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

Zapier Security Practices

Revised May 2018

Zapier Security Practices

At Zapier, keeping customer data safe is a top priority. That's why we run a best-in-class security practice, informed by internal research, third-party resources, public threat intelligence, and best practices from peer startups. This document offers a short description of some of the components of that program.

Application Security

Zapier operates a mature application security program that adds security controls at the design phase, during the development phase, and after deployment.

We run a modern pull-request-based development process for traceability, tying code changes back to design discussions. 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.

Network and Cloud Monitoring

Zapier continually monitors its networks for indicators of attack or out-of-process changes. Our networks are scanned from both internal and external vantage points to detect unintentional exposure.

We're deployed in AWS. We take advantage of AWS APIs to monitor the integrity of our deployed cloud resources, including by snapshotting and comparing those resources over time. We take full advantage of AWS security features to monitor and log access to our cloud environments, and strive to provide least-privilege access to our engineers.

Wherever possible, our infrastructure is managed using configuration management systems. That configuration is managed in source control using the same high standard of a pull-request based process with mandatory code review. This gives us an audit trail of changes combined with continuous oversight.

Audit and Assessment

Zapier has had multiple 3rd party security assessments performed, covering both our application and network footprints. We continue to have periodic, point-in-time assessments conducted, augmenting our internal application security program.

In addition, Zapier runs a public bug bounty, which we triage internally. On the occasions where legitimate issues are observed by bounty researchers, we conduct systematic reviews to ascertain root cause and eradicate issues across our whole codebase. You can find the details of our bug bounty here: https://zapier.com/engineering/bug-bounty-program/

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. In doing so, we improve our internal security efforts by inheriting the research and best practices of other organizations.

Our platform provides intrinsic defenses against common OWASP-style web application vulnerabilities, including on-by-default XSS filtering, a comprehensive anti-CSRF system, and ORM-level defenses against SQL injection.

Our applications operate exclusively under HTTPS/TLS. We use a carefully tuned TLS configuration which is graded A+ by Qualys SSL Labs, including TLS 1.2 and forward secrecy, with 64 bit ciphers disabled.

Our applications provide two factor authentication and single sign-on integration.

Corporate Security

Zapier's has mature internal security security controls that are subject to audit. These controls include, but are not limited to:

- VPN, access to which is gated via SSO.
- Mandatory password manager. Audits include password strength, password reuse, access audits.
- Enforcement of SSO and 2FA where possible to gate access to important services.

- Applications authorized to access GSuite services via OAuth.
- Access audits to important services, such as source code.

Enforcement of strong two-factor authentication wherever possible.

Physical Security

Zapier's applications and customer assets are housed in the AWS cloud. No staging or testing environments with customer data are co-located on Zapier's own physical property. Our corporate IT footprint is designed to ensure that our information assets inherit the full measure of security provided by AWS.

AWS provides one of the most secure data center environments in the world, where security informs everything from day-to-day access control to site selection for new data centers.