Robin

53 State St, Suite 2601, Boston, MA 02209
robinpowered.com | 1 (617) 910-0454

Our company

Robin helps companies all over the world deliver a better workplace experience and has done so since 2014, with the introduction of our conference room scheduling tablet app. Today, Robin's cloud-based subscription software enables people to do their best work with an interactive office map that helps to find spaces, desks, and colleagues.

We are the AI platform for workplace operations. Plan, manage and use the office effectively with a unified platform designed for every workplace leader across IT, facilities and operations. Companies can access the platform via web, tablet, and mobile applications and integrate with Google, Microsoft and others. Used by hundreds of thousands of employees from over 1,600 companies, including HubSpot, Spotify, and Splunk, Robin pays the highest level of attention to security, scalability, and reliability to ensure workplace professionals can build the best and most secure version of their office.

Robin is backed by publicly-traded workplace leader MillerKnoll and top-tier venture capital firms FirstMark Capital and Tola Capital that have considerable experience in technology.

We're overwhelmingly an engineering organization, and highly active in developing secure and scalable systems with the best tools available. Prior to Robin, members of our team built companies that served everything from multinational enterprise organizations to high-sensitivity government agencies like the US Air Force.

Robin is headquartered in Boston with over 85 employees. See what's new at robinpowered.com.

53 State St, Suite 2601, Boston, MA 02209
robinpowered.com | 1 (617) 910-0454

Compliance

GDPR

As of May 25th, 2018, Robin is compliant with the EU's General Data Protection Regulations (GDPR). Robin has undergone the appropriate measures to be compliant, and by definition, Robin is a Processor under GDPR. We engaged third-party compliance reviews through Sphaerist Advisory and TrustArc's GDPR Priorities Assessment to ensure legal agreements, processes, and data governance are compliant. As part of the process, we've added better explanations for how Robin uses cookies throughout our Apps. More detailed information is in our updated privacy policy surrounding how Robin collects, uses, stores, and processes data within the United States.

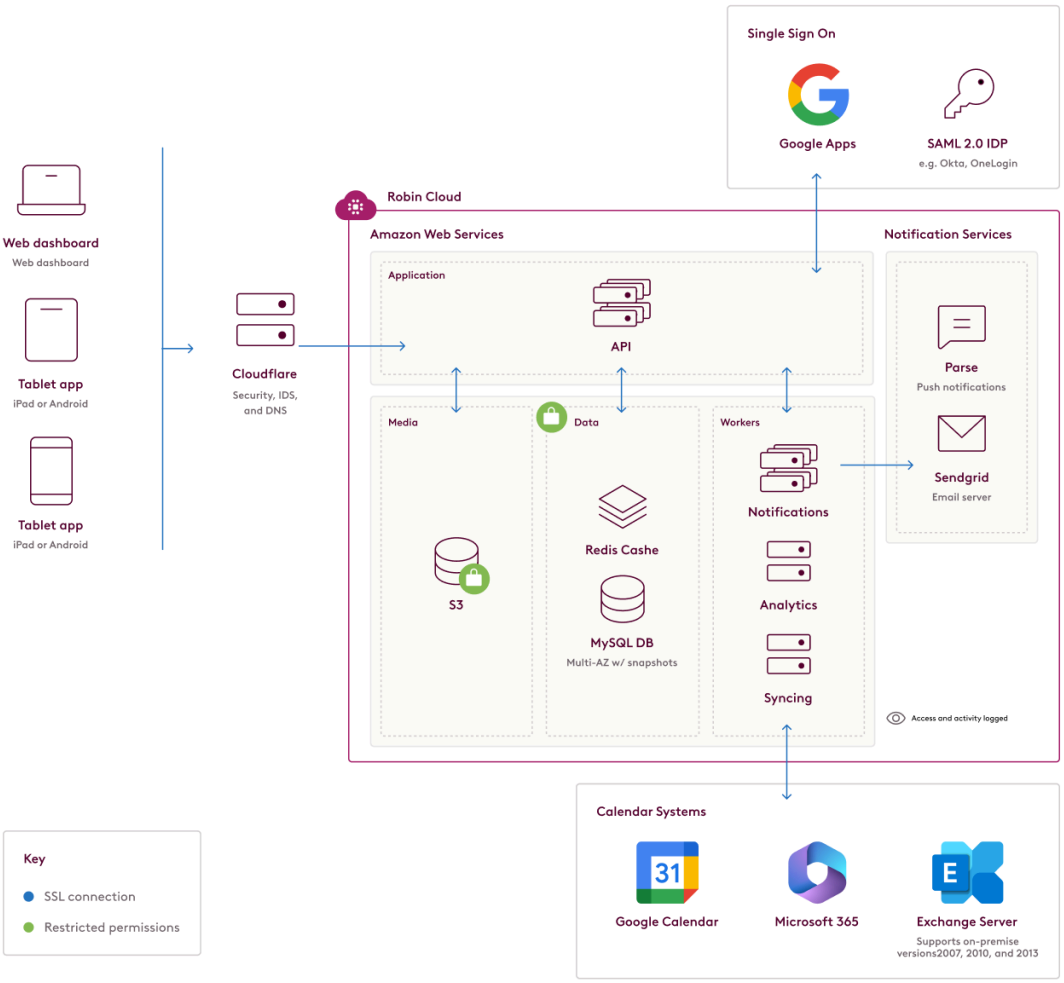
ISO 27001: 2013

ISO/IEC 27001:2013 is an industry-wide accepted information security certification that focuses on the implementation of an Information Security Management System (ISMS) and security risk management processes. Robin achieved ISO 27001 Certification in March 2020 and the certificate is available upon request.

53 State St, Suite 2601, Boston, MA 02209
robinpowered.com | 1 (617) 910-0454

Network architecture

Robin Network Topology



Encryption

Customer data is encrypted when in-transit and at rest. All connections with Robin's services are encrypted and served through SSL/TLS 1.2+. You cannot access the service without using HTTPS. All certificates are verified on both sides with third party authorities. Data is encrypted every step of the way:

- Applications → Cloudflare
- Cloudflare → Amazon Web Services
- REST request → Robin application layer
- Robin application layer → Key Management Service → MySQL session
- API response → Applications

When at rest, customer data is encrypted using a key management system which logs all access automatically. Additionally, passwords are both hashed and salted using one-way encryption, which will protect them even in the unlikely event of unauthorized database access. Application credentials are stored separate from the code base. Clients authenticate with Robin using a token system. Each token has specific access scopes, which can be individually revoked without impacting others on the platform.

IP addresses for whitelists

Robin's public-facing web service uses the following IP addresses for calendar connection and webhooks. If you host your calendar server on-premise (e.g. Exchange), add these addresses to your firewall's whitelist. This will make sure Robin is able to connect.

- 52.2.86.183
- 52.1.210.4
- 52.70.146.223

For additional verification, you can also match user agents containing RobinAPI, which will appear similar to RobinAPI/123456 in the request headers.

Ports

All application traffic is via standard web traffic port 443.

Application Domains

For networks that whitelist outbound connections, you can verify against our DNS (e.g. *.robinpowered.com) which is signed via DNSSEC. DNSSEC removes the need for specific IP address ranges since the DNS record itself is secured and can be validated with third-party authorities similar to an SSL certificate. You can confirm using this tool from Verisign.

Data center

Robin is a cloud service and hosted by data centers with the highest level of certifications including ISO 27001 and SOC. For more compliance information, you can visit AWS Security and AWS Compliance.

Data residency

You can choose whether to store your organization's data in either our U.S. or European data center. All application servers and data storage will be based in the chosen data center, but may be accessed internationally via the internet. Robin's CDN serves static assets (e.g. webpage stylesheets, avatar images) from servers across the world, but does not touch sensitive customer data.

Decommissioning and data removal

All customer data is stored on AWS services, which follows a strict decommissioning policy outlined in the “Media Destruction” section on their Data Center Controls Page.

"Media storage devices used to store customer data are classified by AWS as Critical and treated accordingly, as high impact, throughout their life-cycles. AWS has exacting standards on how to install, service, and eventually destroy the devices when they are no longer useful. When a storage device has reached the end of its useful life, AWS decommissions media using techniques detailed in NIST 800-88. Media that stored customer data is not removed from AWS control until it has been securely decommissioned.."

For customer-specific data, we will manually remove all identifying calendar data associated with your account from our database. Derivate anonymized data (i.e. "Total events booked on the platform this month") will not be removed, as it cannot be linked back to source data. User accounts associated with your organization may also be removed on request. We retain backups for 30 days, after which time the data will be completely unobtainable.

Uptime and Reliability

We constantly monitor our service performance and have automatic notifications to ensure a rapid response for service interruptions. All code is audited and approved by at least two engineers before deploying to production servers. We also monitor updates from the security community and immediately update our systems when vulnerabilities are discovered.

When we do have issues reported or planned maintenance windows, we keep an updated system status here.

Payment information

When you sign up for a paid subscription via credit card, we do not store your information on our servers. We currently use Stripe as a payment processor, which is a PCI-Compliant industry leader and dedicated to safely storing sensitive payment data. You can find a copy of Stripe's security practices here.

We do not store any data with regulatory requirements, such as HIPAA or PCI.

Authentication

Password authentication is available by default to end users and validated by entropy to restrict weak passwords. Robin also supports Single Sign-On through SAML 2.0, Google SSO, and ADFS (via SAML 2.0). Users registered through SSO use JIT provisioning. SCIM 2.0 support is offered for automatic provisioning and de-provisioning of users.

Application Development

New features, performance improvements, and bug fixes are deployed multiple times per week. While agile, our development cycle relies heavily on a strict system for code quality and security. All code is peer reviewed, and requires multiple levels of acceptance in test/staging environments prior to deployment to production.

Key highlights for common questions:

- Changes are checked for security and errors via extensive unit, integration, and static analysis tests
- Production data is separated from development environments
- We have completed rigorous reviews by internal security teams for multiple public companies

Patching vulnerabilities

Servers are patched regularly to maintain a top security rating. Vulnerabilities are tracked via a combination of automated mailing lists, and critical systems are monitored in real time with Threat Stack IDS and vulnerabilities reviewed daily. Third party network vulnerability and web application penetration tests are completed on an annual basis.

Our engineering team actively contributes to security libraries, including an open-source library of Microsoft's NTLM encryption used for secure Exchange authentication.

Audit logs

Robin syncs all calendar data with your existing system (e.g. Exchange), and you can continue to use the audit logs generated there to monitor activity between Robin and your system.

System availability and status updates are also available via

status.robinpowered.com and updates.robinpowered.com where you may also subscribe to automated notifications.

Data collected

You can find an in-depth summary of information we collect in our privacy policy, or refer to the next section for specifics around calendar events.

Calendar syncing

Once an external calendar account is connected to Robin, our cloud service will begin to synchronize data with the designated room calendars. In doing so, a subset of your calendar events and their details will be saved in Robin.

Robin will then keep this data in sync with your calendar system. Events booked through Robin will similarly synchronize the data back to your calendar service so that Robin and connected calendars stay consistent. Synced event details include:

- Title
- Description
- Visibility (i.e. Private/Not Private)
- Start and end times
- Location (e.g. “Acme Conference Room”)
- Organizer
- Attendees

You may apply additional controls by changing the permissions of the associated service account Robin uses to access your calendar system. See an example with private meeting titles with Office 365 and Exchange.

We do not store event attachments. You can learn more about our specific connection practices by service (e.g. Exchange) in our help center.

Employee access

We maintain automatic access and security logs in multiple locations. All Robin employees are required to use two-factor authentication and strong passwords that are unique from other services. Customer data access is governed by our documented security policies, and limited to a small set of employees as required for support and maintenance. Access is further limited to a small whitelist of IP addresses via VPN that require public key authentication and two factor authentication.

Individual employee access follows a principle of least access and access rights are reviewed quarterly.

Privacy

We take the security of customer data very seriously, and treat it as a banner metric for success internally. You can find a complete outline (including our Privacy Shield compliance for international customers) in our privacy policy.

Security policies

All employees are governed by documented strict security policies covering acceptable use, customer data, and encryption standards.

Disaster recovery

Application and customer data is stored redundantly at multiple availability zones within Amazon's data centers with backups available for immediate recovery.

Backups

Customer data is automatically backed up daily to Amazon S3, a highly redundant storage system. Backups are retained for 30 days to recover in the event of a disaster. They are destroyed automatically at the end of this period.

Incident response

In the event of a security breach, our team will notify you within 24 hours of unauthorized access to your data. Service availability incidents are published to our status page with additional information. See an example incident report.

Should your security team need additional logs for their investigation of an incident determined to affect your organization, our security team will coordinate responsibly to provide access as needed.

Appendix

How to contact us

We know these issues are important to you. If you have any additional questions that aren't answered above or by the Robin Help Center, please email security@robinpowered.com and we'll reply as quickly as we can.

You may also reach us via the mailing address below:

Robin Powered Inc.
Attn: Security
53 State St Suite 2601
Boston, MA 02109

If you believe you've found a security vulnerability while using Robin, we'd also like to hear from you. Fixing problems quickly and responsibly is incredibly important to us.

Related Policies

For the full picture, you may also want to review the following:

- Acceptable Use Policy
- Terms of Service
- Privacy Policy
- Amazon Web Services Security Whitepaper