Calendly

Security White Paper

This document provides a technical summary of Calendly's approach to security and compliance.

CONTENTS

3 Calendly's Service Security

3 About Calendly

3 Before Hiring

4 Upon Hiring

4 While Working for Calendly

4 When Departing Calendly

5 The Calendly Cloud Service

5 Calendly Infrastructure

6 Shared Responsibility Model

6 Security Controls

6 Infrastructure & Physical Security

7 Security of Data Centers

7 Data Security

8 Least Privilege Access

8 Secure AI: Principles and Practices

9 Network Security

9 Virtual Private Networks

9 Distributed Denial of Service (DDoS) attacks

9 Man in the Middle (MITM) attacks

10 IP Spoofing

10 Port scanning & Packet sniffing

10 Secure Personnel Practices

10 Software Development Life Cycle (SDLC)

11 Development Practices

12 Auditing of SDLC Processes

12 Supply Chain

12 Disaster Recovery and Continuity Planning

13 Compliance

14 Additional Resources

Calendly's Service Security

About Calendly

Calendly is the market-leading scheduling solution. Our platform allows for secure and efficient scheduling, eliminating the hassle of back-and-forth communication so you can get back to work.

The Calendly Security team diligently works to secure customers scheduling data and interactions on the platform.

Before Hiring

Before hiring, all employees and contractors undergo background checks in accordance with applicable laws. The background check reviews areas such as criminal and financial background indicators and includes a credit check for senior finance positions.

All new hire references, both requested and unrequested, are carefully scrutinized. Employees and contractors are made aware of their responsibilities, plus operational and security policies, as well as repercussions for failure to adhere to said responsibilities and policies.

Upon Hiring

Upon hiring, all employees and contractors go through an onboarding process that includes:

- Signing a Proprietary Information & Inventions Agreement (PIIA). The PIIA states the confidentiality obligations as a Calendly employee or contractor.
- Completing the employment onboard and security awareness training and security policy/procedure acknowledgement. This training helps new hires understand their security responsibilities as a Calendly employee or contractor.

While Working for Calendly

Calendly uses endpoint encryption, antivirus protection, and endpoint management tools to ensure security of company-owned devices. We use Multi-Factor Authentication (MFA) for all SaaS products.

Security awareness training is an ongoing educational process which strives to ensure that employees and contractors understand basic cyber security principles and their responsibility to secure company and customer data. Training includes assorted cybersecurity topics, including but not limited to, phishing awareness and SDLC developer training.

When Departing Calendly

- All Calendly employees and contractors are reminded of their confidentiality obligations upon leaving
- All user accounts, passwords, hardware, and badges are revoked and within 24 hours of termination
- Calendly uses SCIM provisioning to automate deprovisioning user accounts and access

The Calendly Cloud Service

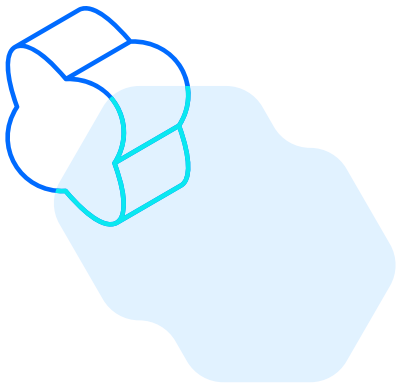
The Calendly cloud service is a software as a service (SaaS) solution built and maintained by Calendly. As a true cloud-native service, it is fully designed and assembled for the cloud and provides some key benefits:

- Subscription-based and cost-efficient
- Drastically reduces setup, operational complexity, and total cost of ownership
- Globally available, 100% multi-tenant, redundant with multiple availability zones
- Regularly updated with security updates and new features
- Minimum downtime as we apply regular updates on the fly where possible (tracked here)

Calendly Infrastructure

The Calendly application uses Google's infrastructure as a service (IaaS) Google Cloud Platform (GCP) offering.

Google Cloud Platform is a suite of cloud compute services offered, hosted, and managed by Google, GCP utilizes continuous monitoring, distributed data centers with layered security, continuous availability, secure by design infrastructure, as well as encryption at rest and in transit. By leveraging GCP, we are able to provide our customers with reliability, security, scalability, and elasticity that meets the demands of modern businesses.



Shared Responsibility Model

Calendly's software as a service is built, managed, monitored, and updated with security as a top priority. As part of our commitment to security, quality, consistency, and compliance, Calendly has adopted the shared security responsibility model

The shared responsibility model is a framework used by all major cloud providers (Google, Amazon, Microsoft, etc.), and serves to identify and define the distinct ownership responsibilities between the cloud provider and the customer. As we build our applications and infrastructure platform with Google Cloud resources, we utilize this responsibility matrix to govern our internal infrastructure controls.

Security Controls

As a SaaS service provider, Calendly is responsible for providing and/or overseeing through its partners the security of the Calendly cloud application service.

The security controls in place are classified into the following general categories:

- Data classification and accountability
- Client and end-point protection
- Identity and access management
- Application-level controls
- Network controls
- Host infrastructure
- Physical security

Infrastructure & Physical Security

Calendly utilizes Google's management services and software interfaces in a shared responsibility model (as detailed above). With this approach, Calendly takes advantage of all the capabilities and controls offered by the Google Cloud.

Calendly utilizes a virtual private cloud (VPC) within GCP to add an additional layer of virtual separation of services. We install and fine-tune application firewall configurations, and implement strict access controls for cloud services, these controls include Identity & Access Management (IAM) role-based access controls that define granular permissions based upon team and role.

Security of Data Centers

Google designs and builds its own data centers, which incorporate multiple layers of physical security protections. Access to these data centers is limited to only a very small fraction of Google employees. Multiple physical security layers are used to protect the data center floors. In addition, technologies like biometric identification, metal detection, cameras, vehicle barriers, and laser-based intrusion detection systems are being used. Google additionally hosts some servers in third-party data centers, where they ensure that there are Google-controlled physical security measures on top of the security layers provided by the data center operator. For example, in such sites they may operate independent biometric identification systems, cameras, and metal detectors.

Data Security

Calendly understands that your data is a valuable asset and we treat it as such. We encrypt all data, in transit and at rest. Calendly requires HTTPS for all services using TLS (v1.2 or higher using non-deprecated cipher suites) with HSTS enabled and SHA-256 with 2048 bit RSA encryption.

We store passwords using an industry standard modern hashing algorithm with the recommended work factor to create a one-way, salted hash. Login pages and logins using Calendly APIs are all protected by rate-limiting controls. Run time systems are supported with high availability data stores that are configured with hot failover replicas.

Calendly has stringent security policies for database data storage, cloud storage, and backups. We utilize Google Cloud Persistent Disk (Block Storage) and Google Cloud Storage (Object Storage) for persisting data. Backups are performed daily and data is persisted on multiple clouds (AWS and GCP). Within cloud providers, we restrict access at the bucket level and only permit certain authenticated users read/write access based on a combination of bucket, roles, policies, and IAM grants.

Least Privilege Access

Calendly requires that all access to its infrastructure, application, and data be controlled based on business and operational requirements. Role based access to systems and data is requested, approved, tracked, and monitored. Right to access is restricted based on employee role and audited for continued need, at a minimum, quarterly. System and data interactions are captured in system logs and retained for one year.

Secure AI: Principles and Practices

At Calendly, we are committed to the ethical and responsible development and deployment of artificial intelligence. As AI becomes increasingly integrated into our products and operations, we recognize the importance of aligning our practices with industry-leading standards for security, transparency, fairness, and accountability. To that end, Calendly maintains a zero data retention policy, meaning no user inputs or outputs are stored or used for model training. This ensures that customer data remains private and protected.

In addition to rigorously tested guardrails, we also conduct regular third-party penetration testing to validate the security and resilience of our "Note taker" AI platform and ensure the timely remediation of identified potential vulnerabilities.

Network Security

Calendly leverages Google Cloud in tandem with best-of-breed security solutions to provide protection against traditional network security threads. They include some of the following:

Virtual Private Networks

We utilize Google's virtual private network capabilities to create and connect the necessary private networking infrastructure and isolate traffic between any of the underlying components from the public. This includes peering with third-party service providers.

Distributed Denial of Service (DDoS) attacks

Successfully handling DDoS attacks is a shared responsibility between Google Cloud and Calendly. It involves detection systems, barriers, and scalability in order to absorb attacks. As part of the shared responsibility model, we've provided extra layers of protection by actively reducing the attack surface for our deployments, isolating all internal traffic, utilizing proxy-based load balancing, and autoscaling.

Our added DDoS mitigation infrastructure provides protection against attacks at Open Systems Interconnection (OSI) layers 3, 4, and 7.

Man in the Middle (MITM) attacks

For every machine or container, Calendly uses automation services to issue secure TLS certificates via Internet Security Research Group's (ISRG) Let's Encrypt. We leverage secure APIs to access the certificates before using an instance.

IP Spoofing

Google provides anti-spoofing protection of IP addresses in virtual private networks by default. Furthermore, isolation between virtual networks comes by default. Anti-spoofing checks are performed against traffic, ensuring that traffic exiting virtual machines (VMs) uses VM IP addresses and pod IP addresses as source addresses. The checks verify that VMs don't send traffic with arbitrary source IP addresses.

Port scanning & Packet sniffing

Calendly utilizes the existing built-in protection of GCP along with firewalls and VPCs to protect against those types of attacks. All network communication is encrypted and network ports explicitly opened when necessary. In addition, we utilize external security tools for attack monitoring and prevention.

Secure Personnel Practices

Software Development Life Cycle (SDLC)

Calendly's Software Development Life Cycle is designed to identify and reduce security risks from feature inception through delivery and maintenance of our software to the production environment. As an idea becomes a feature concept, we perform research and user testing to gather requirements that undergo architecture evaluation of system and application design. Architecture teams work closely with engineering teams in the design phase to create an implementation plan that enumerates data flows as well as potential security and privacy concerns.

Upon passing security review, the implementation plan moves into the development phase. Changes to our codebase are required to include unit tests, integration tests, and end-to-end tests to confirm functionality. One or more code reviews are required to address standards adherence. Changes are also run against our

continuous integration server, and include static code analysis as well as vulnerability scanning. This enables us to automatically detect any issues in development.

The change set is then evaluated by our quality assurance team to thoroughly test areas of expected impact, regression test, and further evaluate the user experience. After all checks are completed successfully, deployments are secured with image scanning, logging, and anomaly detection. Our 24/7 response procedures backed with a suite of monitoring, logging, detection, and alerting tools provides protection against real-time risks and enforces patching of newly identified vulnerabilities.

Development Practices

Our rigorous application development processes adhere to Open Web Application Security Project (OWASP) and with the CLASP concepts. Continuous training for developers helps to ensure appropriate awareness, focus and protection for various types of potential attacks, such as:

- Malformed input
- SQL injection
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- Broken Authentication and Session Management
- Insecure Direct Object References
- Security Misconfiguration
- Sensitive Data Exposure
- Other Open Web Application Security Project
    - Top 10 threats (OWASP's Top 10)

Auditing of SDLC Processes

On a regular basis, no less than annually, evidence of the above testing and change management is gathered and analyzed to ensure that these testing flows and change management procedures are being performed as required.

Supply Chain

Prior to engaging new vendors, Calendly compares multiple competing solutions and performs thorough security and compliance assessments. Once we have reviewed the competing solutions, accompanying documentation, and security/ compliance questionnaires, we utilize a review process to assess security, compliance, and total cost of ownership. Every vendor that handles customer Personal Identifiable Information (PII) is required to have a Data Protection Agreement (DPA) in place that contractually obligates them to handle PII according to privacy law requirements. Our sub-processor list on our website is also updated prior to onboarding vendors that handle customer PII.

We maintain system configuration and consistency through standardized, up-to-date images, configuration management software, and automated continuous delivery processes. Within our application, each new library requires explicit request and evaluation prior to inclusion into the code base. We continuously scan libraries for new Common Vulnerabilities and Exposures (CVEs.) Any issues discovered are ranked based upon risk, prioritized, addressed, and then validated, internally and externally, for resolution. We deploy systems using updated images managed through versioned configuration changes that contain the latest security updates. Once deployed, existing systems are decommissioned and replaced with the up-to-date system.

Disaster Recovery and Continuity Planning

While we work tirelessly to prevent them, disasters happen and that is why we create, maintain, and execute plans for them. At a minimum, once a year, we come together to assess new risks, design new plans, review existing plans, and test likely failure scenarios to exercise the

plans as if they were occurring in real time. The plans include but are not limited to:

- Incident response for security, data, and production service disruptions
- Emergency succession plan
- Data classification and protection plan
- Service classification and recovery plan
- Data backup and restoration plan
- Mass media management plan

Compliance

Calendly goes through third-party SOC 2 Type II and ISO-27001 security audits on an annual basis. A copy of our SOC 2 audit report and ISO-27001 certificate can be requested under an NDA when appropriate. Calendly routinely monitors and actively addresses compliance and regulatory requirements. Calendly offers pre-filled security questionnaires (the SIG or CAIQ) covering our environment upon agreement of an NDA.

To access Calendly compliance documents, a user must create a profile and submit an access request via the Whistic platform available here.

If a Non-Disclosure Agreement (NDA) is a prerequisite for specific documents, the necessary instructions will be provided within the Whistic platform.

Calendly is fully committed to compliance with the General Data Protection Regulation (GDPR). We incorporate privacy by design standards, cookie compliance, and other requirements as put forth by GDPR into our data practices. Calendly's compliance department ensures that our customer data from the EU, UK, and Swiss Economic Area is handled in a secure and confident manner according to GDPR. Calendly also aligns to the California Consumer Privacy Act (CCPA) requirements as well as many other extraterritorial privacy laws around the world. Calendly is also a certified member of the EU-US Data Privacy Framework.

Additional Resources

1. Calendly Security and compliance: https://help.calendly.com/hc/en-us/sections/4411772410519-Security-Compliance
2. Calendly Note taker https://help.calendly.com/hc/en-us/articles/21652725311383-Calendly-Notetaker-overview
3. Google Cloud platform Shared Responsibility Matrix https://docs.cloud.google.com/architecture/framework/security/shared-responsibility-shared-fate
4. Google Cloud compliance center https://cloud.google.com/security/compliance
5. Google Cloud DDoS Protection and Mitigation https://cloud.google.com/files/ GCPDDoSprotection-04122016.pdf
6. Google Cloud Security https://cloud.google.com/security