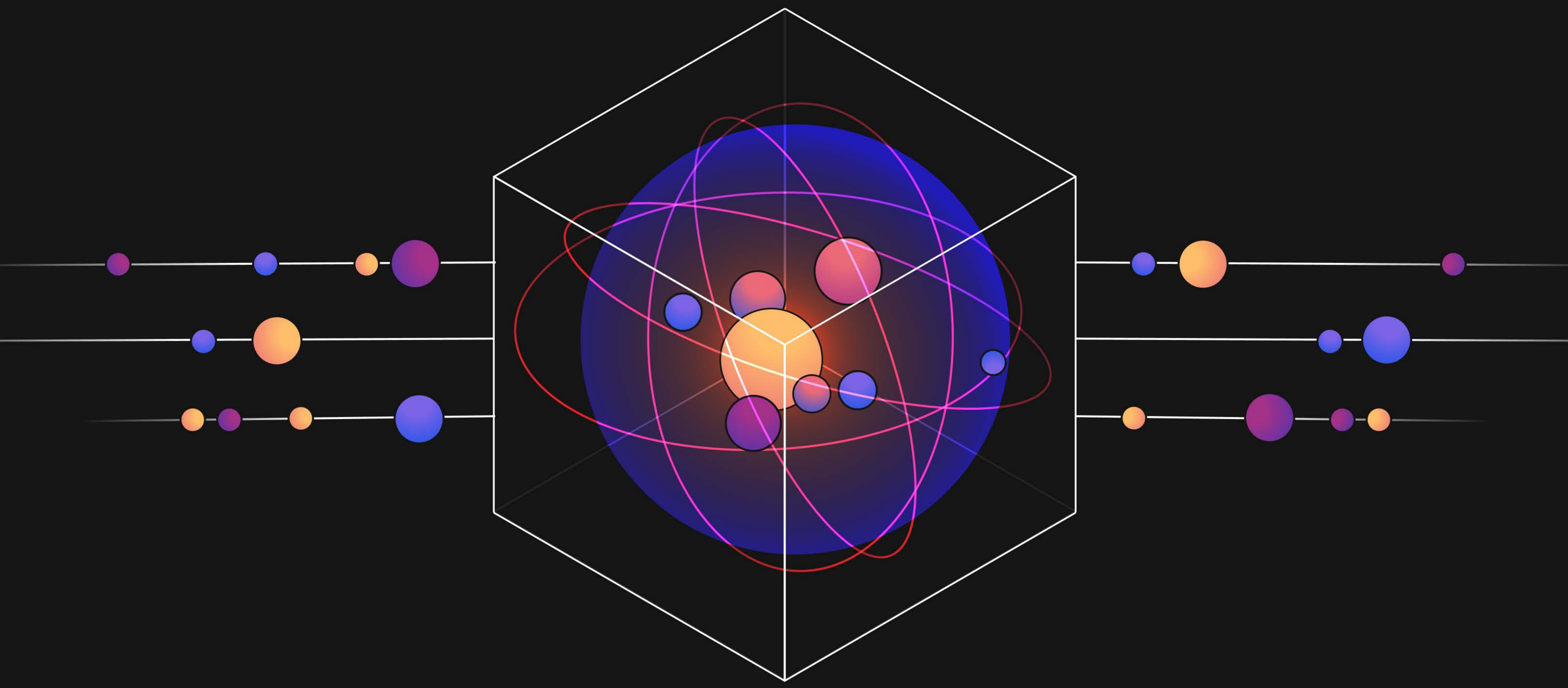
Statype

Security Whitepaper

HOW WE GO ABOVE & BEYOND YOUR SECURITY EXPECTATIONS



JULY 2023

WHITEPAPER

00 Table of Contents

01 Introduction

Statype asks a lot from our customers: we ingest sensitive financial, performance, and customer information to generate deep insights. Our customers trust us to get this right because security is a core tenant of everything we build, and we prioritize getting security right.

Startups have a bad reputation for being careless when it comes to security. We have taken the opposite approach and believe that by being security minded early on, we'll build a better product and have happier customers.

We follow industry best practices, and set the bar for who you should trust with your data.

02 Statype's security culture

Customer Trust as a core value

Our values enrich and enable. They're not everything that is important to us, they are the things most important to us that make us unique from everyone else. They are the deal-breakers, the non-negotiables. We rely on them to get hiring right, and to make the right prioritization decisions for the work we do and the business decisions we make.

"Customer Trust" has been one of our 4 core values from the beginning. From hiring, to system architecture, to how we communicate, we think about how something impacts security and our customer's data before acting.

We follow industry best practices, and set the standard for getting this right. Our customers use us as the standard to hold their other vendors up to. If we identify a more secure way to do something, we spend the time to validate and make it happen.

People

The people make the culture, and we think about security when hiring. Our founders have worked as co-founders and leads at tech companies like DigitalOcean and Dropbox where security is paramount, as well as companies in the financial services space where regulatory requirements around security are higher than anywhere else.

We look for this kind of experience when hiring, and almost everyone on the team has a background with some combination of cloud platform, financial services, and confidential data work.

Our Founders

Moisey Uretsky

CEO

Joonas Bergius

CTO

Marie Sokolovsky

CHIEF OF STAFF

David Worth

VP OF ENGINEERING

03 Operational Security

Vulnerability Management

All software is built on top of other pieces of software, and even if we get every line of code right we're still exposed to vulnerabilities in the tools on which we are built. To minimize risks, we rely on automation and tooling to identify, notify, and correct vulnerabilities in our systems. Some of the practices we follow include:

- Using **Github's Supply-Chain security tooling including dependabot**.
  Every code repository in our organization is continually scanned and kept up to date.
- Using **Amazon's automated vulnerability management tooling including Amazon Inspector.**
  Every piece of code interacting with our customer's data is packaged as a container and continually scanned.
- Using **Amazon's cloud security posture management service Security Hub**.
  Every potential issue across our entire software and infrastructure stack is collected, aggregated, reported on, and alarmed.

Malware prevention

While our infrastructure and customer data is in the cloud, our team uses computers to get their work done. Every device is managed by our MDM provider **JumpCloud**, and we rely on their agent and endpoint protection to ensure devices are configured correctly and free of malware.

Monitoring and Alerting

Information about changes to our application and things happening in production environments all stream into a "heartbeat" Slack channel for auditing. All logs and monitoring data about our environments are streamed to an append-only environment with read-only audit access. Exceptions are captured using **Sentry**, and anything requiring action is routed to an "alerts" Slack channel for immediate all-hands-on-deck response.

Change Management

Any software or infrastructure change goes through our deployment pipeline.
Some of the controls here include:

- Every change goes through a Github Pull Request as a set of checks and an audit trail.
- Every change requires approval from a specific set of approvers.
- Every change is scanned by security automation tooling including **tfsec** , **brakeman**, linters, and others.
- Every artifact is packaged as a container and pushed by automation to an access controlled container repository which performs further scanning.
- Customer environments "pull" artifacts from this repository. Engineers cannot manually "push" any changes into any environments.
- Infrastructure changes are all made using Terraform, which is also packaged as a container and "pulled" into customers' environments. All infrastructure changes are audited using **AWS CloudTrail** , and alarms are triggered for any changes with potential security impacts.
- Any actions that must bypass any of these steps have dedicated role accounts identified as "break glass" accounts, which create audit logs and trigger alarms whenever they are used.

04 Technology with security at its core

Single Tenant Architecture

Statype operates a Single Tenant architecture, each Statype customer exists in a tenant separate from internal Statype systems and all other Statype customers.

Specifically, each tenant includes:

- **A dedicated AWS account**
- **Access controls** (no users, no passwords, no api keys, no access except through a very specific need-to-access path using role assumption and SSO with MFA and adaptive authentication)
- **Network controls** (ingress and egress are limited to specific paths created by our engineers that are required for our applications to function, and documented as part of architecture designs.)
- **Auditing/alerting**
- **Dedicated encryption keys** stored in **Amazon KMS** to encrypt all data, logs, and systems.

Environments pull what they need to run, instead of having things pushed into them, so nobody can "push" any code, data, or changes into an environment.

It is not possible to access a customer environment without requiring both peer-reviewed infrastructure changes applied with audited automation, and having pre-approved group membership with an audit trail. Such actions trigger an alarm which goes to the entire engineering team.

Securing Data

There are still people out there not using encryption. We are not one of them. All traffic is encrypted in transit using SSL using either Elliptic Curve or RSA encryption with at least 2048 bits. All data at rest is encrypted using at least AES-256-GCM, with dedicated keys for each type of data in each environment, stored in **AWS KMS**.

In the rare cases where a customer approves us to access their data, the only way to access it is via a multi-layer tunnel using multiple access controls and encryption components.

Following Industry Standards and Best Practices

There are a huge number of "best practices" out there, from reputable and less-than-reputable sources. We really like what AWS has put together with their "Well Architected" framework, and we attempt to follow it in its entirety, specifically the **Security Pillar**.

Some bits that we really like:

- **Dedicated AWS accounts** for each type of workload, including each customer
- **Read-only containers** for execution environments
- **All Secrets in AWS Secrets Manager** with KMS managed keys
- **Logs/audit data shipped to a separate environment** with append-only access for automation, and read-only access for dedicated admin roles.
- **Prescriptive guidance** for access and network configuration and controls.

05 Data usage

Our philosophy

Customer data belongs to our customers. It is more important than our company data, and it's unacceptable to leak it, or otherwise expose it to anyone.

Statype engineers should not need customer data to do their jobs. Any time this is needed, it's up to us to figure out a way to do it in a different way. We rely on **Tonic** to generate synthetic data sets for day-to-day engineering work. We slow down to build tooling to keep us from needing "real" data.

Customers may want to share their data with Statype Support for specific, time-bound, situations. This should be done in an auditable way, with only the level of access required to perform a specific task.

06 Data access and restrictions

Administrative access

Administrative access is an exceptional case at Statype. There are no "day-to-day" pieces of work that rely on Administrative access. Every use of administrative access at Statype is through role assumption, using accounts protected by hardware security tokens and SSO with adaptive authentication; and every administrative action creates auditable log entries and triggers alarms.

For customer administrators

Each Statype customer has an administrator role within their Statype tenant, and they control who has access to this role using group membership within their own SSO Identity Provider. Through configuration in their SSO IdentityProvider, they control who within their organization can access Statype as a user, or as an administrator.

Third-party suppliers

Statype uses well-vetted, industry standard, industry leading providers for all tooling that we use. Every provider brings a handful of certifications and compliance documentation, and we'll only use vendors that hold up to our high security bar. Currently, we rely on AWS, Fivetran, and Microsoft/Github.

07 Regulatory compliance

SOCII compliance

Several people on the team have moved organizations through the SOCII process in the past. We've achieved SOCII Type 1 as of June 2023, and expect to achieve SOCII type 2 in late 2023 or early 2024.

Documentation is available on request.

08 Penetration Testing

Statype conducts annual penetration testing of the Statype platform using 3rd party testers. Testing is “tier 2” and authenticated including users with admin permissions. Our most recent test was conducted by Cacilian[https://www.cacilian.com/] in June 2023, and after several small changes, we’ve received a clean bill of health with no open known vulnerabilities.

Documentation is available on request.

09 Conclusion

Customer Trust **is our core value** at Statype.

Statype takes security seriously, and it shows in the design of our systems and the way we approach our business. We are continuously expanding our portfolio of Security & Compliance Reports as our customers request them. Please contact Statype for information on reports or to find out if a particular certification will soon be available.

If you have questions, contact us at **security@statype.com**.

Statype

Statype is working on a new approach to business intelligence.

Statype replaces your entire data stack with our Multipass software to ingest all of your data and automatically generate insights and analysis without ever having to write a single line of SQL. Just point us to your data and we will take care of the rest, configuration over convention.

Learn more at **statype.com/learn** .