harvest

Security whitepaper

Introduction

At Harvest, security is very important — our customers trust us and they expect their data to be secure. Safeguarding this data is a critical responsibility we have to them. All data stored on Harvest is safe, secure, and reliable. For us, it's the only way to do business.

Organizational Security

The focus of Harvest's security efforts is to prevent unauthorized access to customer data. To this end, our security and operations teams, working with peers across all our teams, take exhaustive steps to identify and mitigate risks, implement best practices, and constantly evaluate ways to improve.

Principle of Least Privilege
To minimize the risk of data exposure, Harvest adheres to the principle of least privilege. People working at Harvest are only authorized to access data that they reasonably must handle in order to fulfill their current job responsibilities.

Security Policies
Our internal systems and tools require the use of SSO with MFA, and we monitor access and usage. We rotate passwords, keys, and secrets every time someone leaves the company.

For external services, we require the usage of a password manager to generate passwords with long, secure, random strings. We periodically review that everyone has enabled 2FA in the services we use and that accounts in place in all services are correct and essential.

Internal Endpoint Security
Harvest's internal computer security policy requires all employees to comply with our standards for security. These standards require all workstations to run the latest operating system version with the latest security patches and follow updated security guidelines that are reviewed every six months.

Data Protection

Encryption
All data is encrypted in transit, and all connections use TLS 1.2/1.3. Passwords are stored hashed and salted using bcrypt with a work function of 12. Backups are encrypted using the AES-256 cipher. Attachments and other file assets are stored encrypted at rest on Amazon S3 and Google Cloud Storage.

Login Protection
Account logins are protected from brute force attacks with rate limiting. We keep an eye on external breaches to ensure that leaked credentials are not used. We have protections against distributed attacks such as password stuffing.

Secure SDLC
We maintain separate and distinct production, staging, and development environments. No Service Data is used in our development or test environments.

At Harvest, we use a continuous integration system and development process where everything is reviewed and deployed from a secure and monitored version control system. The source code repositories are scanned for security issues via our integrated static analysis tooling.

We constantly monitor security notifications around all third-party software libraries, and if identified, we immediately apply any relevant security patches as soon as they are released. Our engineers work alongside the product teams to ensure that all of Harvest's code and infrastructure is secure.

Bounty Program
Harvest currently runs our Responsible Disclosure Program via HackerOne. Our current policy is to give bounties for legitimate vulnerability reports. This approach ensures that our security is under constant review by hundreds of independent security researchers, that there is a good reason to report security issues to us, and that we are not hiding security issues from the general public.

Please see our HackerOne page for our security policy.

System Logging and Hardening

All of our servers and compute instances are monitored in order to provide a comprehensive view of the security state of corporate and application infrastructure. Harvest collects, stores, and indexes production logs for analysis. Logs are protected from modification.

New servers deployed to production are hardened by disabling unneeded and potentially insecure services and applying Harvest custom configuration settings to each server before use.

Incident Management and Business Continuity

The Harvest operations team has designed systems for resilience, and to withstand many different types of infrastructure issues or outages. Harvest revisits and tests the various components of our Business Continuity plans to ensure continued operations.

On detection and confirmation of an incident, immediate corrective action is taken to contain it. The root causes for incidents are analyzed and an appropriate solution is implemented to prevent further occurrences of the problem.

Conclusion

Security is not just about technology — it’s about trust, and the 70,000+ businesses that use Harvest need to be confident that their data is secure so that they can focus on the work which matters most to their business. We've constantly improved our security during the last 15 years and we aim to maintain that trust to keep getting better. Security is a top priority at Harvest.