548 Market St #62411
San Francisco, CA 94104-5401
contact@zapier.com

Zapier Security Whitepaper

Revised August 2024

Introduction to security at Zapier

Gaining and maintaining our customers' trust, and safeguarding customer workflows and data are the primary goals of Zapier's security initiatives. To meet these goals, we continuously monitor and improve our security, technical, and organizational measures to better protect your sensitive information.

Zapier's security team is part of our engineering organization and is run by the Head of Security. The team covers the following core functions:

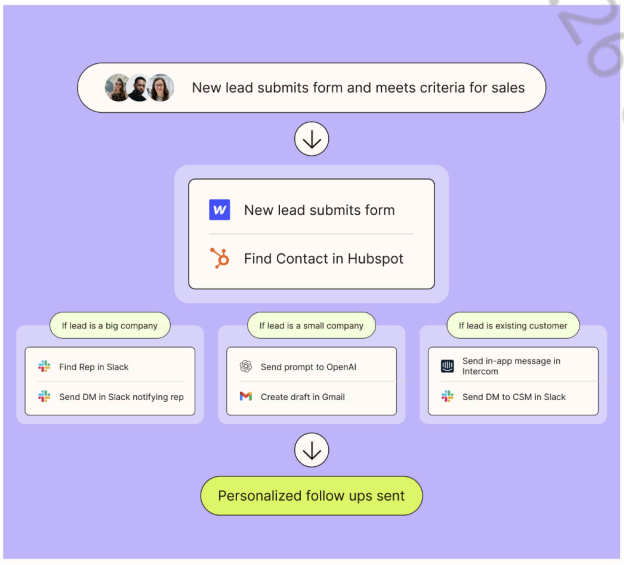
- **Application security** (secure development, security feature design, the Security Champions program, and secure development training)
- **Infrastructure security** (infrastructure security, cloud security, and strong authentication)
- **Monitoring and incident response** (cloud native and custom)
- **Vulnerability management** (vulnerability scanning and resolution)
- **Compliance and technical privacy**
- **Security awareness** (onboarding training and awareness campaigns)

The effectiveness of our security initiatives is verified through internal tools and metrics, and company objectives and key results (OKRs). We also perform external penetration testing annually, run an ongoing public bug-bounty program, and maintain SOC 2 Type 2 certification.

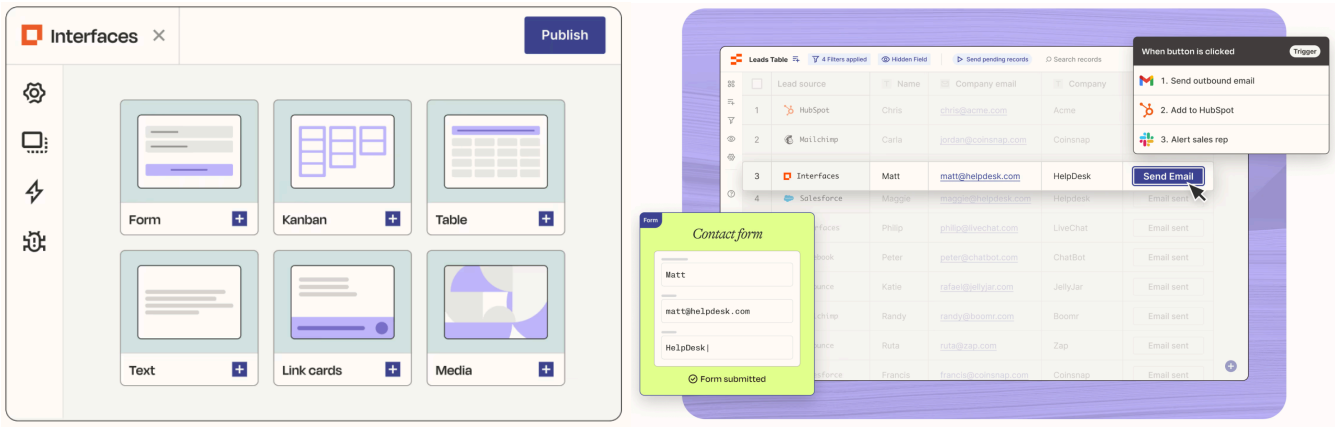
Company overview

Zapier is a cloud-based platform and online automation tool that integrates various web applications and services. Users can create Zaps, which are automated workflows consisting of a trigger and action, that connect two or more applications via their application programming interfaces (APIs). These Zaps automate repetitive tasks without needing the ability to code or rely on developers to build out the integration. Zapier Interfaces and Tables enable users to extend automation workflows by triggering Zaps from user designed no-code web pages & data tables respectively.

In providing these services to users, Zapier serves as the data processor of user personal information, responsible for safeguarding customer content that is transferred in and out of Zaps as data flows through the system, while the users are considered the data controllers.
Zapier is a global organization that is remotely operated and maintains a customer base of over 8 million users. Zapier is headquartered in San Francisco, California and was founded in 2012.



An example Zap



An example of Interfaces (left) and Tables (right)

How do we handle your data?

Zapier stores a few different types of data on your behalf. This summarizes what kind of data we store, why, and how we protect it.

Throughout this document, "User Content" will refer to any data, information, or material originated by you that you transmit through Zapier. You can read more about “User Content” in the Terms of Service.

Credentials

Credentials are the authorizations you grant to Zapier so your Zaps can access applications and services on your behalf. In most cases, we hold an OAuth token and not your username and password.

OAuth is a protocol that allows users to grant applications limited access to perform actions or access data without having to share a password. When a user grants access with OAuth, a unique access token is created that is used by the application to access the resources. OAuth 2.0 is the current version used by applications.

When a user signs in from an application that supports OAuth, Zapier asks for all the necessary permissions required to run all of the triggers and actions supported by the application.

In limited cases, we may hold credentials such as an access key or store a username and password if it's necessary to communicate with certain applications.

In all cases, credentials will be stored encrypted by AES-GCM with 256 bit-keys.

Data from your applications

Zapier stores data from applications in different ways depending on the type of data and the application it comes from.

For Zaps, the content transferred when you test a Zap is stored until you delete the Zap. Once you have deleted the Zap, the Zap Content will then be subject to other retention periods. Zap Metrics, which are statistical metadata about Zaps, are stored in your Zapier account to provide you with relevant metrics about your Zaps. These metrics are also stored in Zapier’s non-production database for internal Zapier product analytics purposes. Source: Data Retention/Deletion/Exposure disclosure

For Tables, the content contained in your Tables is stored in your Zapier account until you delete the specific content or entire table itself. Once you have deleted the specific content or entire table, then the Tables Content will also be removed from backup within 4 months. Source: Data Retention/Deletion/Exposure disclosure

For Interfaces, the content contained in submissions to your Interfaces form is stored in your Zapier account until you delete the Interface from within the product. Once you delete the Interface, the Interfaces Content will also be removed from backup within 4 months. Source: Data Retention/Deletion/Exposure disclosure

Personally identifiable information

Zapier collects personally identifiable information (PII) such as your name, email address, and any other information you give us when signing up for your account. You can refer to our Privacy Policy for more information about your PII.

Your PII is stored in encrypted databases and is encrypted while in transit.

We do not store any credit card or other financial information or claim payment card industry (PCI) compliance. All financial information you give us for payment purposes is held by our payment processor who is certified to hold such information securely.

GDPR

The General Data Protection Regulation (GDPR) is a European Union (EU) law on data protection and privacy for individuals within the European Union. GDPR aims to give control to its citizens and residents over their data and to simplify the regulatory environment across the EU. Zapier is compliant with the applicable provisions of the GDPR.

CCPA

The California Consumer Privacy Act (CCPA) is a California law on data protection and privacy for individuals within California. Zapier has been CCPA-compliant since January 1, 2020.

EU-U.S. and Swiss-U.S. Privacy Shield Frameworks

Zapier complies with the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks regarding the collection, use, and retention of personal information from European Union member countries and Switzerland.

Return and deletion of User Content

At any time, you may export or delete your data stored by Zapier by going to your data management settings (see: https://zapier.com/app/settings/data).

If there is data you wish to access that is not available in your data management settings, Zapier will make a reasonable effort to support you in the retrieval or deletion of your User Content, subject to technical feasibility.

Sensitive data

While Zapier aims to protect all User Content, regulatory and contractual limitations require us to restrict the use of our product for certain types of information.

Zapier cannot advise on how Zapier usage may or may not comply with your unique requirements to store the following types of data:

- Government-issued identification numbers and images of identification documents.
- Information related to an individual's health, including, but not limited to, Protected Health Information (PHI) identified in the U.S. Health Insurance Portability and Accountability Act (HIPAA) and related laws and regulations.
- Information related to financial accounts and payment instruments, including, but not limited to, credit card data. The only general exception to this provision extends to explicitly identified payment forms and pages that are used by Zapier to collect payment.
- Any information especially protected by applicable laws and regulations, specifically information about individuals' race, ethnicity, religious or political beliefs, organizational memberships, etc.

Tracking and analytics

Zapier continuously improves its websites by using various third-party web analytics tools which help us understand how visitors use our products, what they like and dislike, and where they may have problems. For further details, refer to our Privacy Policy. Encryption at rest and in transit

All authentication credentials for Zapier customers are encrypted with AES-GCM-256 and stored in a database that itself is encrypted at rest. Additionally, we use an internal crypto-anchoring microservice that is the only piece of our infrastructure that can decrypt the credentials. Credentials are also only ever decrypted on demand when needed to access a third-party API on behalf of a customer.

Following [National Institute of Standards and Technology (NIST)] recommendations, we store Zapier.com login credentials as one-way PBKDF2 hashes. You can read more about PBKDF2 from 1Password (see: https://support.1password.com/pbkdf2/).

All of our internal databases are encrypted at rest. We practice infrastructure as code (IaC) with mandatory code review for the creation of new resources. This serves as a control, preventing new databases from being created without encryption.

We use Transport Layer Security (TLS) 1.2 wherever possible, requiring modern cipher suites, key exchange protocols, and hashing functions for traffic to zapier.com. We received a grade of A+ on Qualys's SSL Labs server test: (see: https://www.ssllabs.com/ssltest/analyze.html?d=zapier.com).

Product security features

Zapier is built on some of the industry's most mature and secure application frameworks, and we take full advantage of the security features and best practices of that platform. Examples include, but are not limited to:

- Our platform provides intrinsic defenses against the Open Web Application Security Project (OWASP) Top 10 web application vulnerabilities.
- Our application operates under HTTPS (TLS 1.2).
- Our application provides two-factor authentication and single sign-on integration.
- Our application offers domain capture to ensure your employees join your Zapier account, domain insights to manage who can access your Enterprise account, and audit logs to review account activity.
- You can authorize a third-party app to access your Zapier account. When you do, the app can access some or all of your Zapier data. The Authorized applications page lists all third-party apps that are connected to your Zapier account.
- We use GitLab for our continuous integration (CI) tooling. Every merged PR is automatically subjected to a pipeline of rigorous tests and analysis as appropriate for the code being merged.
- We complete robust unit testing where individual units/components of Zapier are tested before release.
- Our status page provides real-time updates on our systems.

Technical security controls

Logical access control

The logical access control procedures we have in place are designed to prevent or mitigate the threats of unauthorized application access and data loss in corporate and production environments. Employees are granted minimum (or “least privilege”) access to specified Zapier systems, applications, networks, and devices, as needed. User privileges are also segregated based on functional role and environment.

Data segregation

Zapier leverages a multi-tenant architecture, logically separated at the database level, based on a user’s or organization’s account. Only authenticated parties are granted access to relevant accounts.

Data backup and availability

Zapier’s databases are backed up regularly and these backups are periodically tested.

Security testing

Zapier undergoes an external penetration test by an independent third party on an annual cadence, at minimum. We also maintain a bug bounty program.

Encryption

Zapier maintains a cryptographic standard that meets industry standards. This standard is periodically reviewed, and selected technologies and ciphers may be updated following the assessed risk and market acceptance of new standards. All connections to our public service are encrypted in transit following this standard.

Monitoring and alerting

Zapier has globally distributed site reliability engineering (SRE) and security teams on call 24/7. We take advantage of Amazon Web Services (AWS) APIs, tools, and security features to monitor the integrity of our deployed cloud resources and log access to our cloud environments. We strive to provide least-privilege access to our engineers. Zapier uses Infrastructure-as-Code.

Physical security

Zapier’s applications and customer assets are housed in the AWS cloud. Staging or testing environments with customer data are not co-located on Zapier’s physical property. Zapier employees all work remotely and we do not have an in-person office location.

Corporate security

Zapier's internal security security controls include, but are not limited to, the following tools and practices:

- Company-wide use of a VPN. Access to the VPN is gated through single sign-on (SSO) and two-factor authentication (2FA).
- Mandatory use of a password manager.
- Enforcement of SSO and 2FA, where possible, to gate access to important services.
- Regular reviews of access to important services, such as our source code repository.
- Use of an MDM to manage our corporate laptops.
- Patch management for laptops and core apps.

Application security

Zapier implements an application security program to ensure our product code is as secure as possible. In addition to finding and fixing security flaws, this helps us understand our vulnerabilities and who might want to take advantage of them. It also helps us find the best path to mitigating those risks. The main elements of the program are detailed in the following sections.

Zapier's change management practices trace development from design to production. Security staff contribute to design discussions before code is authored and review code after PRs are submitted. Our deployed software lives in both production and staging environments, and both are actively tested using interactive, dynamic application security testing tools and techniques.

Security Champions

We believe that security is everyone’s responsibility. Our Champions program helps promote this.

Security Champions embedded in product teams promote secure development practices and ensure Zapier’s security policies are followed. They receive additional training on security best practices and help integrate this knowledge into team workflows.

Some of the responsibilities of Security Champions include:

- Serving as the first point of contact for security-related questions;
- Ensuring the team is following the Security Development Lifecycle (SDLC);
- Promoting best practices in secure development; and
- Ensuring security features and tickets are prioritized appropriately.

Security Development Lifecycle

The Zapier Security Development Lifecycle (SDLC) is the set of processes and procedures we use to introduce security and privacy awareness during the software development process. The goal of the SDLC is to make security an intrinsic part of design, implementation, and testing during development. Security Champions are integral to helping teams follow the SDLC.

Code reviews

Every new piece of code—including new features and bug fixes—is subjected to a peer review before it's deployed. The work is checked for completeness, and correctness, and with an eye toward security. This ensures the new code has been properly tested, does what it's supposed to do, and does it securely before it's deployed.

Threat modeling

Zapier uses threat modeling to assess the level of risk presented in new features and fix any security issues in the development process. We also revisit previously modeled features to address any new risks based on new functionality or circumstances.

Bug bounty program

As part of our vulnerability management strategy, Zapier offers a public bug bounty program (see: https://zapier.com/engineering/bug-bounty-program/). We welcome most efforts by security researchers to identify vulnerabilities in the Zapier application, platform, and infrastructure. We conduct systematic reviews to find the root cause and eradicate issues across our whole codebase. In return, we offer compensation for verifiable items that we take action on.

Vendor management

Zapier's vendor management practices include mandatory review & periodic re-review of vendors that process customer data (see: https://zapier.com/legal/subprocessors). At a minimum, Zapier's IT, Security, Legal, and Finance review vendors to ensure Zapier's standard of security & legal obligations are met.

Compliance

Zapier pursues third-party compliance to build trust with customers and partners by ensuring that its practices meet rigorous standards for security, availability, privacy, and confidentiality.

Zapier is audited, no less than annually, against AICPA's SOC2 Type II and SOC3. These reports are made available to partners & customers.