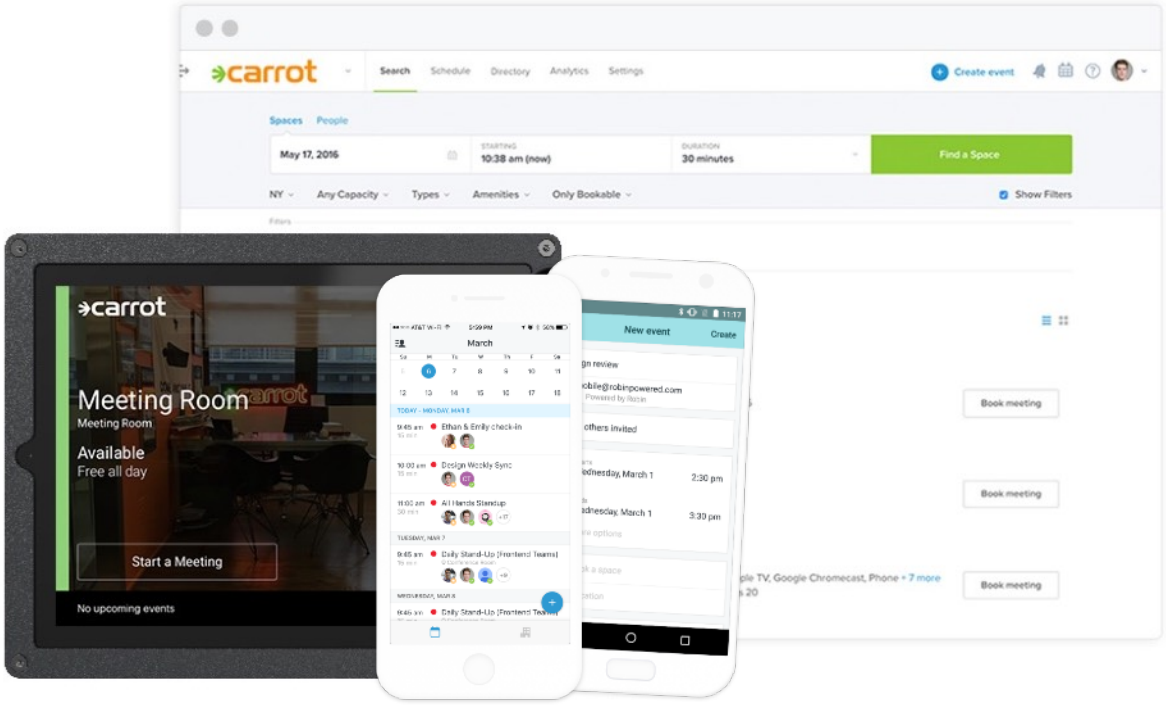
Product

Robin is cloud-based subscription software for managing offices. It integrates with the calendars you're already running, to enable better coordination of shared resources such as conference rooms. Robin is accessed through web, tablet, and mobile applications. It provides scheduling and analytics tools that office admins (and the employees they assist) find easier to work with. You can learn more **on our website.**



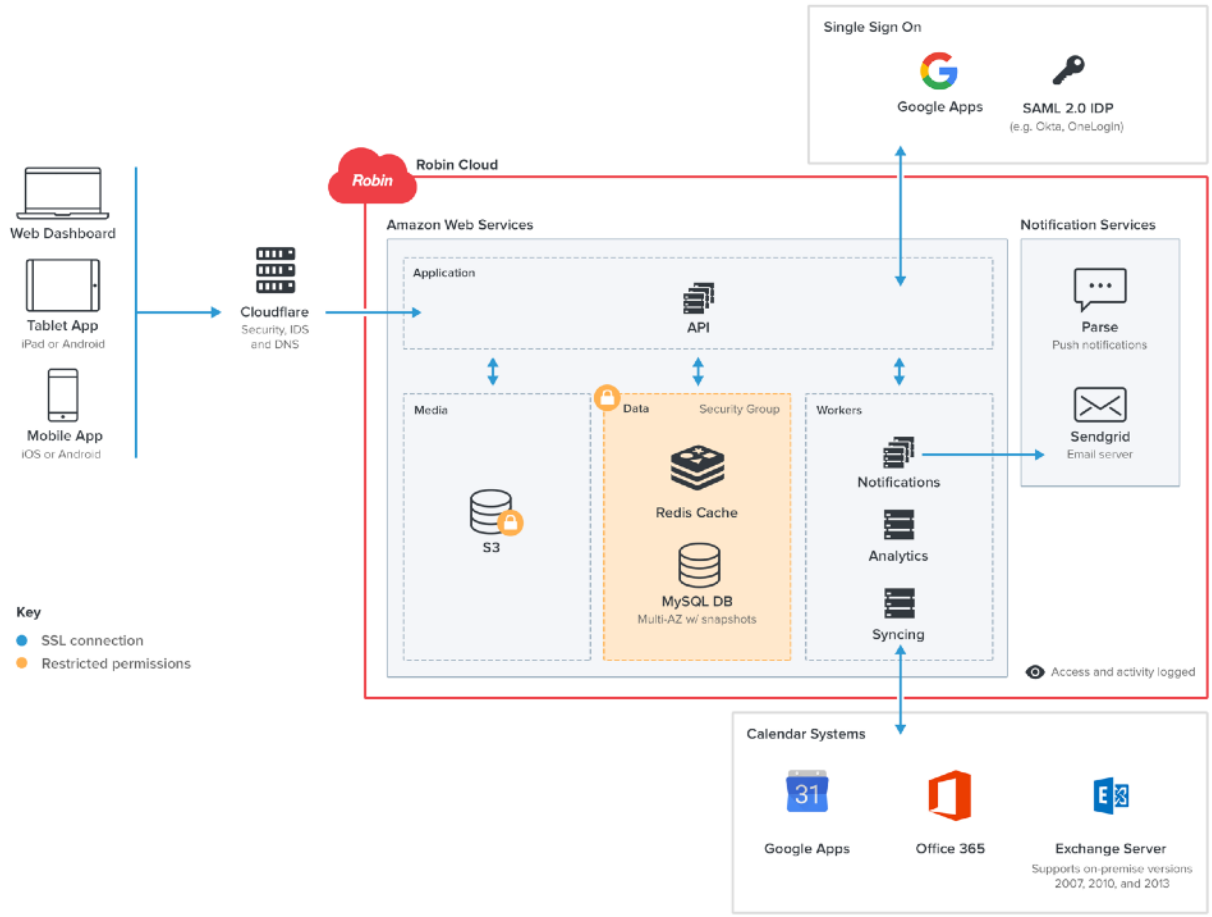
Company

Today Robin manages hundreds of offices of all sizes and industries, ranging from start up to highly-regulated institutions. We count companies of all sizes (and virtually all habitable parts of the world) as customers. They expect the highest level of attention to security, scalability, and reliability. We don't take this trust lightly.

Robin is backed by publicly-traded technology and workplace leaders like **Autodesk** and **Herman Miller**. We are also funded by investments from several top tier venture capital firms with 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 multi-national enterprise companies to high-sensitivity government agencies like the US Air Force. You'll be able to have a deeply technical conversation with virtually any member of the team.

Please ask hard questions. We're happy to answer them.



Compliance

Network Architecture

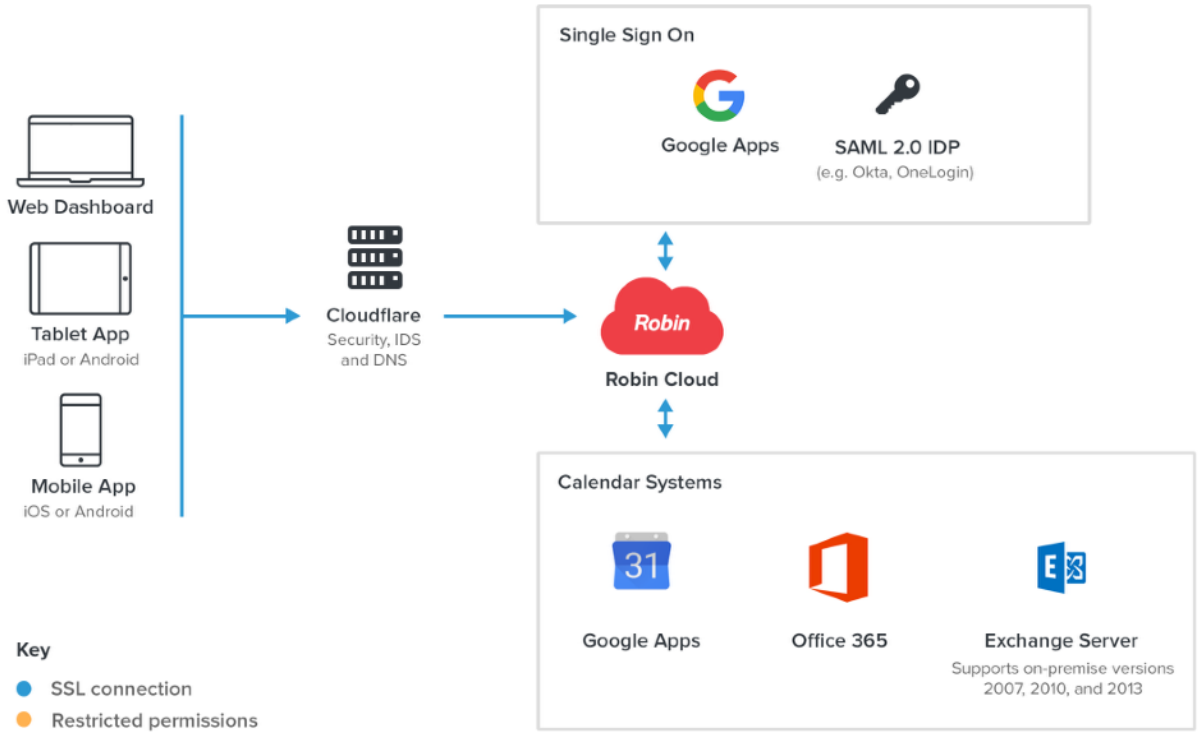
The diagrams above will give you the fastest overview of Robin's service architecture and external entities involved. Larger versions are available **on our site**.

Encryption

Customer data is encrypted in 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 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

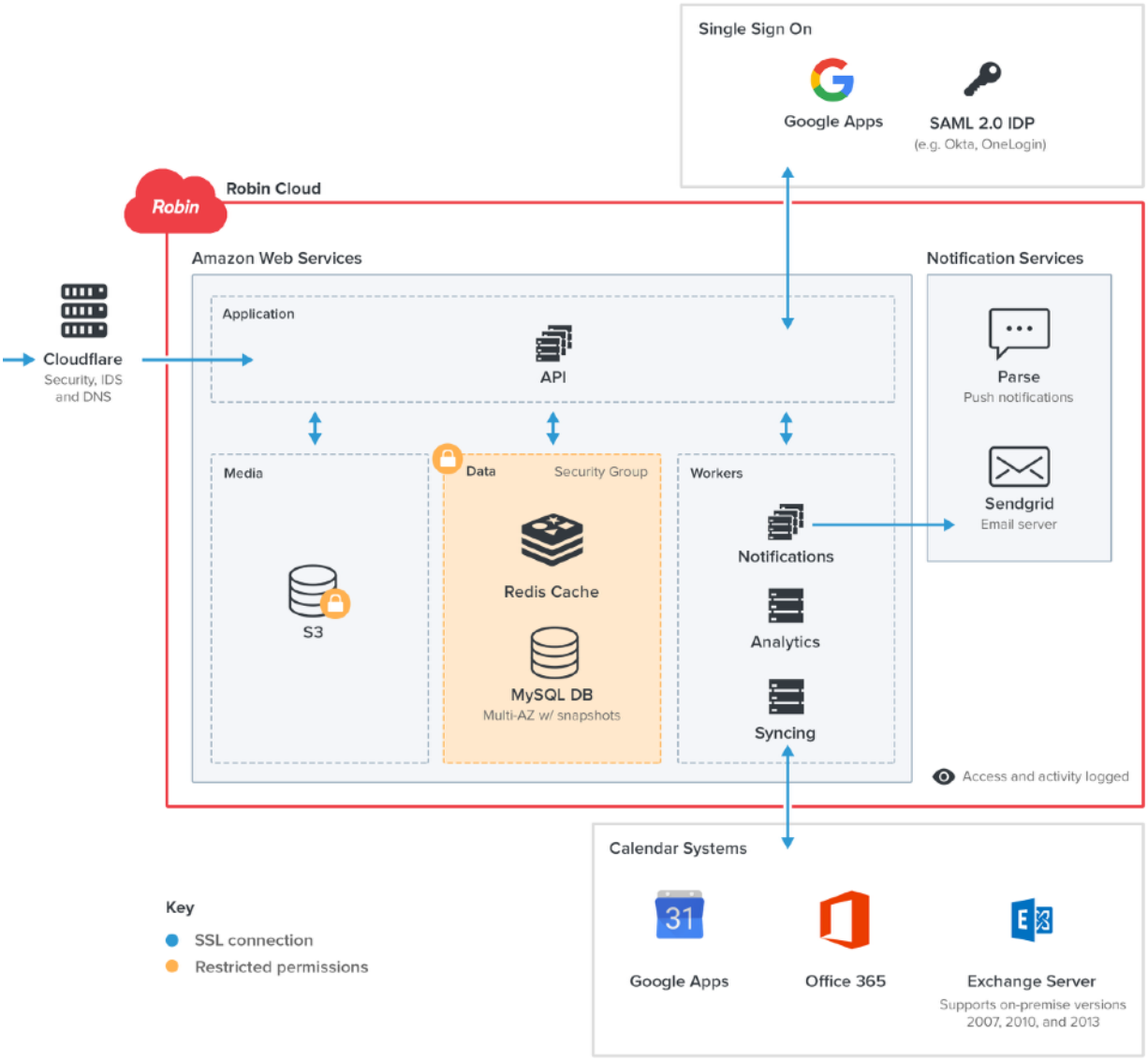
For additional verification, you can also match user agents containing `RobinAPI`, which will appear similar to `RobinAPI/123456` in the request headers

Ports

The majority of application traffic is via standard web traffic port `443`. Rooms displays also use port `28989` specifically for logging device diagnostic information used in uptime analysis.

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 range 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

All application servers are based in the US, 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 outlines on **page 8 of their security whitepaper**.

> *"AWS uses the techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual ") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process."*

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 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 & Reliability

We constantly monitor our service performance and have automatic notifications to ensure 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: **http://status.robinpowered.com**

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 **their security practices here**.

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

Application

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 for automatic de-provisioning is in development and planned for 2017 release.

Development Process

New features, performance improvements, and bugfixes 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 on test/staging environments prior to deployment on 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 proactive internal audits completed on production machines weekly.

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. Additional activity logs are available for download in our admin portal or upon request from your account manager.

System availability and status updates are also available via **status.robinpowered.com** and **updates.robinpowered.com** where you may also subscribe for 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 and require public key authentication.

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

Organizational

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. If you would like to request a copy of these policies, please contact your account manager.

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 in our data center. 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 promptly notify you 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 provide access as needed.

Appendix

How to contact us

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

You may also reach us via the mailing address below:

Attn: Security
Robin Powered Inc.
11 Farnsworth St. 2nd Floor
Boston, MA
02210

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 will also want to review the following:

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