calendly

Security white paper

Calendly takes data security and privacy very seriously. We recognize that information security is important to you. This paper outlines our approach to security and compliance and describes the organizational and technical controls we use to protect your data.

Our commitment to you

- We only access, store, and process customer data for product functionality and improvements
- We provide the highest level of security and availability within our means.
- Our support and service interactions with you will be human.
- We will communicate transparently.

How we provide physical security

Calendly leverages Heroku, the cloud application platform, to facilitate the operation and deployment of our software. Calendly personnel don't directly access any serving or networking infrastructure; instead, we rely on Heroku's services.

With this approach, Calendly takes advantage of the following capabilities.

"Heroku utilizes ISO 27001 and FISMA certified data centers managed by Amazon. Amazon has many years of experience in designing, constructing, and operating large-scale data centers. This experience has been applied to the AWS platform and infrastructure. AWS data centers are housed in nondescript facilities, and critical facilities have extensive setback and military grade perimeter control berms as well as other natural boundary protection. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, state-of-the-art intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication no fewer than three times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.

Amazon only provides data center access and information to employees who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical and electronic access to data centers by Amazon employees is logged and audited routinely."

Amazon's data center operations are certified to be compliant with these standards:

- ISO 27001, 27017, and 27018
- SOC 1 and 2
- SSAE 16
- PCI Level 1
- FISMA Moderate
- Sarbanes-Oxley (SOX)

For more information, see:

https://aws.amazon.com/security

Environmental safeguards

Fire detection and suppression

AWS deploys automatic fire detection and suppression equipment and smoke detection sensors to reduce risk in all data center environments, mechanical and electrical infrastructure spaces, and chiller and generator equipment rooms. These areas are protected by wet-pipe, double-interlocked pre-action, or gaseous sprinkler systems.

Power

Data center electrical power systems are fully redundant and maintainable without impact to operations, 24 hours a day, seven days a week. Uninterruptible Power Supply (UPS) units provide back-up power in the event of electrical failure for critical and essential loads in the facility. Generators provide backup power for the entire facility.

Climate and temperature control

Climate control is required to maintain a constant operating temperature for servers and other hardware to prevent overheating and reduce the possibility of service outages. Data centers are conditioned to maintain atmospheric conditions at optimal levels. Monitoring systems and data center personnel ensure temperature and humidity are at the appropriate levels.

Management

Data center staff monitor electrical, mechanical, and life support systems and equipment so issues are immediately identified. Preventative maintenance is performed to maintain the continued operation of equipment.

Network security measures

Firewalls

Firewalls restrict access to systems from external networks and between internal systems. By default, access to ports and protocols is allowed based on business need. Each system is assigned to a firewall security group based on the system's function. To mitigate risk, security groups restrict access to those ports and protocols required for a system's specific function.

To isolate customer applications, host-based firewalls restrict applications from establishing localhost connections over the loopback network interface. Host-based firewalls also limit inbound and outbound connections as needed.

DDoS mitigation

Our infrastructure provides DDoS mitigation techniques including TCP Syn cookies, connection rate limiting, and multiple backbone connections, and internal bandwidth capacity that exceeds the Internet carrier-supplied bandwidth. We work closely with our providers to quickly respond to events and enable advanced DDoS mitigation controls when needed.

Spoofing and sniffing protections

To ensure spoofing is not possible, managed firewalls prevent IP, MAC, and ARP spoofing on the network and between virtual hosts. Packet sniffing is prevented by infrastructure, including the hypervisor, which won't deliver traffic to an interface on which it is not explicitly addressed. To further ensure risk is mitigated at all levels.

Heroku uses application isolation, operating system restrictions, and encrypted connections.

Port scanning

Port scanning is prohibited and every reported instance is investigated by our infrastructure provider. When port scans are detected, they are stopped and access is blocked.

Application security

Calendly incorporates security checks throughout the Agile process. This begins with requirements definition where security improvements, patches, and remediation items are prioritized according to risk and severity classification (provided by an internal security team and supported by best-in-class external partners).

In the planning phase for new features, we require explicit risk analysis, data review, and documentation. Each change set must have unit, integration, and end-to-end tests, based on associated test cases.

To Calendly's coding standards all code is statically analyzed for vulnerabilities in our CI/CD pipeline and manually reviewed to ensure adherence. With each commit during development, QA, and stakeholder testing, we execute an exhaustive automation test suite.

We maintain system configuration and consistency through standardized, up-to-date images, configuration management software, and automated continuous delivery processes. 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.

We continuously scan libraries for new Common Vulnerabilities and Exposures (CVEs) and monitor anomalous traffic patterns and behaviors, and employ best practice alerting and incident management procedures.

Data security

We read the free and busy times from the calendars you connect with Calendly to prevent double booking. We store appointment data for events booked through Calendly so that our customers are able to view past and future appointments that invitees have booked.

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 RSA encryption. We store passwords using a one-way, salted hash algorithm that can't be decrypted.

Login pages and logins using Calendly APIs have brute force protection. Run time systems are supported with high availability data stores that are configured with hot failover replicas. Data is backed up and encrypted nightly and stored in geographically disparate locations.

We have procedures defined for disaster recovery and business continuity in event of catastrophic infrastructure failure, natural disaster, or pandemic scenarios.

Corporate Security

Calendly has implemented policies and procedures that cover many security and compliance topics which are reviewed on an annual basis or more frequently when needed.

Newly-hired Calendly employees receive security training on company policies and procedures, information security, privacy law, and other security and compliance topics. We administer that training annually and require role-based training (depending on the job function).

Physical access to our building is monitored 24/7 by building security and access to Calendly's office is monitored by our security team. Physical access to Calendly's corporate facilities is restricted to Calendly personnel and registered visitors that are accompanied by Calendly personnel. We use a badge access system to ensure that only authorized individuals have access to restricted areas within Calendly's facilities such as areas that contain servers and network equipment. We review the list of individuals approved for physical access at least quarterly.

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 where it's available.

Compliance

Calendly contracts with best-in-class third-party security professionals who annually perform penetration tests, vulnerability assessments, and source code analysis to validate the security of our application. Our engagements cover the full spectrum of application architecture, role-based security, data stewardship, and application functionality. Any issues discovered are ranked based upon risk, prioritized, addressed, and then validated, internally and externally, for resolution.

Calendly processes payments using integrations with Stripe and PayPal. We never retain customer credit card data.

For more information about our payment processors' security

See:

- Stripe, https://stripe.com/docs/security.
- PayPal, https://developer.paypal.com/docs/authentication-security/.

Calendly's security is audited by a third-party auditor using the SOC 2 framework. To see a copy of our latest SOC 2 report, please contact support@calendly.com.

References:

"Heroku Security" Heroku, https://www.heroku.com/policy/security Accessed 20 April 2020