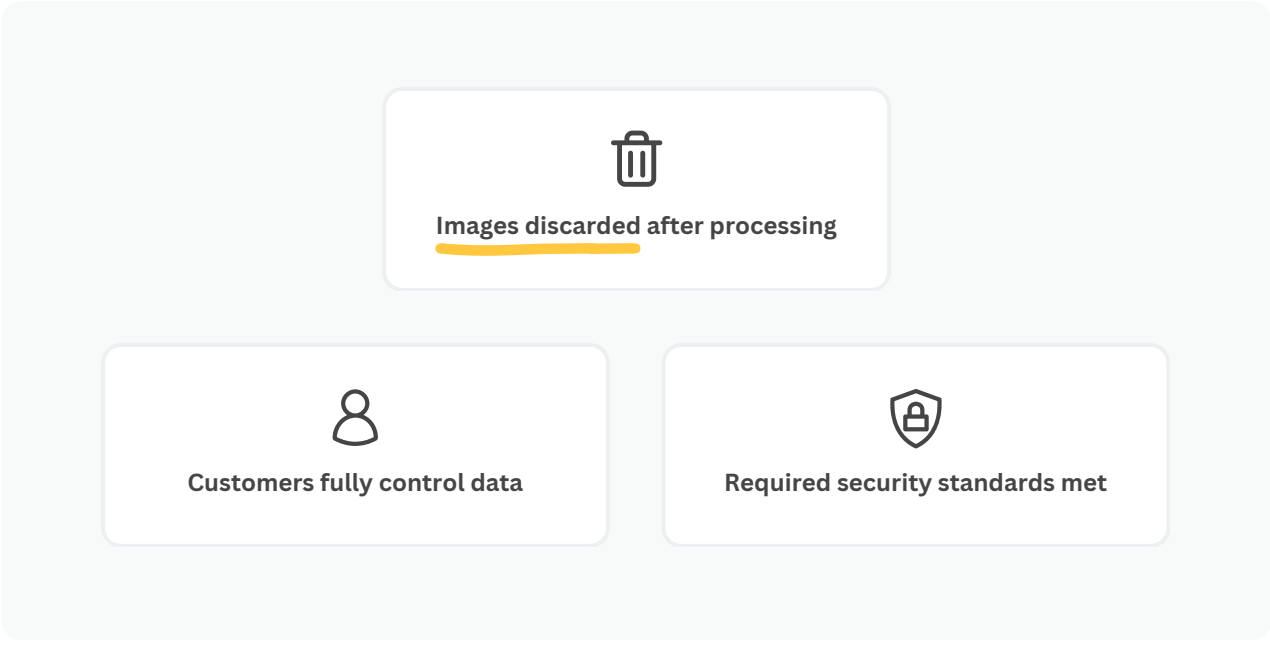
Privacy first

Security and privacy are vital to remove.bg. Our mission is to enable businesses of all sizes to use our visual AI product as the foundation for something bigger, and we understand the responsibility that comes with handling confidential and personal information. As long as we are operative, we will be committed to offering a reliable and high-quality service. **We are transparent about how we protect customer data and design our products based on this principle**. Our security model uses cloud-based computing to implement highly redundant and scalable systems that are cost-efficient for organizations of all sizes.

Full deletion of images

Regularly storing image data comes with the risks of unauthorized access, manipulation, data loss, and more. To mitigate risks in the most effective way, **remove.bg does not persistently store any image data.**

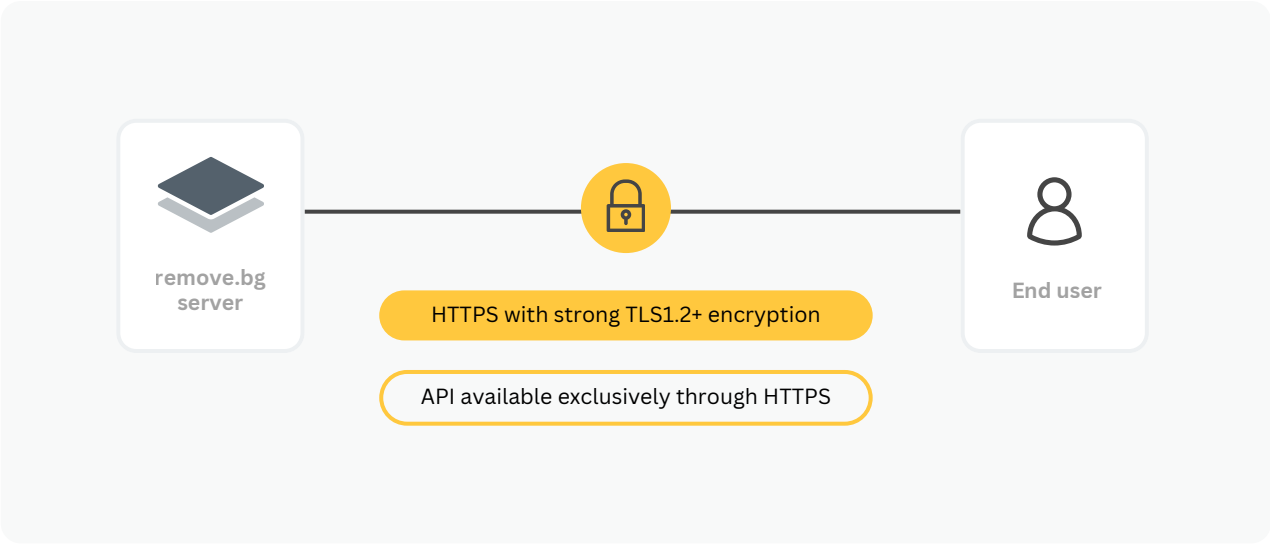
Image files are only accessed for the purpose of foreground detection and background removal, as per the API documentation. Once the processing is finished and the client has received the resulting image, it is **discarded** (usually within 60 minutes) without anything left on our infrastructure at all. After 90 days, remove.bg has **no way of restoring past data**. This gives our **customers full control over data** saving on any medium.



Securing data in transit

On the Internet, unprotected data is vulnerable to unauthorized access during transit. remove.bg, therefore, employs strong encryption protocols such as TLS1.2+ to protect data to the same level as banking systems and e-commerce platforms.

Our API is available exclusively through HTTPS, which means data transmission is possible only through encrypted and secure channels.

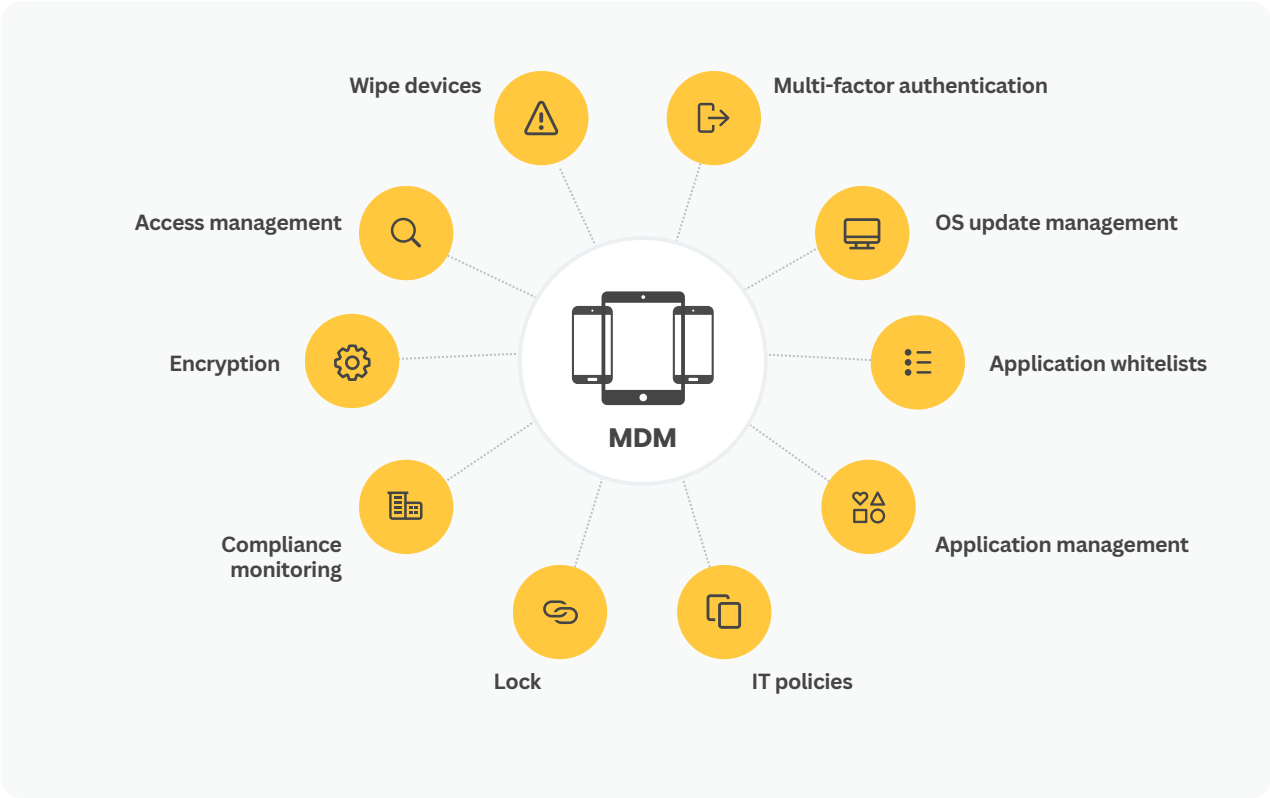


Secure API communication using HTTPS strong encryption

Mobile Device Management (MDM)

As part of Canva, remove.bg uses an MDM solution for endpoint management, which includes the ability to roll out management policies remotely to all devices, monitor compliance in real-time, and manage OS and software program updates.

Monitored parameters include general device settings, installed software on the endpoint device, and operating system versions. Moreover, this gives us the ability to remotely wipe and/or lock devices, if required.



remove.bg's MDM Solution for endpoint management

Physical security

While cloud-based processing removes the need to get involved in hardware-level issues, all processing eventually takes place on physical machines that need to be protected against unpermitted access.

We host our products in **data centers** operated by some of the **global leaders** in cloud computing. All of them are extensively protected through **state-of-the-art security** measures, such as layered security models, electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, high-resolution CCTV monitoring, laser beam intrusion detection systems and experienced security guard patrols who have undergone rigorous background checks and training. All hardware is tracked meticulously from acquisition via installation and operation to secure disposal. Uninterrupted power and environmental control are provided through **redundant supply systems**.

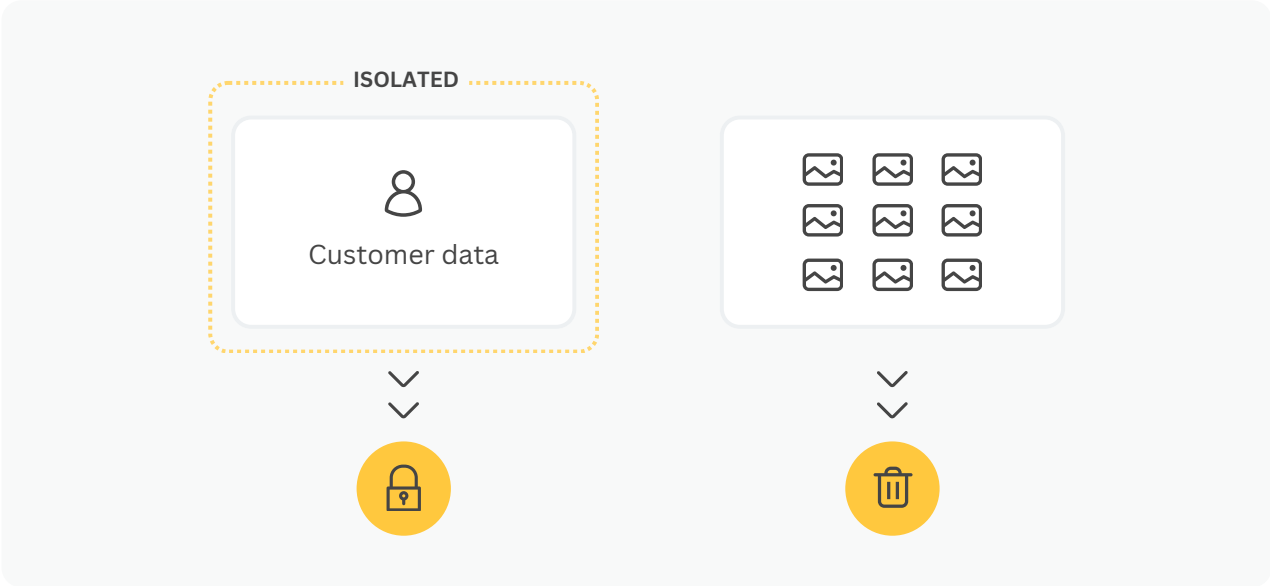
For more information on the physical security measures used by our cloud providers, please refer to cloud.google.com/security/.

Isolation of data

To keep data private and secure, we logically **isolate our customers' image data from their other data, even when it's processed on the same server.**

Data is classified and handled strictly according to their respective policies. For instance, retention of metadata and access logs serve accountability purposes while image contents are always fully discarded.

Administrative access is limited to a small number of experienced employees under narrowly defined scenarios, such as error analysis and debugging.



Securing data privacy by isolating customer data while fully discarding image contents

Protection of personal data

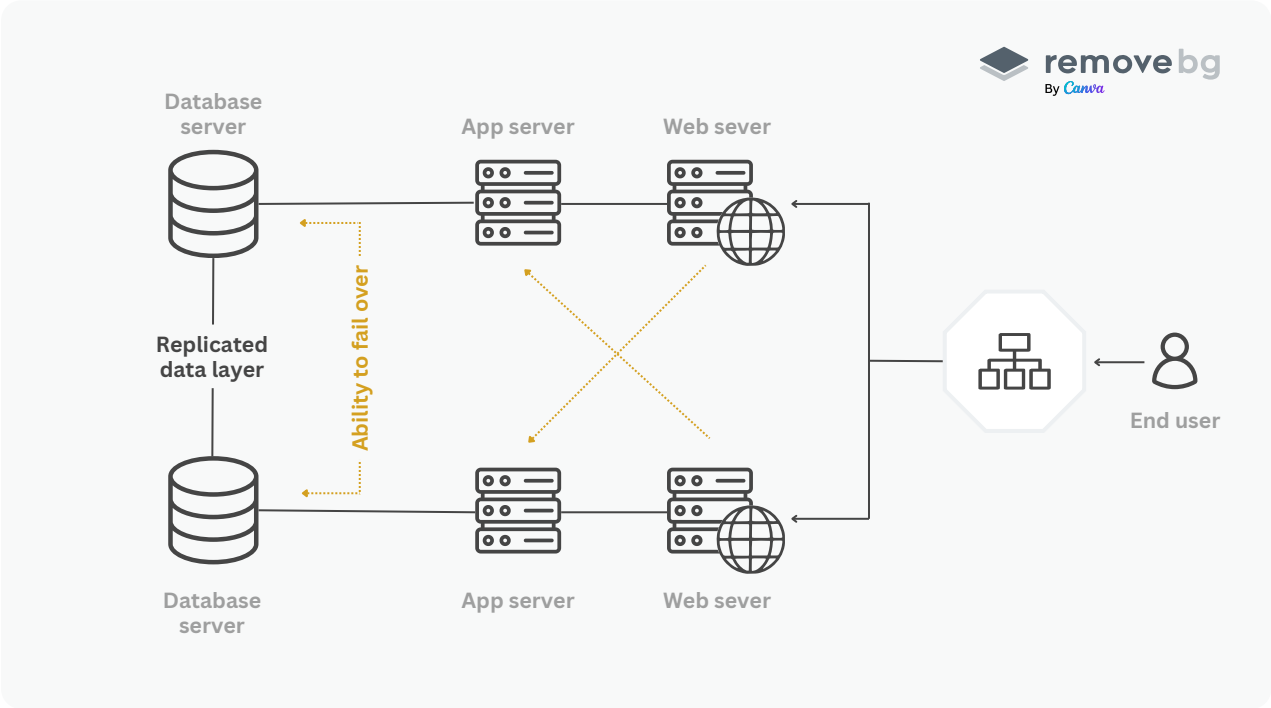
Processing of personally identifiable information (PII) requires a high level of security and a transparent legal basis. One of the most extensive privacy regulations in the world, Europe's General Data Protection Regulation (**GDPR**) is a solid legal framework with strict requirements.

remove.bg is committed to being compliant with **GDPR** and provides a **Data Processing Agreement (DPA)** according to Article 28 GDPR for the processing of PII.

GDPR

Fully redundant infrastructure

To provide uninterrupted availability of service, the remove.bg infrastructure is fully redundant. All critical components are replicated on separate hardware, enabling high availability, even in the event of infrastructure-related failures. Distributed processing clusters, **failover systems, and self-healing architectures** enable us to provide a platform that offers a maximum of reliability.



Fully redundant infrastructure to ensure uninterrupted service availability

24/7 monitoring for availability & performance

Automated Recovery Measures

The remove.bg infrastructure is monitored 24/7 to immediately detect any availability issues or performance degradation and ensure reliable service at all times.

remove.bg employs both **automated recovery measures and human alert-and-escalation procedures.**

Infrastructure is monitored on various levels, from hardware to connectivity and high-level API functioning, to cover an extensive range of error scenarios.

Frequent security updates with near zero downtime

Unpatched systems and outdated dependencies pose a security risk that could lead to unauthorized access or code execution. remove.bg **frequently reviews and updates the remove.bg server infrastructure** and software components to protect the integrity of the system and all data processed through it.

Our redundant architecture ensures that the remove.bg's **API is fully available with near zero downtime, even during maintenance events**.

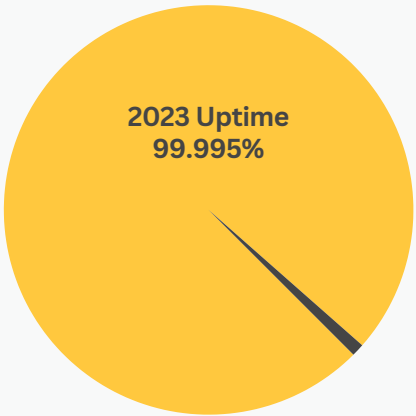
Near Zero Downtime

Recent track record

As a result of our commitment to providing a dependable service for our users, from January to December 2023* remove.bg has demonstrated exceptional reliability with an **uptime of 99.995%.** This indicates that the platform was virtually always accessible, providing a nearly uninterrupted service to its users.

This high percentage demonstrates remove.bg's commitment to ensuring that our customers can access and utilize our services whenever they need to and our dedication to reliability and consistent service.

remove.bg has had an uptime of 99.995% over the past year



**Please note that the uptime percentage is based on this specific time period. Hence, it is not always guaranteed.*

Cloud Provider Certifications

Our infrastructure hosting partners have received numerous independent security and compliance certifications, including ISO/IEC 27001, covering the frameworks and checklists for comprehensive and continually improving security management models.

You can find more information about the security certifications our cloud providers have obtained at the following locations:

cloud.google.com/security/compliance/iso-27001
cloud.google.com/security/compliance/soc-2

ISO/IEC 27001 Certified Hosting Partner

Further improvements & contact

This document summarizes remove.bg's security measures as of **February 2024.** As we strive to continuously improve our practices, new versions of this whitepaper may be released in the future.

If you have any questions or feedback on the content of this Whitepaper, please contact us: **team@remove.bg**