Vanta

Vanta Security and Privacy Brief

July 1, 2022

Letter from the CEO

Our first customers were friends who had started companies, and we still spend a lot of time with startups. There's a myth that startups don't care about security, but that's not true. Our customers, from the smallest startups to the largest enterprises, try to prioritize security but are often stymied by legacy tools, opaque processes, and an industry that under invests in bringing outsiders along.

Vanta takes a different approach. We build tools that guide motivated founders, leaders, and engineers toward a pragmatic balance of business needs and security best practices. We're proud of the protection we offer our customers when they trust Vanta, and we hope others in the industry follow our lead.

Vanta's customers rely on us to get them secure and then prove that security. As part of doing so, we've hired a team of security leaders with dozens of years of experience, built a culture that permeates every part of the business, and made security a competitive edge. We understand that our leadership position is built on trust, and we work hard to ensure that we are both trusted and trustworthy.

I'm grateful to help thousands of companies along this journey every day.

Christina Cacioppo
CEO & Founder

Introduction

Vanta was founded in 2016, in the wake of several high-profile data breaches that shook our collective faith in internet businesses. Online security was only becoming more important, but we knew firsthand how hard it could be for fast-growing companies to invest the time and resources it takes to build a solid security foundation.

We started by automating security monitoring for compliance certifications like SOC 2, HIPAA, and ISO 27001. But that's just the beginning. Vanta's vision is to restore trust in internet businesses by enabling companies to improve and prove their security and compliance posture to their customers, prospects, and partners.

Security is at the heart of what we do. Helping our customers improve their security and compliance posture starts with our own. The mission of our Security and Privacy program captures this well: "Ensure that Vanta is a trusted and trustworthy steward of sensitive data." All of our customer data is sensitive data.

This document is intended to give a more detailed overview of the practices and tools we use to live up to that mission.

Governance

As you might imagine, Vanta uses Vanta quite a bit. Our Security and Legal teams work closely on the Security and Privacy program. Together, we establish policies and controls, monitor compliance with those controls, and prove our compliance to third-party auditors. Most of this is continuously monitored in Vanta, so we can trust that our governance framework is being followed rigorously.

Fundamentally, our policies are based around a few key principles:

1. Access should be limited to only those with a legitimate business need and granted based on the principle of least privilege.
2. Security controls should be implemented and layered according to the principle of defense-in-depth.
3. Security controls should be applied consistently across all areas of the enterprise.
4. The implementation of controls should be iterative, continuously maturing across the dimensions of improved effectiveness, increased auditability, and decreased friction.

Vanta maintains a SOC 2 Type II attestation and an ISO 27001 compliance certification. For more information on Vanta's infrastructure, organizational, procedural, and product security, we provide documentation at trust.vanta.com.

Product overview

Vanta integrates with the key services your organization uses, and uses data about those services to monitor your security and compliance posture in a continuous way.

Vanta Web Application

When you use Vanta, you'll typically be interacting with our web application at app.vanta.com. Our dashboard is where you'll keep track of your controls, see their current status, provide custom evidence, and administer your program overall. We have many features, including vulnerability management, vendor management, trust packets, and asset inventory that help you achieve your compliance and security goals.

This application is built using TypeScript, GraphQL, and React. We don't store passwords, and we don't charge more for SSO. All authentication to Vanta's application is done via SSO or one-time email links.

Vanta Agent

Many of our customers choose to use the Vanta Agent to assist in monitoring employee endpoints for compliance with their security policies. If you choose to use this product, your employees will be prompted to install the agent on their workstations, and the agents will report back to Vanta regarding certain settings on their machine such as disk encryption and screen lock configurations.

The Vanta Agent is based on Osquery, with a small custom wrapper written in Go. We use an industry-standard framework called The Update Framework to deliver secure updates. You can monitor the deployment and results from the Vanta Agent using the Vanta web application.

Resource Fetcher

When you connect one of your systems to Vanta, such as your cloud provider or human resources system, Vanta's Resource Fetcher is responsible for collecting the relevant metadata.

Vanta's backend services, such as Resource Fetcher, are implemented in AWS via Elastic Container Service. Our integrations use the minimal set of permissions, usually read-only if supported by the service. You have full control over which connections are active at a given point in time.

Data protection

Data at rest

Vanta uses MongoDB, hosted by MongoDB Atlas, as our primary datastore. We have two secondary datastores hosted in AWS: MySQL RDS, Redis and Redshift. All datastores with customer data, in addition to S3 buckets, are encrypted at rest. This invariant is monitored via Vanta itself.

In addition, sensitive collections and tables are encrypted at the "row-level." This means the data is encrypted even before it hits the database, so that neither physical access, nor logical access to the database is enough to access the most sensitive information stored there. Access to these encryption keys is strictly limited.

Data in transit

Vanta uses TLS 1.2 or higher everywhere data is transmitted over potentially insecure networks. We also use features such as HSTS (HTTP Strict Transport Security) to maximize the security of our data in transit.

Server TLS keys and certificates are managed by AWS and deployed via Application Load Balancers.

User authentication

Vanta's product does not support password based authentication. All user authentication is enforced via SSO integrations, or email-based "magic links."

Secrets management

Encryption keys are managed via AWS Key Management System (KMS). KMS stores key material in Hardware Security Modules (HSMs), which prevents direct access by any humans, including employees of Amazon and Vanta. The keys stored in HSMs are used for encryption and decryption via Amazon's KMS APIs.

Application secrets are stored securely via AWS Secrets Manager and access to these values is strictly limited.

Product security

Penetration testing

Vanta engages with one of the best penetration testing consulting firms in the industry at least annually. Our current preferred penetration testing firm is Doyensec, one of the leading experts in GraphQL security.

All areas of the Vanta product are in-scope for these assessments, and source code is fully available to the testers in order to maximize the effectiveness and coverage.

We make summary penetration test reports available under NDA. Please feel free to request our most recent report at trust.vanta.com.

Vulnerability management

Vanta uses Vanta to monitor our vulnerability management program against our SLA commitments. We regularly review the vulnerabilities shown in Vanta’s product, which are sourced primarily from AWS Inspector.

Vulnerabilities are raised to Vanta through multiple sources including AWS Inspector, ongoing static and dynamic analysis, penetration testing, and our responsible disclosure page. Once raised, these findings are systematically tracked through the stages of our vulnerability management program in Vanta's engineering task tracking system.

We use a set of industry standard stages in connection with vulnerability management:

- ↓ Reported
- ↓ Validation
- ↓ Remediation
- ↓ Forensics
- ↓ Retrospective
- ↓ (Rejected, Fixed, or Accepted)

The Security team is responsible for triaging, validating, assessing risk, and prioritizing vulnerabilities. Engineering teams are responsible for scheduling work to fix the vulnerabilities assigned to their team. Engineering leadership regularly reviews vulnerabilities approaching SLA with each engineering team as part of their standard key performance indicators (KPIs).

We also have monthly engineering security meetings with all engineers where we demonstrate any interesting or noteworthy vulnerabilities, or “near misses” (i.e. vulnerabilities which were not exploitable, but given a lack of defense-in-depth could have been exploitable) for educational purposes.

Static analysis

Vanta uses GitHub Advanced Security for static analysis of our application code.

There are three primary products bundled with GitHub Advanced Security:

1. CodeQL, which looks for common vulnerabilities and mistakes in pull requests before they are merged.
2. Dependabot, which provides information about known vulnerabilities in NPM packages.
3. Secret Scanner, which looks for known patterns in secrets (e.g. AWS API keys) and ensures that they are not committed to the codebase.

4. Linters, in particular we use ESLint and Checkov to enforce best practices and catch security issues early in our software development lifecycle.

5. Socket, which we use to augment our supply chain security.

We are always exploring new tools to add to our static analysis stack and give engineers additional context during the development process.

Data privacy

Vanta treats data privacy as a first class priority. Our Legal and Security teams collaborate on the Security and Privacy program to ensure that all company controls and policies take privacy best practices and regulations into account.

We strive to be trustworthy stewards of all sensitive data.

Privacy Shield

Vanta maintains an active Privacy Shield membership which can be reviewed here.

- Vanta's Privacy Policy can be viewed on our website: https://www.vanta.com/privacy
- Our list of subprocessors is available here: https://www.vanta.com/privacy/subprocessors
- Our DPA can be reviewed here: https://www.vanta.axdraft.com/

Regulatory compliance

Vanta aligns its privacy practices with GDPR and CCPA. We are continuously evaluating updates to these regulatory frameworks and emerging frameworks to determine necessary changes to our program.

All additional resources can be found at trust.vanta.com.

About the author

Rob leads Vanta's internal security program. He has spent almost 8 years in the security industry, including time as a penetration tester, an early hire in Robin Hood's security team, and a Y Combinator backed founder. Rob enjoys camping with his wife and two dogs, cooking, and drinking good bourbon.

Rob Picard

Internal Security Lead

Vanta

Vanta is the easy way to get and stay compliant. Thousands of fast-growing companies depend on Vanta to automate their security monitoring and get ready for security audits in weeks, not months. Simply connect your tools to Vanta, fix the gaps on your dashboard, and then work with a Vanta-trained auditor to complete your audit.

Interested in learning more about Vanta?

Request a demo from our website: https://www.vanta.com/