DRATA

Security as a core value

At Drata, we're here to help companies earn and keep the trust of their users, customers, partners, and prospects. We believe the best way to earn trust is by first proving that you deserve it. That's why we take a security-first approach to everything we do. From building our infrastructure as code to monitoring our environment with anomaly detection and automated remediation, security is a core value that drives our business forward.

Here's how we walk the walk when it comes to our own security program:

Application

- **Web Application Firewall** with automatic updates to block against the latest threats
- **DDoS Protection** on two levels - application level DDoS protection from our CDN provider and network level DDoS protection from our cloud provider
- **DNSSEC** used for Drata's domains to block against dns hijacking attacks
- **Encryption** at rest and in transit. Drata enforces TLS 1.2 minimum for data in transit and enforces encryption at rest for all instances and database

Infrastructure

- **Amazon Web Services (AWS)** as infrastructure backbone; AWS Fargate limits our footprint and enables strong security posture
- **Spoofing Protection** enabled in our cloud provider, preventing adversaries from spoofing traffic or arp addresses
- **Infrastructure As Code** deployed using Terraform, allowing peer review infrastructure changes, vulnerability scanning, and quick recovery for failover
- **Anomaly Detection** supported by GuardDuty as well as third party security services from trusted vendors

Code

- **Static Code Analysis** check must be passed before code can be merged to main
- **Credential Checking** to prevent any chance of an accidental code merge
- **Content Security Policies** deployed across our application to mitigate certain types of attacks
- **Peer Reviewed Merges** conducted by a Senior Engineer before being pushed to main
- **Third Party Library Scanning** solution scans all libraries in real time to identify and block potential vulnerabilities before production

Endpoint

- **Mobile Device Management** ensures all devices centrally managed with policies around security, patching, and encryption enforced
- **Endpoint Detection Response** to see malicious activity and chain of events that lead up to it
- **Advanced Persistent Threat Detection** solution that has ATP protections and 24/7 managed threat hunting capabilities
- **Advanced DNS Filtering** on endpoints to filter malicious requests that could harm employees (or our company)

General

- **Third Party Penetration Testing** completed annually and in between major feature releases
- **Annual Security Training** provided by a leading security training company to cover 13 different major topics with our employees
- **Phishing Testing** sent monthly with all staff using realistic email communications

Privilege

Drata makes every effort to grant all of our integrations the least privilege available in order to collect the evidence we need to meet your security and compliance needs. Most of the time we can do this with a read-only credential with limited scope. As we collect data, we store it in an encrypted RDS instance in your own private database in a US region.

Compliance

Along with helping our customers be compliant, Drata also meets a number of regulatory, compliance and privacy frameworks today. We are currently SOC 2 Type II, GDPR, and CCPA compliant. We have also filled out a CSA CAIQ located here.