37signals

Security Overview

Introduction

Keeping customer data safe and secure is a huge responsibility and a top priority for 37signals. We work hard to protect our customers from the latest threats. We store all our own sensitive information on the same servers our customers do. We don't want our information compromised, so we're motivated by self-preservation as well. Aligning our goals with your goals is the best way to see eye-to-eye on the need to keep everything as secure as we can.

Access control and organizational security

Personnel

All our employees and contractors (workers) sign confidentiality agreements before gaining access to our code and data. Background checks aren't performed on our workers. Everybody at 37signals is trained and made aware of security concerns and best practices for their systems. Remote access to servers is via our VPN using two factor authentication, and limited to workers who need access for their day to day work. We log all access to all accounts by IP address.

We harden all computers used by 37signals workers with an automated test suite called Shipshape. Shipshape builds on top of Bats (https://github.com/sstephenson/bats). It ensures that everyone at 37signals has a secured environment, and audits that environment daily.

For our newer apps, HEY and BC3, all employee access to data is audited by our Security team using our built-in and open-sourced tools, console1984 (https://github.com/basecamp/console1984) and audits1984 (https://github.com/basecamp/audits1984). In HEY, data is encrypted at-work (see section about

Penetration testing

We run a bounty program in HackerOne and welcome reports from security researchers. More details are available here: https://basecamp.com/about/policies/security/response.

We've also gone through security reviews and penetration tests performed by 3rd party security firms for HEY and BC3.

Dedicated teams

Our Operations team and our Security, Infrastructure and Performance (SIP) team are in charge of access/identity management, network connectivity, firewalls and log file management. These two teams' responsibilities include:

- Manage our bug bounty program in HackerOne
- Maintain and support our automated test suite for development machines
- Review all changes to the code and infrastructure to ensure they follow best practices and security guidelines (such as OWASP)
- Build and operate the Basecamp and HEY infrastructure, including logs, monitoring and authentication
- Review, test and design incident response processes
- Respond to alerts triggered by any security events
- Coordinate external audits and security and privacy certifications
- Monitor and alert on anomalous activity
- Coordinate vulnerability testing with external security researchers
- Implement and roll out app-level encryption and tools to protect customer data internally

Audits, Security Policies and Standards

We submit a self assessment (SAQ A 3.2) for PCI compliance, which is good for a year each time. A copy of our PCI compliance certificate is available upon request, after completing an NDA. 37signals LLC itself has not completed a SOC audit. We can provide a copy of the SOC reports for the data centers we use after completing an NDA.

We have an internally built system that monitors and automatically blocks suspicious activity (including vulnerability scanning, failed logins, and a host of other suspicious activity). We also have alerts in place for excessive resource use that escalates to our Ops team for manual

investigation. Our products run on a dedicated network secured with firewalls and carefully monitored.

Data protection and privacy

Our overall privacy policy is available at https://basecamp.com/about/policies/privacy. Some highlights:

Data Location

Our primary data centers are in the United States, in Chicago and Ashburn, Virginia. We also use Amazon AWS. All data is written to multiple disks instantly, backed up daily, and stored in multiple locations. Files that our customers upload are stored on servers that use modern techniques to remove bottlenecks and points of failure. Our software infrastructure is updated regularly with the latest security patches.

Encryption in-transit, at-rest and at-work

We offer encryption in-transit and at-rest for all our apps, and for our newest app, HEY, we also offer encryption at-work.

Over public networks we send data using strong encryption. We use SSL certificates issued by GeoTrust Inc, RapidSSL CA. The connection uses AES_128_CBC for encryption, with SHA2 for message authentication and ECDHE_RSA as the key exchange mechanism. You can check our currently supported ciphers here:
https://www.ssllabs.com/ssltest/analyze.html?d=basecamp.com&latest

Any files which you upload to us are stored and encrypted at rest. Our storage system uses AES-256/ SHA-256 encryption. Files are encrypted with AES-256, sliced, replicated, and geographically dispersed to separate data centers on private, end-to-end encrypted network connections. Our application databases are not encrypted at rest — the information you add to the applications is active in our databases and subject to the same protection and monitoring as the rest of our systems. All passwords are hashed and salted using BCrypt with a cost factor of 10. Our backups of your data are encrypted using GPG.

As mentioned before, in HEY, data is also encrypted at-work. At-work encryption means that our main database also deals with encrypted data while it's working. We're particularly proud of this bit, as this is not a common approach. It means that every content field in our database is encrypted with its own key, which is then encrypted with a master key. This allows us to introspect, service, and operate HEY without having programmers and administrators inadvertently exposed to private data during the course of their work. They see the metadata connecting everything, so they can resolve bugs, improve performance, and perform maintenance, but they don't see the content of your emails. We've open-sourced the work that went into this and made it part of Rails (https://github.com/rails/rails/pull/41659).

Physical Security

Our state-of-the-art servers are protected by biometric locks and round-the-clock interior and exterior surveillance monitoring. Only authorized personnel have access to the data center. 24/7/365 onsite staff provides extra protection against unauthorized entry and security breaches.

Law enforcement

37signals won't hand your data over to law enforcement unless a court order says we have to. We flat out reject requests from local and federal law enforcement when they seek data without a court order. And unless we're legally prevented from it, we'll always inform you when we receive such requests.

Data deletion

For all our apps except HEY, all your content will be inaccessible immediately upon cancellation. For HEY, you have the option of canceling your subscription and continue using your account until it expires and the account is automatically canceled. Within 30 days of cancellation, all your content in any of our apps will be permanently deleted from all servers and logs. This information can not be recovered once it has been permanently deleted.

We also keep backups stored off-site for a maximum of 30 additional days.

Therefore, after cancellation, all data will be permanently deleted from backups within 60 days.

37signals

Security Overview

Incident management and disaster recovery

We practice regular recovery drills where we test diverse disaster and failure scenarios. We perform hourly backups of all databases and files are backed up automatically after they are uploaded to Basecamp. Our backups are tested on a regular basis and are stored off-site for a maximum of 30 days. We have procedures for responding to incidents managed by our dedicated Operations and Security, Infrastructure and Performance teams. In the event of an incident, we would contact your account owner within 24 hours, and work with you throughout.

Conclusion

We've been around the block and we've seen a lot of companies come and go. Security isn't just about technology, it's about trust. Over the past 18 years we've worked hard to earn the trust of over hundreds of thousands of companies world wide. We'll continue to work hard every day to maintain that trust.

Longevity and stability is core to our mission at 37signals.

Want to know more?

Submit a support request if you have other security questions. We'll get back to you as quickly as we can.