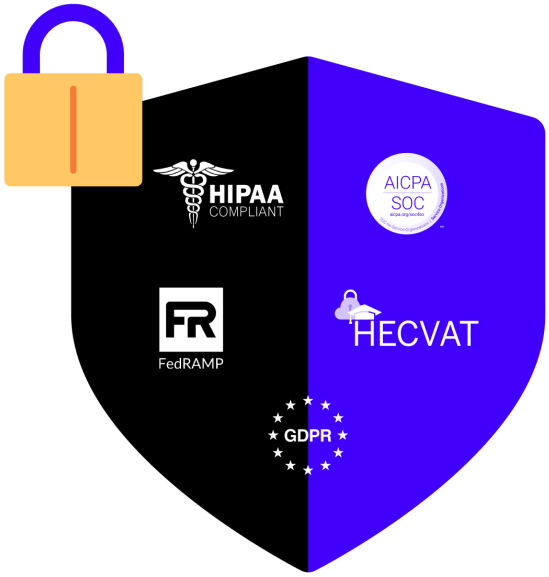
Waitwhile

Security & Compliance whitepaper



Introduction

This paper outlines Waitwhile's approach to security and compliance for our cloud-based queue management service and across our entire organization.

Table of contents

1. Security Culture

Waitwhile has created an active and inclusive security culture for all employees. The influence of this culture is apparent during the hiring process, employee onboarding, as part of ongoing training and in company-wide events to raise awareness.

Employee background checks

Before they join our staff, Waitwhile will verify an individual's education and previous employment, and perform internal and external reference checks. Where local labor law or statutory regulations permit, Waitwhile may also conduct criminal, credit, immigration, and security checks. The extent of these background checks is dependent on the desired position.

Security training for all employees

All Waitwhile employees undergo security training as part of the orientation process and receive ongoing security training throughout their careers. During orientation, new employees agree to our Code of Conduct, which highlights our commitment to keep customer information safe and
secure. Depending on their job role, additional training on specific aspects of security may be required. For instance, the information security team instructs new engineers on topics like secure coding practices, product design and automated vulnerability testing tools.

2. Operational Security

Waitwhile has a strong focus on operational security. Far from being an afterthought or the focus of occasional initiatives, security is an integral part of our operations.

Access Management

For Waitwhile employees, access rights and levels are based on their job function and role, using the concepts of least-privilege and need-to-know to match access privileges to defined responsibilities. All Waitwhile personnel are required to use multi-factor authentication and strong passwords.

Vulnerability Management

Waitwhile administers a vulnerability management process that involves scans for security threats using a combination of commercially available tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The owner then tracks the issue and follows up frequently until they can verify that the issue has been remediated. Waitwhile also offers bug bounties for disclosed vulnerabilities from external parties.

Malware prevention

An effective malware attack can lead to account compromise, data theft, and possibly additional access to a network. Waitwhile takes these threats to its networks and its customers very seriously and uses a variety of methods to prevent, detect and eradicate malware. Waitwhile leverages Google Cloud Platform anti-malware services for our cloud infrastructure. Employees are mandated to use Google's Safe Browsing in Chrome to prevent malware to be installed through visiting infected websites and make use of the built-in antivirus engines of G Suite Email and Google Drive.

Monitoring

Waitwhile's security monitoring program leverages Security Command Center's automated threat prevention (IDP) and threat detection (IDS) services. Automatic analysis is supplemented by examining system logs to identify unusual behavior, such as attempted access of customer data. Waitwhile security engineers place standing search alerts on public data repositories to look for security incidents that might affect the company's infrastructure. They actively review inbound security reports and monitor public mailing lists, blog posts, and wikis.

Incident Management

We have a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. If an incident involves customer data, Waitwhile will inform the customer and support investigative efforts via our support team.

Data Center Security

Waitwhile uses Google Cloud Platform for our cloud infrastructure. Google's data centers physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, and biometrics, and the data center floor features laser beam intrusion detection. Data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. All hardware is tracked and disposed of in a secured manner. To keep things running 24/7 and ensure uninterrupted services, data centers feature redundant power systems and environmental controls.

Encrypting data in transit and at rest

Waitwhile customers' data and our own data is encrypted when it's on a disk, moving over the Internet, or traveling between data centers. Only standardized encryption protocols and algorithms, such as TLS 1.2, 1.3 and AES, are used.

Low latency and highly available solution

Waitwhile designs the components of our platform to be highly redundant. Customer data is replicated synchronously in real-time over multiple geographically distributed data centers to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, automatic failover allows Waitwhile customers to continue working in most cases without interruption. Our highly redundant design has allowed Waitwhile to achieve an uptime of 99.95% for our service over the last years with no scheduled downtime. Simply put, when Waitwhile needs to service or upgrade our platform, users do not experience downtime or maintenance windows. Our production servers run a stripped-down and hardened version of Linux. Server resources are dynamically allocated, allowing for flexibility in growth and the ability to adapt quickly and efficiently, adding or reallocating resources based on customer demand. This homogeneous environment is maintained by software that continually monitors systems for binary modifications. If a modification is found that differs from the standard approved image, the system is automatically returned to its official state.

Leveraging Google Cloud Platform's IP data network consisting of their own fiber allows us to deliver highly available and low latency services across the globe.

3. Data Access and Restrictions

Administrative access

To keep data private and secure, Waitwhile logically isolates each customer's data from that of other customers and users, even when it's stored on the same physical server. Only a small group of Waitwhile employees have access to customer data. Waitwhile employees are only granted a limited set of default permissions to access company resources, such as employee email and internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Waitwhile's security policies. Support services are only provided to authorized customer administrators and any access to customer data is audit logged.

For customer administrators

Within customer organizations, administrative roles and privileges for Waitwhile are configured and controlled by the customer. This means that individual team members can manage certain services or perform specific administrative functions without gaining access to all settings and
data. Integrated audit logs offer a detailed history of administrative actions, helping customers monitor internal access to data and adherence to their own policies.

Law enforcement data requests

The customer, as the data owner, is primarily responsible for responding to law enforcement data requests; however, like other technology companies, Waitwhile may receive direct requests from governments and courts around the world about how a person has used the company's services. We take measures to protect customers' privacy and limit excessive requests while also meeting our legal obligations. Respect for the privacy and security of data you store with Waitwhile remains our priority as we comply with these legal requests. When we receive such a request, our team reviews the request to make sure it satisfies legal requirements and Waitwhile's policies.

Third-party suppliers

Waitwhile relies on several third-party vendors to deliver our service. Prior to onboarding third-party suppliers, Waitwhile conducts an assessment of the security and privacy practices of third-party suppliers to ensure they provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Waitwhile has assessed the risks presented by the third-party supplier, the supplier is required to enter into appropriate security, confidentiality, and privacy contract terms.

4. Empowering Users and Administrators to Improve Security and Compliance

Single Sign-On (SAML 2.0)

Waitwhile offers customers a single sign-on (SSO) service that lets users access multiple services using the same sign-in page and authentication credentials. It is based on SAML 2.0, an XML standard that allows secure web domains to exchange user authentication and authorization data. For additional security, SSO accepts public keys and certificates generated with either the RSA or DSA algorithm. Customer organizations can use the SSO service to integrate single sign-on for Waitwhile into their LDAP, Active Directory or other SSO system.

Audit logs

Waitwhile keeps an audit trail that lists all important events across customers' accounts. Audit entries contain what data changed, who made the change and when. The retention period for audit logs are 365 days.

Data recovery

Waitwhile performs daily backup of all customer data and empowers administrators to restore deleted data and users for up to 90 days after deletion. After 90 days the data cannot be restored, even if you contact technical support.
Waitwhile will delete all customer-deleted data from our systems as soon as reasonably practicable or within a maximum period of 90 days.

5. Regulatory Compliance

Waitwhile's customers have varying regulatory compliance needs. Our clients operate across regulated industries, including retail, health and finance.

General Data Protection Regulation (GDPR)

Waitwhile wholeheartedly support the privacy rights of our customers and our users and have fully implemented the required steps for GDPR compliance. Waitwhile is acting both as a Data Controller and as a Data Processor within the realm of GDPR compliance. As a Data Controller, Waitwhile is responsible for safeguarding the data of our customers as they interact directly with our services. As a Data Processor, Waitwhile is responsible for safeguarding the data of our partners' and customers' users as it flows through our system.

Partners or customers who need further documentation of compliance with Waitwhile acting as a Processor (for example, as a customer who processes their own user's data through Waitwhile or as a partner who integrates directly with Waitwhile) we offer a Data Processor Agreement that includes the Standard Contractual Clauses adopted by the European Commission.

U.S. Health Insurance Portability and Accountability Act (HIPAA)

Waitwhile supports our customers' compliance with the U.S. Health Insurance Portability and
Accountability Act (HIPAA), which governs the confidentiality and privacy of protected health
information (PHI). Customers who are subject to HIPAA and wish to use Waitwhile with PHI must sign a business associate agreement (BAA) with Waitwhile.

Children's Online Privacy Protection Act of 1998 (COPPA)

Protecting children online is important to us. We require our customers to obtain parental consent that COPPA calls for to use our services, and our services can be used in
compliance with COPPA. If we learn that we have inadvertently collected Personal Information from a child under age 13, we will delete that information as quickly as possible.

6. Independent Third-Party Certifications

Waitwhile's customers and regulators expect independent verification of our security, privacy, and compliance controls. In order to provide this, we undergo several independent third-party audits on a regular basis. When customers consider Waitwhile, these certifications can help them confirm that the product suite meets their security, compliance and data processing needs.

SOC 2

Waitwhile has passed an SOC 2 Type 2 audit without exceptions and the report is available upon request. The certification will be renewed bi-annually.

HIPAA

Waitwhile has passed an SOC 2 Type 2 audit with an HIPAA mapping and the report is available upon request.

Penetration Test

Waitwhile conducts third-party penetration tests annually.

7. Conclusion

The protection of user data and high availability are the primary design considerations for all of Waitwhile's infrastructure, services and personnel operations. We strive to create the most comprehensively secure queue management service available. We also offer strong regulatory compliance and contractual commitments to make sure our customers maintain control over the data and how it is processed.