SOC 2 Gap Assessment from Vanta

FOR SHUTTLEROCK

The American Institute of Certified Public Accountants (AICPA) defined the SOC (System and Organization Controls) reporting framework to help businesses manage risks. Their SOC 2 standard defines criteria for managing customer data based on five trust service principles: security, availability, processing integrity, confidentiality, and privacy.

Vanta performed a gap analysis of Shuttlerock's security and IT infrastructure in preparation for a SOC 2 audit. Vanta's SOC 2 analysis identified gaps in Shuttlerock's infrastructure and provided steps to correct them.

In this report, Vanta:

- Tests a complete set of security and infrastructure controls that may appear in a SOC 2 audit
- Identifies gaps and vulnerabilities in infrastructure and processes

Intended use

This gap assessment can be used by:

- Shuttlerock to identify issues critical for remediation
- Shuttlerock's customers to understand the company's progress toward SOC 2 compliance

Continuous gap assessment approach: continuous monitoring

Vanta continuously monitors the company's policies, procedures, and IT infrastructure to ensure the company adheres to AICPA's Trust Service Principles of security, availability, and confidentiality.

To do this, Vanta connects directly to the company's infrastructure accounts, version control tools, task trackers, endpoints, hosts, HR tools, and internal policies. Vanta then continuously monitors these resources to determine if Shuttlerock meets the SOC 2 standard.

In compiling this gap assessment, Vanta took into account Shuttlerock's unique requirements and technical environment, including business model, products and services, and interactions with customer data.

CC 1.0

Control Environment

CC 1.1

4 CONTROLS

Code of Conduct acknowledged by contractors

✓ COMPLETE

The company requires contractor agreements to include a code of conduct or reference to the company code of conduct.

1 DOCUMENT

Contractor agreement ✓

Confidentiality Agreement acknowledged by contractors

✓ COMPLETE

The company requires contractors to sign a confidentiality agreement at the time of engagement.

1 DOCUMENT

Contractor agreement ✓

Confidentiality Agreement acknowledged by employees

✓ COMPLETE

The company requires employees to sign a confidentiality agreement during onboarding.

2 DOCUMENTS

Employee agreement ✓

Signed confidentiality agreement ✓

Employee background checks performed

✓ COMPLETE

The company performs background checks on new employees.

1 DOCUMENT

Completed employee background checks ✓

CC 1.2

4 CONTROLS

Board charter documented

✓ COMPLETE

The company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.

1 DOCUMENT

Board of directors charter ✓

Board expertise developed

✓ COMPLETE

The company's board members have sufficient expertise to oversee management's ability to design, implement and operate information security controls. The board engages third-party information security experts and consultants as needed.

2 DOCUMENTS

Board of directors CVs ✓

Board of directors charter ✓

Board meetings conducted

✓ COMPLETE

The company's board of directors meets at least annually and maintains formal meeting minutes. The board includes directors that are independent of the company.

1 DOCUMENT

Board of directors meeting minutes and agenda ✓

Board oversight briefings conducted

✓ COMPLETE

The company's board of directors or a relevant subcommittee is briefed by senior management at least annually on the state of the company's cybersecurity and privacy risk. The board provides feedback and direction to management as needed.

1 DOCUMENT

Board of directors meeting minutes and agenda ✓

CC 1.3

3 CONTROLS

Board charter documented

✓ COMPLETE

The company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.

1 DOCUMENT

Board of directors charter ✓

Organization structure documented

✓ COMPLETE

The company maintains an organizational chart that describes the organizational structure and reporting lines.

1 DOCUMENT

Company organization chart ✓

Roles and responsibilities specified

✓ COMPLETE

Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.

1 DOCUMENT

Job descriptions for key security roles ✓

CC 1.4

3 CONTROLS

Employee background checks performed

✓ COMPLETE

The company performs background checks on new employees.

1 DOCUMENT

Completed employee background checks ✓

Roles and responsibilities specified

✓ COMPLETE

Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.

1 DOCUMENT

Job descriptions for key security roles ✓

Security awareness training implemented

✓ COMPLETE

The company requires employees to complete security awareness training within thirty days of hire and at least annually thereafter.

2 TESTS

Security awareness training selected: Verifies that a security awareness training program has been selected within Vanta. ✓

General security awareness training records tracked: Verifies that all relevant employees have uploaded documentation indicating that they have completed general security training. ✓

1 DOCUMENT

Security awareness training completion ✓

CC 1.5

1 CONTROL

Roles and responsibilities specified

✓ COMPLETE

Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.

1 DOCUMENT

Job descriptions for key security roles ✓

CC 2.0

Communication and Information

CC 2.1

3 CONTROLS

Control self-assessments conducted

COMPLETE

The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings. If the company has committed to an SLA for a finding, the corrective action is completed within that SLA.

1 TEST

Company uses Vanta for continuous security monitoring: Automatically passes.

Log management utilized

COMPLETE

The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.

7 TESTS

VPC Flow Logs enabled: Verifies that all AWS VPCs have flow logs enabled.

Heroku logs archived for 365 days: Verifies that all Heroku apps are using a plugin that stores logs for 365 days, or are using a custom log drain.

CloudTrail enabled: Verifies that all linked AWS accounts have CloudTrail enabled.

User activity and API use is tracked (Heroku): This feature is built into Heroku.

Cloud infrastructure linked to Vanta: Verifies that AWS, GCP, Heroku, Azure, or DigitalOcean is linked to Vanta.

Only authorized users can access logging buckets: Verifies that no AWS S3 logging buckets grant access to the built-in AWS groups AllUsers or AuthenticatedUsers

S3 server access logs enabled: Verifies there is at least one AWS S3 bucket acting as a destination for server access logging or CloudTrail data event logging. **Vanta Scope consideration:** make sure that either the S3 bucket acting as destination for server access logging or the CloudTrail data event logging is [scoped](https://help.vanta.com/hc/en-us/articles/360062025631-Frequently-Asked-Questions-How-do-I-Mark-Resources-out-of-Scope-) in Vanta otherwise this test will fail.

Vulnerabilities scanned and remediated

✓ COMPLETE

Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.

6 TESTS

Employee computers monitored with the Vanta Agent: Verifies that all employees required to install the Vanta Agent have installed the agent on their workstations. ✓

Critical vulnerabilities identified in packages are addressed (AWS Inspector): Verifies that all critical severity vulnerabilities detected by AWS Inspector scanning are resolved. ✓

High vulnerabilities identified in packages are addressed (AWS Inspector): Verifies that all high severity vulnerabilities detected by AWS Inspector scanning are resolved. ✓

Low vulnerabilities identified in packages are addressed (AWS Inspector): Verifies that all low severity vulnerabilities detected by AWS Inspector scanning are resolved. ✓

Medium vulnerabilities identified in packages are addressed (AWS Inspector): Verifies that all medium severity vulnerabilities detected by AWS Inspector scanning are resolved. ✓

Records of security issues being tracked: Verifies that at least one task in the linked task tracker is labeled with a `security` tag. ✓

1 DOCUMENT

Sample of remediated vulnerabilities ✓

CC 2.2

5 CONTROLS

Roles and responsibilities specified

✓ COMPLETE

Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.

1 DOCUMENT

Job descriptions for key security roles ✓

Security awareness training implemented

✓ COMPLETE

The company requires employees to complete security awareness training within thirty days of hire and at least annually thereafter.

2 TESTS

Security awareness training selected: Verifies that a security awareness training program has been selected within Vanta. ✓

General security awareness training records tracked: Verifies that all relevant employees have uploaded documentation indicating that they have completed general security training. ✓

1 DOCUMENT

Security awareness training completion ✓

Service description communicated

✓ COMPLETE

The company provides a description of its products and services to internal and external users.

2 DOCUMENTS

Network diagram ✓

Product documentation site ✓

System changes communicated

✓ COMPLETE

The company communicates system changes to authorized internal users.

1 DOCUMENT

Internal communication for system updates ✓

Whistleblower policy established

✓ COMPLETE

The company has established a formalized whistleblower policy, and an anonymous communication channel is in place for users to report potential issues or fraud concerns.

1 DOCUMENT

Anonymous whistleblower channel ✓

CC 2.3

6 CONTROLS

Company commitments externally communicated

✓ COMPLETE

The company's security commitments are communicated to customers in Master Service Agreements (MSA) or Terms of Service (TOS).

3 DOCUMENTS

- **MSA template** ✓
- **Security information page** ✓
- **Publicly available terms of service** ✓

External support resources available

✓ COMPLETE

The company provides guidelines and technical support resources relating to system operations to customers.

2 DOCUMENTS

- **Customer support site or email alias** ✓
- **Public change log or release notes** ✓

Service description communicated

✓ COMPLETE

The company provides a description of its products and services to internal and external users.

2 DOCUMENTS

- **Network diagram** ✓
- **Product documentation site** ✓

Support system available

✓ COMPLETE

The company has an external-facing support system in place that allows users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel.

3 DOCUMENTS

- **Customer support site or email alias** ✓
- **Product documentation site** ✓
- **Public change log or release notes** ✓

System changes externally communicated

✓ COMPLETE

The company notifies customers of critical system changes that may affect their processing.

4 DOCUMENTS

- **Customer support site or email alias** ✓
- **Product documentation site** ✓
- **Public change log or release notes** ✓
- **Application status page** ✓

Third-party agreements established

✓ COMPLETE

The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.

2 TESTS

Vendors list maintained: Verifies that at least one vendor has been manually added to the vendors list on the [Vendors page](/vendors). ✓

Vendors assigned risk levels: Verifies that all vendors on the [Vendors page](/vendors) have a risk level assigned. ✓

3 DOCUMENTS

Cloud provider service agreement ✓

Publicly available privacy policy ✓

Publicly available terms of service ✓

CC 3.0

Risk Assessment

CC 3.1

1 CONTROL

Risk assessment objectives specified

✓ COMPLETE

The company specifies its objectives to enable the identification and assessment of risk related to the objectives.

1 TEST

Risk Assessment exercise completed annually: Verifies that a snapshot of your risk register has been taken in the past year and is shared with auditors. ✓

CC 3.2

3 CONTROLS

Continuity and disaster recovery plans tested

✓ COMPLETE

The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.

1 DOCUMENT

Tabletop disaster recovery exercise ✓

Risks assessments performed

✓ COMPLETE

The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.

1 TEST

Risk Assessment exercise completed annually: Verifies that a snapshot of your risk register has been taken in the past year and is shared with auditors. ✓

Vendor management program established

✓ COMPLETE

The company has a vendor management program in place. Components of this program include:

- critical third-party vendor inventory;
- vendor's security and privacy requirements; and
- review of critical third-party vendors at least annually.

3 TESTS

Company completes security reviews for relevant vendors: Verifies that all vendors that need security reviews have an up-to-date review. ✓

Vendors list maintained: Verifies that at least one vendor has been manually added to the vendors list on the [Vendors page](/vendors). ✓

Vendors assigned risk levels: Verifies that all vendors on the [Vendors page](/vendors) have a risk level assigned. ✓

CC 3.3

1 CONTROL

Risks assessments performed

✓ COMPLETE

The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.

1 TEST

Risk Assessment exercise completed annually: Verifies that a snapshot of your risk register has been taken in the past year and is shared with auditors. ✓

CC 3.4

3 CONTROLS

Configuration management system established

✓ COMPLETE

The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.

1 DOCUMENT

CI/CD system in use ✓

Penetration testing performed

✓ COMPLETE

The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.

2 DOCUMENTS

Penetration test report ✓

Penetration test remediation ✓

Risks assessments performed

✓ COMPLETE

The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.

1 TEST

Risk Assessment exercise completed annually: Verifies that a snapshot of your risk register has been taken in the past year and is shared with auditors. ✓

CC 4.0

Monitoring Activities

CC 4.1

4 CONTROLS

Control self-assessments conducted

✓ COMPLETE

The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings. If the company has committed to an SLA for a finding, the corrective action is completed within that SLA.

1 TEST

Company uses Vanta for continuous security monitoring: Automatically passes. ✓

Penetration testing performed

✓ COMPLETE

The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.

2 DOCUMENTS

Penetration test report ✓

Penetration test remediation ✓

Vendor management program established

✓ COMPLETE

The company has a vendor management program in place. Components of this program include:

- critical third-party vendor inventory;
- vendor's security and privacy requirements; and
- review of critical third-party vendors at least annually.

3 TESTS

Company completes security reviews for relevant vendors: Verifies that all vendors that need security reviews have an up-to-date review. ✓

Vendors list maintained: Verifies that at least one vendor has been manually added to the vendors list on the [Vendors page](/vendors). ✓

Vendors assigned risk levels: Verifies that all vendors on the [Vendors page](/vendors) have a risk level assigned. ✓

Vulnerabilities scanned and remediated

✓ COMPLETE

Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.

6 TESTS

Employee computers monitored with the Vanta Agent: Verifies that all employees required to install the Vanta Agent have installed the agent on their workstations. ✓

Critical vulnerabilities identified in packages are addressed (AWS Inspector): Verifies that all critical severity vulnerabilities detected by AWS Inspector scanning are resolved. ✓

High vulnerabilities identified in packages are addressed (AWS Inspector): Verifies that all high severity vulnerabilities detected by AWS Inspector scanning are resolved. ✓

Low vulnerabilities identified in packages are addressed (AWS Inspector): Verifies that all low severity vulnerabilities detected by AWS Inspector scanning are resolved. ✓

Medium vulnerabilities identified in packages are addressed (AWS Inspector): Verifies that all medium severity vulnerabilities detected by AWS Inspector scanning are resolved. ✓

Records of security issues being tracked: Verifies that at least one task in the linked task tracker is labeled with a `security` tag. ✓

1 DOCUMENT

Sample of remediated vulnerabilities ✓

CC 4.2

2 CONTROLS

Control self-assessments conducted

✓ COMPLETE

The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings. If the company has committed to an SLA for a finding, the corrective action is completed within that SLA.

1 TEST

Company uses Vanta for continuous security monitoring: Automatically passes. ✓

Vendor management program established

✓ COMPLETE

The company has a vendor management program in place. Components of this program include:

- critical third-party vendor inventory;
- vendor's security and privacy requirements; and
- review of critical third-party vendors at least annually.

3 TESTS

Company completes security reviews for relevant vendors: Verifies that all vendors that need security reviews have an up-to-date review. ✓

Vendors list maintained: Verifies that at least one vendor has been manually added to the vendors list on the [Vendors page](/vendors). ✓

Vendors assigned risk levels: Verifies that all vendors on the [Vendors page](/vendors) have a risk level assigned. ✓

CC 5.0

Control Activities

CC 5.2

1 CONTROL

Access control procedures established

✓ COMPLETE

The company's access control policy documents the requirements for the following access control functions:

- adding new users;
- modifying users; and/or
- removing an existing user's access.

1 DOCUMENT

Access request ticket and history ✓

CC 5.3

5 CONTROLS

Backup processes established

✓ COMPLETE

The company's data backup policy documents requirements for backup and recovery of customer data.

1 DOCUMENT

Tabletop disaster recovery exercise ✓

Change management procedures enforced

✓ COMPLETE

The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.

3 TESTS

Application changes reviewed: Verifies that at least one approval is required to merge to the default branch (or production branch, if it was explicitly specified during linking) for all linked version control repositories. ✓

Author is not the reviewer of pull requests: Verifies that all pull requests have been reviewed by someone that is not the author of the pull request. For Github, this is a default requirement for all pull requests and cannot be changed. [Github documentation](https://docs.github.com/en/pull-requests/collaborating-with-pull-requests/reviewing-changes-in-pull-requests/about-pull-request-reviews) states “Pull request authors cannot approve their own pull requests”. ✓

GitHub repository visibility has been set to private: Verifies that the visibility of all repositories (except forked repositories) has been set to private. ✓

1 DOCUMENT

CI/CD system in use ✓

Risk assessment objectives specified ✓ COMPLETE

The company specifies its objectives to enable the identification and assessment of risk related to the objectives.

1 TEST

Risk Assessment exercise completed annually: Verifies that a snapshot of your risk register has been taken in the past year and is shared with auditors. ✓

Roles and responsibilities specified ✓ COMPLETE

Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.

1 DOCUMENT

Job descriptions for key security roles ✓

Vendor management program established ✓ COMPLETE

The company has a vendor management program in place. Components of this program include:

- critical third-party vendor inventory;
- vendor's security and privacy requirements; and
- review of critical third-party vendors at least annually.

3 TESTS

Company completes security reviews for relevant vendors: Verifies that all vendors that need security reviews have an up-to-date review. ✓

Vendors list maintained: Verifies that at least one vendor has been manually added to the vendors list on the [Vendors page](/vendors). ✓

Vendors assigned risk levels: Verifies that all vendors on the [Vendors page](/vendors) have a risk level assigned. ✓

CC 6.0

Logical and Physical Access Controls

CC 6.1

17 CONTROLS

Access control procedures established

✓ COMPLETE

The company's access control policy documents the requirements for the following access control functions:

- adding new users;
- modifying users; and/or
- removing an existing user's access.

1 DOCUMENT

Access request ticket and history ✓

Access requests required

✓ COMPLETE

The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.

1 DOCUMENT

Access request ticket and history ✓

Data encryption utilized

✓ COMPLETE

The company's datastores housing sensitive customer data are encrypted at rest.

3 TESTS

User data is encrypted at rest: Verifies that all Amazon RDS instances are encrypted. ✓

User data is encrypted at rest (Heroku): Verifies that Heroku databases are encrypted at rest. This feature is automatically provided by Heroku Postgres plans on the Standard tier or higher. ✓

User data in S3 is encrypted at rest (AWS): Verifies that all AWS S3 buckets marked as containing user data are encrypted. ✓

Firewall access restricted

✓ COMPLETE

The company restricts privileged access to the firewall to authorized users with a business need.

9 TESTS

EC2 instance public ports restricted (AWS): Verifies that each EC2 instance's attached Security Groups expose at most ports 80 and 443 to the public internet for protocols other than ICMP. ✓

Unwanted traffic filtered: Verifies that all AWS EC2 instances have network ACLs or security groups attached. ✓

Unwanted traffic filtered (Heroku): This feature is built into Heroku. ✓

Firewall default disallows traffic: This feature is built into AWS. ✓

Firewall default disallows traffic (Heroku): This feature is built into Heroku. ✓

Public SSH denied (AWS): Verifies that AWS EC2 instances do not allow unrestricted access to TCP port 22. ✓

Public SSH denied (Heroku): This feature is built into Heroku. ✓

RDS instance IP restricted (AWS): Verifies that each RDS instance's attached Security Groups are only accessible by restricted IP addresses. ✓

Employees have unique SSH keys: Verifies that any two workstations with the Vanta Agent installed share no SSH keys if the workstations are owned by different users. This test doesn't check Windows machines. ✓

Network segmentation implemented

✓ COMPLETE

The company's network is segmented to prevent unauthorized access to customer data.

1 DOCUMENT

Network segregation ✓

Password policy enforced

✓ COMPLETE

The company requires passwords for in-scope system components to be configured according to the company's policy.

4 TESTS

Password policy configured for infrastructure: Verifies that all AWS accounts have password policies enabled. ✓

Password policy configured for infrastructure (Heroku): This feature is built into Heroku. ✓

Password manager records: Verifies that all employee workstations with the Vanta Agent installed have a password manager installed. ✓

Password manager records (Kandji): Verifies that all Kandji-managed workstations except those within the Computer Setup SLA are reporting a password manager installed. ✓

Production application access restricted

✓ COMPLETE

System access restricted to authorized access only

7 TESTS

Groups manage employee accounts permissions: Verifies that every AWS group has at least one IAM policy attached. ✓

Service accounts used: Verifies that every AWS account is assigned a role. ✓

Service accounts used (Heroku): This feature is built into Heroku. ✓

Root infrastructure account unused: Verifies that the AWS root user account has not been used in the last 30 days. ✓

Old infrastructure accounts disabled (AWS): Verifies that all AWS IAM users have performed at least one action in the past 90 days. ✓

No user account has a policy attached directly: Verifies that no AWS IAM policies are attached directly to users. ✓

No user account has a policy attached directly (Heroku): This feature is built into Heroku. ✓

Production database access restricted

✓ COMPLETE

The company restricts privileged access to databases to authorized users with a business need.

2 TESTS

Heroku accounts associated with users: Verifies that all Heroku accounts have been linked to users within Vanta. ✓

AWS accounts reviewed: Verifies that all AWS accounts have been linked to users within Vanta. ✓

Production deployment access restricted

✓ COMPLETE

The company restricts access to migrate changes to production to authorized personnel.

6 TESTS

Pending organization invitations are not older than 1 year: Verifies that all invitations to an organization are not older than 1 year. ✓

Application changes reviewed: Verifies that at least one approval is required to merge to the default branch (or production branch, if it was explicitly specified during linking) for all linked version control repositories. ✓

Author is not the reviewer of pull requests: Verifies that all pull requests have been reviewed by someone that is not the author of the pull request. For Github, this is a default requirement for all pull requests and cannot be changed. [Github documentation](https://docs.github.com/en/pull-requests/collaborating-with-pull-requests/reviewing-changes-in-pull-requests/about-pull-request-reviews) states “Pull request authors cannot approve their own pull requests”. ✓

Pending organization invitations are not older than 1 year: Verifies that all invitations to an organization are not older than 1 year. ✓

GitHub repository visibility has been set to private: Verifies that the visibility of all repositories (except forked repositories) has been set to private. ✓

Company has a version control system: Verifies that at least one repository in the linked version control system has been updated in the last 30 days. ✓

Production inventory maintained

✓ COMPLETE

The company maintains a formal inventory of production system assets.

3 TESTS

Inventory items have descriptions: Verifies that all items on the Vanta inventory page have descriptions. ✓

Inventory items have active owners: Verifies that all items on the Vanta inventory page have been assigned owners, and that these owners are still active employees. ✓

Inventory list tracks resources that contain user data: Verifies that these resource types - storage buckets, databases, PaaS apps, queues, data warehouses, or custom items - are marked as containing user data in Vanta. ✓

Production network access restricted

✓ COMPLETE

The company restricts privileged access to the production network to authorized users with a business need.

1 TEST

AWS accounts reviewed: Verifies that all AWS accounts have been linked to users within Vanta. ✓

Production OS access restricted

✓ COMPLETE

The company restricts privileged access to the operating system to authorized users with a business need.

3 TESTS

Heroku accounts associated with users: Verifies that all Heroku accounts have been linked to users within Vanta. ✓

AWS accounts reviewed: Verifies that all AWS accounts have been linked to users within Vanta. ✓

Snowflake accounts associated with users: Verifies that all Snowflake accounts have been linked to users within Vanta. ✓

Remote access encrypted enforced

✓ COMPLETE

The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.

2 TESTS

SSL/TLS on admin page of infrastructure console: This feature is built into AWS. ✓

SSL/TLS on admin page of infrastructure console (Heroku): This feature is built into Heroku. ✓

Remote access MFA enforced

✓ COMPLETE

The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.

4 TESTS

MFA on GitHub: Verifies that MFA is enabled on all GitHub accounts that aren't marked as external or non-human. ✓

MFA on Google Workspace: Verifies that all members of the Google Workspace organization have multi-factor authentication enabled, unless that user has been added to the organization within the configured SLA. ✓

MFA on infrastructure provider: Verifies that all AWS accounts have MFA enabled. ✓

MFA on infrastructure root accounts (AWS): Verifies that all AWS root accounts have MFA enabled. ✓

Unique account authentication enforced

COMPLETE

The company requires authentication to systems and applications to use unique username and password or authorized Secure Socket Shell (SSH) keys.

8 TESTS

Groups manage employee accounts permissions: Verifies that every AWS group has at least one IAM policy attached.

Service accounts used: Verifies that every AWS account is assigned a role.

Service accounts used (Heroku): This feature is built into Heroku.

Root infrastructure account unused: Verifies that the AWS root user account has not been used in the last 30 days.

Old infrastructure accounts disabled (AWS): Verifies that all AWS IAM users have performed at least one action in the past 90 days.

No user account has a policy attached directly: Verifies that no AWS IAM policies are attached directly to users.

No user account has a policy attached directly (Heroku): This feature is built into Heroku.

Employees have unique SSH keys: Verifies that any two workstations with the Vanta Agent installed share no SSH keys if the workstations are owned by different users. This test doesn't check Windows machines.

Unique network system authentication enforced

COMPLETE

The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.

5 TESTS

Password policy configured for infrastructure: Verifies that all AWS accounts have password policies enabled.

Password policy configured for infrastructure (Heroku): This feature is built into Heroku.

SSL/TLS on admin page of infrastructure console: This feature is built into AWS.

SSL/TLS on admin page of infrastructure console (Heroku): This feature is built into Heroku.

Employees have unique SSH keys: Verifies that any two workstations with the Vanta Agent installed share no SSH keys if the workstations are owned by different users. This test doesn't check Windows machines.

Unique production database authentication enforced

✓ COMPLETE

The company requires authentication to production datastores to use authorized secure authentication mechanisms, such as unique SSH key.

4 TESTS

MFA on GitHub: Verifies that MFA is enabled on all GitHub accounts that aren't marked as external or non-human. ✓

AWS accounts reviewed: Verifies that all AWS accounts have been linked to users within Vanta. ✓

MFA on Google Workspace: Verifies that all members of the Google Workspace organization have multi-factor authentication enabled, unless that user has been added to the organization within the configured SLA. ✓

MFA on infrastructure provider: Verifies that all AWS accounts have MFA enabled. ✓

CC 6.2

5 CONTROLS

Access control procedures established

✓ COMPLETE

The company's access control policy documents the requirements for the following access control functions:

- adding new users;
- modifying users; and/or
- removing an existing user's access.

1 DOCUMENT

Access request ticket and history ✓

Access requests required

✓ COMPLETE

The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.

1 DOCUMENT

Access request ticket and history ✓

Access reviews conducted

✓ COMPLETE

The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.

12 TESTS

Apollo accounts associated with users: Verifies that all Apollo accounts have been linked to users within Vanta. ✓

CrowdStrike accounts associated with users: Verifies that all CrowdStrike accounts have been linked to users within Vanta. ✓

Curricula accounts associated with users: Verifies that all Curricula accounts have been linked to users within Vanta. ✓

GitHub accounts associated with users: Verifies that all GitHub accounts have been linked to users within Vanta. ✓

Heroku accounts associated with users: Verifies that all Heroku accounts have been linked to users within Vanta. ✓

HubSpot accounts associated with users: Verifies that all HubSpot accounts have been linked to users within Vanta. ✓

Identity provider linked to Vanta: Verifies that Google Workspace, Office 365, or Okta has been linked to Vanta. ✓

AWS accounts reviewed: Verifies that all AWS accounts have been linked to users within Vanta. ✓

Cloud infrastructure linked to Vanta: Verifies that AWS, GCP, Heroku, Azure, or DigitalOcean is linked to Vanta. ✓

Jira accounts associated with users: Verifies that all Jira accounts have been linked to users within Vanta. ✓

Slack accounts associated with users: Verifies that all Slack accounts have been linked to users within Vanta. ✓

Snowflake accounts associated with users: Verifies that all Snowflake accounts have been linked to users within Vanta. ✓

1 DOCUMENT

Proof of completed access review ✓

Access revoked upon termination

✓ COMPLETE

The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.

9 TESTS

Apollo accounts deprovisioned when employees leave: Verifies that Apollo accounts linked to removed users are removed. ✓

AWS accounts deprovisioned when employees leave: Verifies that AWS accounts linked to removed users are removed. ✓

CrowdStrike accounts deprovisioned when employees leave: Verifies that CrowdStrike accounts linked to removed users are removed. ✓

GitHub accounts deprovisioned when employees leave: Verifies that GitHub accounts linked to removed users are removed. ✓

Heroku accounts deprovisioned when employees leave: Verifies that Heroku accounts linked to removed users are removed. ✓

HubSpot accounts deprovisioned when employees leave: Verifies that HubSpot accounts linked to removed users are removed. ✓

Jira accounts deprovisioned when employees leave: Verifies that Jira accounts linked to removed users are removed. ✓

Slack accounts deprovisioned when employees leave: Verifies that Slack accounts linked to removed users are removed. ✓

Offboarding completed for ex-employees within SLA: Verifies that all ex-employees linked to Vanta have had their accounts deprovisioned and offboarding marked as completed. ✓

2 DOCUMENTS

Employee termination checklist ✓

Employee termination security policy ✓

Unique network system authentication enforced

✓ COMPLETE

The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.

5 TESTS

Password policy configured for infrastructure: Verifies that all AWS accounts have password policies enabled. ✓

Password policy configured for infrastructure (Heroku): This feature is built into Heroku. ✓

SSL/TLS on admin page of infrastructure console: This feature is built into AWS. ✓

SSL/TLS on admin page of infrastructure console (Heroku): This feature is built into Heroku. ✓

Employees have unique SSH keys: Verifies that any two workstations with the Vanta Agent installed share no SSH keys if the workstations are owned by different users. This test doesn't check Windows machines. ✓

5 CONTROLS

Access control procedures established

✓ COMPLETE

The company's access control policy documents the requirements for the following access control functions:

- adding new users;
- modifying users; and/or
- removing an existing user's access.

1 DOCUMENT

Access request ticket and history ✓

Access requests required

✓ COMPLETE

The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.

1 DOCUMENT

Access request ticket and history ✓

Access reviews conducted

COMPLETE

The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.

12 TESTS

Apollo accounts associated with users: Verifies that all Apollo accounts have been linked to users within Vanta.

CrowdStrike accounts associated with users: Verifies that all CrowdStrike accounts have been linked to users within Vanta.

Curricula accounts associated with users: Verifies that all Curricula accounts have been linked to users within Vanta.

GitHub accounts associated with users: Verifies that all GitHub accounts have been linked to users within Vanta.

Heroku accounts associated with users: Verifies that all Heroku accounts have been linked to users within Vanta.

HubSpot accounts associated with users: Verifies that all HubSpot accounts have been linked to users within Vanta.

Identity provider linked to Vanta: Verifies that Google Workspace, Office 365, or Okta has been linked to Vanta.

AWS accounts reviewed: Verifies that all AWS accounts have been linked to users within Vanta.

Cloud infrastructure linked to Vanta: Verifies that AWS, GCP, Heroku, Azure, or DigitalOcean is linked to Vanta.

Jira accounts associated with users: Verifies that all Jira accounts have been linked to users within Vanta.

Slack accounts associated with users: Verifies that all Slack accounts have been linked to users within Vanta.

Snowflake accounts associated with users: Verifies that all Snowflake accounts have been linked to users within Vanta.

1 DOCUMENT

Proof of completed access review

Access revoked upon termination

COMPLETE

The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.

9 TESTS

Apollo accounts deprovisioned when employees leave: Verifies that Apollo accounts linked to removed users are removed.

AWS accounts deprovisioned when employees leave: Verifies that AWS accounts linked to removed users are removed.

CrowdStrike accounts deprovisioned when employees leave: Verifies that CrowdStrike accounts linked to removed users are removed.

GitHub accounts deprovisioned when employees leave: Verifies that GitHub accounts linked to removed users are removed.

Heroku accounts deprovisioned when employees leave: Verifies that Heroku accounts linked to removed users are removed.

HubSpot accounts deprovisioned when employees leave: Verifies that HubSpot accounts linked to removed users are removed.

Jira accounts deprovisioned when employees leave: Verifies that Jira accounts linked to removed users are removed.

Slack accounts deprovisioned when employees leave: Verifies that Slack accounts linked to removed users are removed.

Offboarding completed for ex-employees within SLA: Verifies that all ex-employees linked to Vanta have had their accounts deprovisioned and offboarding marked as completed.

2 DOCUMENTS

Employee termination checklist

Employee termination security policy

Unique network system authentication enforced

✓ COMPLETE

The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.

5 TESTS

Password policy configured for infrastructure: Verifies that all AWS accounts have password policies enabled. ✓

Password policy configured for infrastructure (Heroku): This feature is built into Heroku. ✓

SSL/TLS on admin page of infrastructure console: This feature is built into AWS. ✓

SSL/TLS on admin page of infrastructure console (Heroku): This feature is built into Heroku. ✓

Employees have unique SSH keys: Verifies that any two workstations with the Vanta Agent installed share no SSH keys if the workstations are owned by different users. This test doesn't check Windows machines. ✓

CC 6.4

1 CONTROL

Access reviews conducted

✓ COMPLETE

The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.

12 TESTS

Apollo accounts associated with users: Verifies that all Apollo accounts have been linked to users within Vanta. ✓

CrowdStrike accounts associated with users: Verifies that all CrowdStrike accounts have been linked to users within Vanta. ✓

Curricula accounts associated with users: Verifies that all Curricula accounts have been linked to users within Vanta. ✓

GitHub accounts associated with users: Verifies that all GitHub accounts have been linked to users within Vanta. ✓

Heroku accounts associated with users: Verifies that all Heroku accounts have been linked to users within Vanta. ✓

HubSpot accounts associated with users: Verifies that all HubSpot accounts have been linked to users within Vanta. ✓

Identity provider linked to Vanta: Verifies that Google Workspace, Office 365, or Okta has been linked to Vanta. ✓

AWS accounts reviewed: Verifies that all AWS accounts have been linked to users within Vanta. ✓

Cloud infrastructure linked to Vanta: Verifies that AWS, GCP, Heroku, Azure, or DigitalOcean is linked to Vanta. ✓

Jira accounts associated with users: Verifies that all Jira accounts have been linked to users within Vanta. ✓

Slack accounts associated with users: Verifies that all Slack accounts have been linked to users within Vanta. ✓

Snowflake accounts associated with users: Verifies that all Snowflake accounts have been linked to users within Vanta. ✓

1 DOCUMENT

Proof of completed access review ✓

CC 6.5

3 CONTROLS

Access revoked upon termination

✓ COMPLETE

The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.

9 TESTS

Apollo accounts deprovisioned when employees leave: Verifies that Apollo accounts linked to removed users are removed. ✓

AWS accounts deprovisioned when employees leave: Verifies that AWS accounts linked to removed users are removed. ✓

CrowdStrike accounts deprovisioned when employees leave: Verifies that CrowdStrike accounts linked to removed users are removed. ✓

GitHub accounts deprovisioned when employees leave: Verifies that GitHub accounts linked to removed users are removed. ✓

Heroku accounts deprovisioned when employees leave: Verifies that Heroku accounts linked to removed users are removed. ✓

HubSpot accounts deprovisioned when employees leave: Verifies that HubSpot accounts linked to removed users are removed. ✓

Jira accounts deprovisioned when employees leave: Verifies that Jira accounts linked to removed users are removed. ✓

Slack accounts deprovisioned when employees leave: Verifies that Slack accounts linked to removed users are removed. ✓

Offboarding completed for ex-employees within SLA: Verifies that all ex-employees linked to Vanta have had their accounts deprovisioned and offboarding marked as completed. ✓

2 DOCUMENTS

Employee termination checklist ✓

Employee termination security policy ✓

Asset disposal procedures utilized

✓ COMPLETE

The company has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.

1 DOCUMENT

Proof of media/device disposal ✓

Customer data deleted upon leaving

✓ COMPLETE

The company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.

1 TEST

Deleting from a logging bucket requires MFA: Verifies that all AWS S3 buckets used as the destination for CloudTrail or S3 access logs require MFA to delete. ✓

1 DOCUMENT

Customer data deletion record ✓

CC 6.6

9 CONTROLS

Data transmission encrypted

✓ COMPLETE

The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.

6 TESTS

SSL/TLS on admin page of infrastructure console: This feature is built into AWS. ✓

SSL/TLS on admin page of infrastructure console (Heroku): This feature is built into Heroku. ✓

Strong SSL/TLS ciphers used: Verifies that the company website (as specified on the business info page) has a valid certificate and only accepts TLS connections using up-to-date cipher suites. ✓

SSL configuration has no known issues: Verifies that the company website (as specified on the business info page) has a valid certificate and issues no TLS warnings. ✓

SSL certificate has not expired: Verifies that the company website (as specified on the business info page) has an unexpired certificate. ✓

SSL enforced on company website: Verifies that the company website (as specified on the business info page) redirects HTTP to HTTPS via a 3XX status code. ✓

Intrusion detection system utilized

✓ COMPLETE

The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.

6 TESTS

Intrusion detection system enabled (AWS): Verifies that AWS GuardDuty is enabled on all accounts and regions. ✓

Intrusion detection system notifications configured (AWS): Verifies that notifications have been configured for new AWS GuardDuty threat detections on all accounts and regions. ✓

CrowdStrike hosts have a non empty prevention policy: Verifies that all of your devices that have CrowdStrike installed are assigned a non empty prevention policy (has some settings enabled). ✓

Employee computers monitored with the Vanta Agent: Verifies that all employees required to install the Vanta Agent have installed the agent on their workstations. ✓

CloudTrail enabled: Verifies that all linked AWS accounts have CloudTrail enabled. ✓

User activity and API use is tracked (Heroku): This feature is built into Heroku. ✓

1 DOCUMENT

Intrusion detection system installation ✓

Network and system hardening standards maintained

✓ COMPLETE

The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.

7 TESTS

Unwanted traffic filtered: Verifies that all AWS EC2 instances have network ACLs or security groups attached. ✓

Unwanted traffic filtered (Heroku): This feature is built into Heroku. ✓

Firewall default disallows traffic: This feature is built into AWS. ✓

Firewall default disallows traffic (Heroku): This feature is built into Heroku. ✓

Public SSH denied (AWS): Verifies that AWS EC2 instances do not allow unrestricted access to TCP port 22. ✓

Public SSH denied (Heroku): This feature is built into Heroku. ✓

AWS accounts reviewed: Verifies that all AWS accounts have been linked to users within Vanta. ✓

Network firewalls reviewed

✓ COMPLETE

The company reviews its firewall rulesets at least annually. Required changes are tracked to completion.

6 TESTS

Unwanted traffic filtered: Verifies that all AWS EC2 instances have network ACLs or security groups attached. ✓

Unwanted traffic filtered (Heroku): This feature is built into Heroku. ✓

Firewall default disallows traffic: This feature is built into AWS. ✓

Firewall default disallows traffic (Heroku): This feature is built into Heroku. ✓

Public SSH denied (AWS): Verifies that AWS EC2 instances do not allow unrestricted access to TCP port 22. ✓

Public SSH denied (Heroku): This feature is built into Heroku. ✓

Network firewalls utilized

✓ COMPLETE

The company uses firewalls and configures them to prevent unauthorized access.

6 TESTS

Unwanted traffic filtered: Verifies that all AWS EC2 instances have network ACLs or security groups attached. ✓

Unwanted traffic filtered (Heroku): This feature is built into Heroku. ✓

Firewall default disallows traffic: This feature is built into AWS. ✓

Firewall default disallows traffic (Heroku): This feature is built into Heroku. ✓

Public SSH denied (AWS): Verifies that AWS EC2 instances do not allow unrestricted access to TCP port 22. ✓

Public SSH denied (Heroku): This feature is built into Heroku. ✓

Remote access encrypted enforced

✓ COMPLETE

The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.

2 TESTS

SSL/TLS on admin page of infrastructure console: This feature is built into AWS. ✓

SSL/TLS on admin page of infrastructure console (Heroku): This feature is built into Heroku. ✓

Remote access MFA enforced

✓ COMPLETE

The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.

4 TESTS

MFA on GitHub: Verifies that MFA is enabled on all GitHub accounts that aren't marked as external or non-human. ✓

MFA on Google Workspace: Verifies that all members of the Google Workspace organization have multi-factor authentication enabled, unless that user has been added to the organization within the configured SLA. ✓

MFA on infrastructure provider: Verifies that all AWS accounts have MFA enabled. ✓

MFA on infrastructure root accounts (AWS): Verifies that all AWS root accounts have MFA enabled. ✓

Service infrastructure maintained

✓ COMPLETE

The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.

11 TESTS

Critical vulnerabilities identified in packages are addressed (AWS Inspector): Verifies that all critical severity vulnerabilities detected by AWS Inspector scanning are resolved. ✓

High vulnerabilities identified in packages are addressed (AWS Inspector): Verifies that all high severity vulnerabilities detected by AWS Inspector scanning are resolved. ✓

Low vulnerabilities identified in packages are addressed (AWS Inspector): Verifies that all low severity vulnerabilities detected by AWS Inspector scanning are resolved. ✓

Medium vulnerabilities identified in packages are addressed (AWS Inspector): Verifies that all medium severity vulnerabilities detected by AWS Inspector scanning are resolved. ✓

Records of security issues being assigned to owners: Verifies that all tasks in the linked task tracker that are labeled with a `security` tag have an owner assigned within the task tracker. ✓

Security issues assigned priorities: Verifies that all tasks in the linked task tracker that are labeled with a `security` have a priority assigned within the task tracker. ✓

Records of security issues being tracked: Verifies that at least one task in the linked task tracker is labeled with a `security` tag. ✓

P0 security issues resolved: Verifies that all tasks in the linked task tracker labeled with a security and p0 tag are marked as complete. ✓

P1 security issues resolved: Verifies that all tasks in the linked task tracker labeled with a security and p1 tag are marked as complete. ✓

P2 security issues resolved: Verifies that all tasks in the linked task tracker labeled with a security and p2 tag are marked as complete. ✓

P3 security issues resolved: Verifies that all tasks in the linked task tracker labeled with a security and p3 tag are marked as complete. ✓

1 DOCUMENT

Sample of remediated vulnerabilities ✓

Unique network system authentication enforced

✓ COMPLETE

The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.

5 TESTS

Password policy configured for infrastructure: Verifies that all AWS accounts have password policies enabled. ✓

Password policy configured for infrastructure (Heroku): This feature is built into Heroku. ✓

SSL/TLS on admin page of infrastructure console: This feature is built into AWS. ✓

SSL/TLS on admin page of infrastructure console (Heroku): This feature is built into Heroku.

Employees have unique SSH keys: Verifies that any two workstations with the Vanta Agent installed share no SSH keys if the workstations are owned by different users. This test doesn't check Windows machines.

CC 6.7

3 CONTROLS

Data transmission encrypted

COMPLETE

The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.

6 TESTS

SSL/TLS on admin page of infrastructure console: This feature is built into AWS.

SSL/TLS on admin page of infrastructure console (Heroku): This feature is built into Heroku.

Strong SSL/TLS ciphers used: Verifies that the company website (as specified on the business info page) has a valid certificate and only accepts TLS connections using up-to-date cipher suites.

SSL configuration has no known issues: Verifies that the company website (as specified on the business info page) has a valid certificate and issues no TLS warnings.

SSL certificate has not expired: Verifies that the company website (as specified on the business info page) has an unexpired certificate.

SSL enforced on company website: Verifies that the company website (as specified on the business info page) redirects HTTP to HTTPS via a 3XX status code.

MDM system utilized

COMPLETE

The company has a mobile device management (MDM) system in place to centrally manage mobile devices supporting the service.

3 TESTS

CrowdStrike hosts have a non empty prevention policy: Verifies that all of your devices that have CrowdStrike installed are assigned a non empty prevention policy (has some settings enabled).

Malware detection on Windows workstations: Verifies that all employee Windows workstations with the Vanta Agent installed have antivirus software installed.

Password manager records (Kandji): Verifies that all Kandji-managed workstations except those within the Computer Setup SLA are reporting a password manager installed.

Portable media encrypted

COMPLETE

The company encrypts portable and removable media devices when used.

2 TESTS

Employee computer hard disk encryption: Verifies that all employee workstations with the Vanta Agent installed have encrypted hard drives.

Employee computer hard disk encryption (Kandji): Verifies that all Kandji-managed workstations except those within the Computer Setup SLA are reporting as encrypted.

1 DOCUMENT

Removable media encryption

CC 6.8

2 CONTROLS

Anti-malware technology utilized

COMPLETE

The company deploys anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems.

3 TESTS

CrowdStrike hosts have a non empty prevention policy: Verifies that all of your devices that have CrowdStrike installed are assigned a non empty prevention policy (has some settings enabled).

Employee computers monitored with the Vanta Agent: Verifies that all employees required to install the Vanta Agent have installed the agent on their workstations.

Malware detection on Windows workstations: Verifies that all employee Windows workstations with the Vanta Agent installed have antivirus software installed.

Service infrastructure maintained

✓ COMPLETE

The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.

11 TESTS

Critical vulnerabilities identified in packages are addressed (AWS Inspector): Verifies that all critical severity vulnerabilities detected by AWS Inspector scanning are resolved. ✓

High vulnerabilities identified in packages are addressed (AWS Inspector): Verifies that all high severity vulnerabilities detected by AWS Inspector scanning are resolved. ✓

Low vulnerabilities identified in packages are addressed (AWS Inspector): Verifies that all low severity vulnerabilities detected by AWS Inspector scanning are resolved. ✓

Medium vulnerabilities identified in packages are addressed (AWS Inspector): Verifies that all medium severity vulnerabilities detected by AWS Inspector scanning are resolved. ✓

Records of security issues being assigned to owners: Verifies that all tasks in the linked task tracker that are labeled with a `security` tag have an owner assigned within the task tracker. ✓

Security issues assigned priorities: Verifies that all tasks in the linked task tracker that are labeled with a `security` have a priority assigned within the task tracker. ✓

Records of security issues being tracked: Verifies that at least one task in the linked task tracker is labeled with a `security` tag. ✓

P0 security issues resolved: Verifies that all tasks in the linked task tracker labeled with a security and p0 tag are marked as complete. ✓

P1 security issues resolved: Verifies that all tasks in the linked task tracker labeled with a security and p1 tag are marked as complete. ✓

P2 security issues resolved: Verifies that all tasks in the linked task tracker labeled with a security and p2 tag are marked as complete. ✓

P3 security issues resolved: Verifies that all tasks in the linked task tracker labeled with a security and p3 tag are marked as complete. ✓

1 DOCUMENT

Sample of remediated vulnerabilities ✓

CC 7.0

System Operations

CC 7.1

4 CONTROLS

Change management procedures enforced

✓ COMPLETE

The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.

3 TESTS

Application changes reviewed: Verifies that at least one approval is required to merge to the default branch (or production branch, if it was explicitly specified during linking) for all linked version control repositories. ✓

Author is not the reviewer of pull requests: Verifies that all pull requests have been reviewed by someone that is not the author of the pull request. For Github, this is a default requirement for all pull requests and cannot be changed. [Github documentation](https://docs.github.com/en/pull-requests/collaborating-with-pull-requests/reviewing-changes-in-pull-requests/about-pull-request-reviews) states “Pull request authors cannot approve their own pull requests”. ✓

GitHub repository visibility has been set to private: Verifies that the visibility of all repositories (except forked repositories) has been set to private. ✓

1 DOCUMENT

CI/CD system in use ✓

Configuration management system established

✓ COMPLETE

The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.

1 DOCUMENT

CI/CD system in use ✓

Risks assessments performed

✓ COMPLETE

The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.

1 TEST

Risk Assessment exercise completed annually: Verifies that a snapshot of your risk register has been taken in the past year and is shared with auditors. ✓

Vulnerabilities scanned and remediated

✓ COMPLETE

Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.

6 TESTS

Employee computers monitored with the Vanta Agent: Verifies that all employees required to install the Vanta Agent have installed the agent on their workstations. ✓

Critical vulnerabilities identified in packages are addressed (AWS Inspector): Verifies that all critical severity vulnerabilities detected by AWS Inspector scanning are resolved. ✓

High vulnerabilities identified in packages are addressed (AWS Inspector): Verifies that all high severity vulnerabilities detected by AWS Inspector scanning are resolved. ✓

Low vulnerabilities identified in packages are addressed (AWS Inspector): Verifies that all low severity vulnerabilities detected by AWS Inspector scanning are resolved. ✓

Medium vulnerabilities identified in packages are addressed (AWS Inspector): Verifies that all medium severity vulnerabilities detected by AWS Inspector scanning are resolved. ✓

Records of security issues being tracked: Verifies that at least one task in the linked task tracker is labeled with a `security` tag. ✓

1 DOCUMENT

Sample of remediated vulnerabilities ✓

CC 7.2

6 CONTROLS

Infrastructure performance monitored

✓ COMPLETE

An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.

6 TESTS

Load balancer used (Heroku): This feature is built into Heroku. ✓

SQL database freeable memory monitored (AWS): Verifies that all Amazon RDS instances have CloudWatch alarms set for the FreeableMemory metric. ✓

Database IO monitored (AWS): Verifies that all Amazon RDS instances have CloudWatch alarms set for at least one of the following metrics: - `DiskQueueDepth` - `VolumeWriteIOPs` - `VolumeReadIOPs` - `WriteIOPS` - `ReadIOPS` ✓

SQL database free storage space monitored (AWS): Verifies that all Amazon RDS instances have CloudWatch alarms set up for at least one of the following metrics: - `FreeStorageSpace` on MySQL and PostgreSQL databases - `FreeLocalStorage` on Aurora MySQL and Aurora PostgreSQL databases - `AuroraVolumeBytesLeftTotal` on Aurora MySQL Databases ✓

Serverless function error rate monitored (AWS): Verifies that all AWS Lambda functions have a CloudWatch alarm enabled on the Error metric. ✓

Messaging queue message age monitored: Verifies that all AWS SQS queues have a CloudWatch alarm set for the `ApproximateAgeOfOldestMessage` metric. ✓

Intrusion detection system utilized

✓ COMPLETE

The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.

6 TESTS

Intrusion detection system enabled (AWS): Verifies that AWS GuardDuty is enabled on all accounts and regions. ✓

Intrusion detection system notifications configured (AWS): Verifies that notifications have been configured for new AWS GuardDuty threat detections on all accounts and regions. ✓

CrowdStrike hosts have a non empty prevention policy: Verifies that all of your devices that have CrowdStrike installed are assigned a non empty prevention policy (has some settings enabled). ✓

Employee computers monitored with the Vanta Agent: Verifies that all employees required to install the Vanta Agent have installed the agent on their workstations. ✓

CloudTrail enabled: Verifies that all linked AWS accounts have CloudTrail enabled. ✓

User activity and API use is tracked (Heroku): This feature is built into Heroku. ✓

1 DOCUMENT

Intrusion detection system installation ✓

Log management utilized

✓ COMPLETE

The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.

7 TESTS

VPC Flow Logs enabled: Verifies that all AWS VPCs have flow logs enabled. ✓

Heroku logs archived for 365 days: Verifies that all Heroku apps are using a plugin that stores logs for 365 days, or are using a custom log drain. ✓

CloudTrail enabled: Verifies that all linked AWS accounts have CloudTrail enabled. ✓

User activity and API use is tracked (Heroku): This feature is built into Heroku. ✓

Cloud infrastructure linked to Vanta: Verifies that AWS, GCP, Heroku, Azure, or DigitalOcean is linked to Vanta. ✓

Only authorized users can access logging buckets: Verifies that no AWS S3 logging buckets grant access to the built-in AWS groups AllUsers or AuthenticatedUsers ✓

S3 server access logs enabled: Verifies there is at least one AWS S3 bucket acting as a destination for server access logging or CloudTrail data event logging. **Vanta Scope consideration:** make sure that either the S3 bucket acting as destination for server access logging or the CloudTrail data event logging is [scoped] (https://help.vanta.com/hc/en-us/articles/360062025631-Frequently-Asked-Questions-How-do-I-Mark-Resources-out-of-Scope-) in Vanta otherwise this test will fail. ✓

Penetration testing performed

✓ COMPLETE

The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.

2 DOCUMENTS

Penetration test report ✓

Penetration test remediation ✓

Service infrastructure maintained

✓ COMPLETE

The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.

11 TESTS

Critical vulnerabilities identified in packages are addressed (AWS Inspector): Verifies that all critical severity vulnerabilities detected by AWS Inspector scanning are resolved. ✓

High vulnerabilities identified in packages are addressed (AWS Inspector): Verifies that all high severity vulnerabilities detected by AWS Inspector scanning are resolved. ✓

Low vulnerabilities identified in packages are addressed (AWS Inspector): Verifies that all low severity vulnerabilities detected by AWS Inspector scanning are resolved. ✓

Medium vulnerabilities identified in packages are addressed (AWS Inspector): Verifies that all medium severity vulnerabilities detected by AWS Inspector scanning are resolved. ✓

Records of security issues being assigned to owners: Verifies that all tasks in the linked task tracker that are labeled with a `security` tag have an owner assigned within the task tracker. ✓

Security issues assigned priorities: Verifies that all tasks in the linked task tracker that are labeled with a `security` have a priority assigned within the task tracker. ✓

Records of security issues being tracked: Verifies that at least one task in the linked task tracker is labeled with a `security` tag. ✓

P0 security issues resolved: Verifies that all tasks in the linked task tracker labeled with a security and p0 tag are marked as complete. ✓

P1 security issues resolved: Verifies that all tasks in the linked task tracker labeled with a security and p1 tag are marked as complete. ✓

P2 security issues resolved: Verifies that all tasks in the linked task tracker labeled with a security and p2 tag are marked as complete. ✓

P3 security issues resolved: Verifies that all tasks in the linked task tracker labeled with a security and p3 tag are marked as complete. ✓

1 DOCUMENT

Sample of remediated vulnerabilities ✓

Vulnerabilities scanned and remediated

✓ COMPLETE

Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.

6 TESTS

Employee computers monitored with the Vanta Agent: Verifies that all employees required to install the Vanta Agent have installed the agent on their workstations. ✓

Critical vulnerabilities identified in packages are addressed (AWS Inspector): Verifies that all critical severity vulnerabilities detected by AWS Inspector scanning are resolved. ✓

High vulnerabilities identified in packages are addressed (AWS Inspector): Verifies that all high severity vulnerabilities detected by AWS Inspector scanning are resolved. ✓

Low vulnerabilities identified in packages are addressed (AWS Inspector): Verifies that all low severity vulnerabilities detected by AWS Inspector scanning are resolved. ✓

Medium vulnerabilities identified in packages are addressed (AWS Inspector): Verifies that all medium severity vulnerabilities detected by AWS Inspector scanning are resolved. ✓

Records of security issues being tracked: Verifies that at least one task in the linked task tracker is labeled with a `security` tag. ✓

1 DOCUMENT

Sample of remediated vulnerabilities ✓

CC 7.3

1 CONTROL

Incident management procedures followed

✓ COMPLETE

The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.

4 TESTS

P0 security issues resolved: Verifies that all tasks in the linked task tracker labeled with a security and p0 tag are marked as complete. ✓

P1 security issues resolved: Verifies that all tasks in the linked task tracker labeled with a security and p1 tag are marked as complete. ✓

P2 security issues resolved: Verifies that all tasks in the linked task tracker labeled with a security and p2 tag are marked as complete. ✓

P3 security issues resolved: Verifies that all tasks in the linked task tracker labeled with a security and p3 tag are marked as complete. ✓

CC 7.4

4 CONTROLS

Incident management procedures followed

✓ COMPLETE

The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.

4 TESTS

P0 security issues resolved: Verifies that all tasks in the linked task tracker labeled with a security and p0 tag are marked as complete. ✓

P1 security issues resolved: Verifies that all tasks in the linked task tracker labeled with a security and p1 tag are marked as complete. ✓

P2 security issues resolved: Verifies that all tasks in the linked task tracker labeled with a security and p2 tag are marked as complete. ✓

P3 security issues resolved: Verifies that all tasks in the linked task tracker labeled with a security and p3 tag are marked as complete. ✓

Incident response plan tested

✓ COMPLETE

The company tests their incident response plan at least annually.

2 DOCUMENTS

Incident report or root cause analysis ✓

Test of incident response plan ✓

Service infrastructure maintained

✓ COMPLETE

The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.

11 TESTS

Critical vulnerabilities identified in packages are addressed (AWS Inspector): Verifies that all critical severity vulnerabilities detected by AWS Inspector scanning are resolved. ✓

High vulnerabilities identified in packages are addressed (AWS Inspector): Verifies that all high severity vulnerabilities detected by AWS Inspector scanning are resolved. ✓

Low vulnerabilities identified in packages are addressed (AWS Inspector): Verifies that all low severity vulnerabilities detected by AWS Inspector scanning are resolved. ✓

Medium vulnerabilities identified in packages are addressed (AWS Inspector): Verifies that all medium severity vulnerabilities detected by AWS Inspector scanning are resolved. ✓

Records of security issues being assigned to owners: Verifies that all tasks in the linked task tracker that are labeled with a `security` tag have an owner assigned within the task tracker. ✓

Security issues assigned priorities: Verifies that all tasks in the linked task tracker that are labeled with a `security` have a priority assigned within the task tracker. ✓

Records of security issues being tracked: Verifies that at least one task in the linked task tracker is labeled with a `security` tag. ✓

P0 security issues resolved: Verifies that all tasks in the linked task tracker labeled with a security and p0 tag are marked as complete. ✓

P1 security issues resolved: Verifies that all tasks in the linked task tracker labeled with a security and p1 tag are marked as complete. ✓

P2 security issues resolved: Verifies that all tasks in the linked task tracker labeled with a security and p2 tag are marked as complete. ✓

P3 security issues resolved: Verifies that all tasks in the linked task tracker labeled with a security and p3 tag are marked as complete. ✓

1 DOCUMENT

Sample of remediated vulnerabilities ✓

Vulnerabilities scanned and remediated

✓ COMPLETE

Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.

6 TESTS

Employee computers monitored with the Vanta Agent: Verifies that all employees required to install the Vanta Agent have installed the agent on their workstations. ✓

Critical vulnerabilities identified in packages are addressed (AWS Inspector): Verifies that all critical severity vulnerabilities detected by AWS Inspector scanning are resolved. ✓

High vulnerabilities identified in packages are addressed (AWS Inspector): Verifies that all high severity vulnerabilities detected by AWS Inspector scanning are resolved. ✓

Low vulnerabilities identified in packages are addressed (AWS Inspector): Verifies that all low severity vulnerabilities detected by AWS Inspector scanning are resolved. ✓

Medium vulnerabilities identified in packages are addressed (AWS Inspector): Verifies that all medium severity vulnerabilities detected by AWS Inspector scanning are resolved. ✓

Records of security issues being tracked: Verifies that at least one task in the linked task tracker is labeled with a `security` tag. ✓

1 DOCUMENT

Sample of remediated vulnerabilities ✓

CC 7.5

3 CONTROLS

Continuity and disaster recovery plans tested

✓ COMPLETE

The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.

1 DOCUMENT

Tabletop disaster recovery exercise ✓

Incident management procedures followed

✓ COMPLETE

The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.

4 TESTS

P0 security issues resolved: Verifies that all tasks in the linked task tracker labeled with a security and p0 tag are marked as complete. ✓

P1 security issues resolved: Verifies that all tasks in the linked task tracker labeled with a security and p1 tag are marked as complete. ✓

P2 security issues resolved: Verifies that all tasks in the linked task tracker labeled with a security and p2 tag are marked as complete. ✓

P3 security issues resolved: Verifies that all tasks in the linked task tracker labeled with a security and p3 tag are marked as complete. ✓

Incident response plan tested

✓ COMPLETE

The company tests their incident response plan at least annually.

2 DOCUMENTS

Incident report or root cause analysis ✓

Test of incident response plan ✓

CC 8.0

Change Management

CC 8.1

6 CONTROLS

Change management procedures enforced

COMPLETE

The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.

3 TESTS

Application changes reviewed: Verifies that at least one approval is required to merge to the default branch (or production branch, if it was explicitly specified during linking) for all linked version control repositories.

Author is not the reviewer of pull requests: Verifies that all pull requests have been reviewed by someone that is not the author of the pull request. For Github, this is a default requirement for all pull requests and cannot be changed. [Github documentation](https://docs.github.com/en/pull-requests/collaborating-with-pull-requests/reviewing-changes-in-pull-requests/about-pull-request-reviews) states “Pull request authors cannot approve their own pull requests”.

GitHub repository visibility has been set to private: Verifies that the visibility of all repositories (except forked repositories) has been set to private.

1 DOCUMENT

CI/CD system in use

Network and system hardening standards maintained

COMPLETE

The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.

7 TESTS

Unwanted traffic filtered: Verifies that all AWS EC2 instances have network ACLs or security groups attached.

Unwanted traffic filtered (Heroku): This feature is built into Heroku.

Firewall default disallows traffic: This feature is built into AWS.

Firewall default disallows traffic (Heroku): This feature is built into Heroku.

Public SSH denied (AWS): Verifies that AWS EC2 instances do not allow unrestricted access to TCP port 22.

Public SSH denied (Heroku): This feature is built into Heroku.

AWS accounts reviewed: Verifies that all AWS accounts have been linked to users within Vanta.

Penetration testing performed

✓ COMPLETE

The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.

2 DOCUMENTS

Penetration test report ✓

Penetration test remediation ✓

Production deployment access restricted

✓ COMPLETE

The company restricts access to migrate changes to production to authorized personnel.

6 TESTS

Pending organization invitations are not older than 1 year: Verifies that all invitations to an organization are not older than 1 year. ✓

Application changes reviewed: Verifies that at least one approval is required to merge to the default branch (or production branch, if it was explicitly specified during linking) for all linked version control repositories. ✓

Author is not the reviewer of pull requests: Verifies that all pull requests have been reviewed by someone that is not the author of the pull request. For Github, this is a default requirement for all pull requests and cannot be changed. [Github documentation](https://docs.github.com/en/pull-requests/collaborating-with-pull-requests/reviewing-changes-in-pull-requests/about-pull-request-reviews) states “Pull request authors cannot approve their own pull requests”. ✓

Pending organization invitations are not older than 1 year: Verifies that all invitations to an organization are not older than 1 year. ✓

GitHub repository visibility has been set to private: Verifies that the visibility of all repositories (except forked repositories) has been set to private. ✓

Company has a version control system: Verifies that at least one repository in the linked version control system has been updated in the last 30 days. ✓

Service infrastructure maintained

✓ COMPLETE

The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.

11 TESTS

Critical vulnerabilities identified in packages are addressed (AWS Inspector): Verifies that all critical severity vulnerabilities detected by AWS Inspector scanning are resolved. ✓

High vulnerabilities identified in packages are addressed (AWS Inspector): Verifies that all high severity vulnerabilities detected by AWS Inspector scanning are resolved. ✓

Low vulnerabilities identified in packages are addressed (AWS Inspector): Verifies that all low severity vulnerabilities detected by AWS Inspector scanning are resolved. ✓

Medium vulnerabilities identified in packages are addressed (AWS Inspector): Verifies that all medium severity vulnerabilities detected by AWS Inspector scanning are resolved. ✓

Records of security issues being assigned to owners: Verifies that all tasks in the linked task tracker that are labeled with a `security` tag have an owner assigned within the task tracker. ✓

Security issues assigned priorities: Verifies that all tasks in the linked task tracker that are labeled with a `security` have a priority assigned within the task tracker. ✓

Records of security issues being tracked: Verifies that at least one task in the linked task tracker is labeled with a `security` tag. ✓

P0 security issues resolved: Verifies that all tasks in the linked task tracker labeled with a security and p0 tag are marked as complete. ✓

P1 security issues resolved: Verifies that all tasks in the linked task tracker labeled with a security and p1 tag are marked as complete. ✓

P2 security issues resolved: Verifies that all tasks in the linked task tracker labeled with a security and p2 tag are marked as complete. ✓

P3 security issues resolved: Verifies that all tasks in the linked task tracker labeled with a security and p3 tag are marked as complete. ✓

1 DOCUMENT

Sample of remediated vulnerabilities ✓

Vulnerabilities scanned and remediated

✓ COMPLETE

Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.

6 TESTS

Employee computers monitored with the Vanta Agent: Verifies that all employees required to install the Vanta Agent have installed the agent on their workstations. ✓

Critical vulnerabilities identified in packages are addressed (AWS Inspector): Verifies that all critical severity vulnerabilities detected by AWS Inspector scanning are resolved. ✓

High vulnerabilities identified in packages are addressed (AWS Inspector): Verifies that all high severity vulnerabilities detected by AWS Inspector scanning are resolved. ✓

Low vulnerabilities identified in packages are addressed (AWS Inspector): Verifies that all low severity vulnerabilities detected by AWS Inspector scanning are resolved. ✓

Medium vulnerabilities identified in packages are addressed (AWS Inspector): Verifies that all medium severity vulnerabilities detected by AWS Inspector scanning are resolved. ✓

Records of security issues being tracked: Verifies that at least one task in the linked task tracker is labeled with a `security` tag. ✓

1 DOCUMENT

Sample of remediated vulnerabilities ✓

CC 9.0

Risk Mitigation

CC 9.1

2 CONTROLS

Cybersecurity insurance maintained

✓ COMPLETE

The company maintains cybersecurity insurance to mitigate the financial impact of business disruptions.

1 DOCUMENT

Cybersecurity insurance policy document ✓

Risks assessments performed

✓ COMPLETE

The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.

1 TEST

Risk Assessment exercise completed annually: Verifies that a snapshot of your risk register has been taken in the past year and is shared with auditors. ✓

CC 9.2

2 CONTROLS

Third-party agreements established

✓ COMPLETE

The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.

2 TESTS

Vendors list maintained: Verifies that at least one vendor has been manually added to the vendors list on the [Vendors page](/vendors). ✓

Vendors assigned risk levels: Verifies that all vendors on the [Vendors page](/vendors) have a risk level assigned. ✓

3 DOCUMENTS

Cloud provider service agreement ✓

Publicly available privacy policy ✓

Publicly available terms of service ✓

Vendor management program established

✓ COMPLETE

The company has a vendor management program in place. Components of this program include:

- critical third-party vendor inventory;
- vendor's security and privacy requirements; and
- review of critical third-party vendors at least annually.

3 TESTS

Company completes security reviews for relevant vendors: Verifies that all vendors that need security reviews have an up-to-date review. ✓

Vendors list maintained: Verifies that at least one vendor has been manually added to the vendors list on the [Vendors page](/vendors). ✓

Vendors assigned risk levels: Verifies that all vendors on the [Vendors page](/vendors) have a risk level assigned. ✓

A 1

Additional Criteria for Availability

A 1.1

2 CONTROLS

Infrastructure performance monitored

✓ COMPLETE

An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.

6 TESTS

Load balancer used (Heroku): This feature is built into Heroku. ✓

SQL database freeable memory monitored (AWS): Verifies that all Amazon RDS instances have CloudWatch alarms set for the FreeableMemory metric. ✓

Database IO monitored (AWS): Verifies that all Amazon RDS instances have CloudWatch alarms set for at least one of the following metrics: - `DiskQueueDepth` - `VolumeWriteIOPs` - `VolumeReadIOPs` - `WriteIOPS` - `ReadIOPS` ✓

SQL database free storage space monitored (AWS): Verifies that all Amazon RDS instances have CloudWatch alarms set up for at least one of the following metrics: - `FreeStorageSpace` on MySQL and PostgreSQL databases - `FreeLocalStorage` on Aurora MySQL and Aurora PostgreSQL databases - `AuroraVolumeBytesLeftTotal` on Aurora MySQL Databases ✓

Serverless function error rate monitored (AWS): Verifies that all AWS Lambda functions have a CloudWatch alarm enabled on the Error metric. ✓

Messaging queue message age monitored: Verifies that all AWS SQS queues have a CloudWatch alarm set for the `ApproximateAgeOfOldestMessage` metric. ✓

System capacity reviewed

COMPLETE

The company evaluates system capacity on an ongoing basis, and system changes are implemented to help ensure that processing capacity can meet demand.

6 TESTS

Load balancer used (Heroku): This feature is built into Heroku.

SQL database freeable memory monitored (AWS): Verifies that all Amazon RDS instances have CloudWatch alarms set for the FreeableMemory metric.

Database IO monitored (AWS): Verifies that all Amazon RDS instances have CloudWatch alarms set for at least one of the following metrics: - `DiskQueueDepth` - `VolumeWriteIOPs` - `VolumeReadIOPs` - `WriteIOPS` - `ReadIOPS`

SQL database free storage space monitored (AWS): Verifies that all Amazon RDS instances have CloudWatch alarms set up for at least one of the following metrics: - `FreeStorageSpace` on MySQL and PostgreSQL databases - `FreeLocalStorage` on Aurora MySQL and Aurora PostgreSQL databases - `AuroraVolumeBytesLeftTotal` on Aurora MySQL Databases

Serverless function error rate monitored (AWS): Verifies that all AWS Lambda functions have a CloudWatch alarm enabled on the Error metric.

Messaging queue message age monitored: Verifies that all AWS SQS queues have a CloudWatch alarm set for the `ApproximateAgeOfOldestMessage` metric.

1 DOCUMENT

Enabled automated log alerting

A 1.2

7 CONTROLS

Backup processes established

COMPLETE

The company's data backup policy documents requirements for backup and recovery of customer data.

1 DOCUMENT

Tabletop disaster recovery exercise

Continuity and disaster recovery plans tested

COMPLETE

The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.

1 DOCUMENT

Tabletop disaster recovery exercise

Database replication utilized

✓ COMPLETE

The company's databases are replicated to a secondary data center in real-time. Alerts are configured to notify administrators if replication fails.

2 TESTS

Daily RDS database backups enabled (AWS): Verifies that all Amazon RDS instances have backups enabled. ✓

Daily database backups (Heroku): Verifies that all Heroku databases are backed up daily. This feature is automatically provided by Heroku Postgres plans on at least the Standard tier. ✓

1 DOCUMENT

Tabletop disaster recovery exercise ✓

Environmental monitoring devices implemented

✓ COMPLETE

The company has environmental monitoring devices in place and configured to automatically generate an alert to management for environmental incidents.

3 TESTS

Company completes security reviews for relevant vendors: Verifies that all vendors that need security reviews have an up-to-date review. ✓

Vendors list maintained: Verifies that at least one vendor has been manually added to the vendors list on the [Vendors page](/vendors). ✓

Vendors assigned risk levels: Verifies that all vendors on the [Vendors page](/vendors) have a risk level assigned. ✓

Production data backups conducted

✓ COMPLETE

The company performs periodic backups for production data. Data is backed up to a different location than the production system.

3 TESTS

Daily RDS database backups enabled (AWS): Verifies that all Amazon RDS instances have backups enabled. ✓

Daily database backups (Heroku): Verifies that all Heroku databases are backed up daily. This feature is automatically provided by Heroku Postgres plans on at least the Standard tier. ✓

Storage buckets versioned: Verifies that all AWS S3 buckets marked as containing user data have versioning enabled. ✓

1 DOCUMENT

Tabletop disaster recovery exercise ✓

Production multi-availability zones established

✓ COMPLETE

The company has a multi-location strategy for production environments employed to permit the resumption of operations at other company data centers in the event of loss of a facility.

1 DOCUMENT

Network diagram ✓

Risks assessments performed

✓ COMPLETE

The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.

1 TEST

Risk Assessment exercise completed annually: Verifies that a snapshot of your risk register has been taken in the past year and is shared with auditors. ✓

A 1.3

3 CONTROLS

Backup processes established

✓ COMPLETE

The company's data backup policy documents requirements for backup and recovery of customer data.

1 DOCUMENT

Tabletop disaster recovery exercise ✓

Continuity and disaster recovery plans tested

✓ COMPLETE

The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.

1 DOCUMENT

Tabletop disaster recovery exercise ✓

Intrusion detection system utilized

✓ COMPLETE

The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.

6 TESTS

Intrusion detection system enabled (AWS): Verifies that AWS GuardDuty is enabled on all accounts and regions. ✓

Intrusion detection system notifications configured (AWS): Verifies that notifications have been configured for new AWS GuardDuty threat detections on all accounts and regions. ✓

CrowdStrike hosts have a non empty prevention policy: Verifies that all of your devices that have CrowdStrike installed are assigned a non empty prevention policy (has some settings enabled). ✓

Employee computers monitored with the Vanta Agent: Verifies that all employees required to install the Vanta Agent have installed the agent on their workstations. ✓

CloudTrail enabled: Verifies that all linked AWS accounts have CloudTrail enabled. ✓

User activity and API use is tracked (Heroku): This feature is built into Heroku. ✓

1 DOCUMENT

Intrusion detection system installation ✓

C 1

Additional Criteria for Confidentiality

C 1.1

2 CONTROLS

Third-party agreements established

✓ COMPLETE

The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.

2 TESTS

Vendors list maintained: Verifies that at least one vendor has been manually added to the vendors list on the [Vendors page](/vendors). ✓

Vendors assigned risk levels: Verifies that all vendors on the [Vendors page](/vendors) have a risk level assigned. ✓

3 DOCUMENTS

Cloud provider service agreement ✓

Publicly available privacy policy ✓

Publicly available terms of service ✓

Unique account authentication enforced

✓ COMPLETE

The company requires authentication to systems and applications to use unique username and password or authorized Secure Socket Shell (SSH) keys.

8 TESTS

Groups manage employee accounts permissions: Verifies that every AWS group has at least one IAM policy attached. ✓

Service accounts used: Verifies that every AWS account is assigned a role. ✓

Service accounts used (Heroku): This feature is built into Heroku. ✓

Root infrastructure account unused: Verifies that the AWS root user account has not been used in the last 30 days. ✓

Old infrastructure accounts disabled (AWS): Verifies that all AWS IAM users have performed at least one action in the past 90 days. ✓

No user account has a policy attached directly: Verifies that no AWS IAM policies are attached directly to users. ✓

No user account has a policy attached directly (Heroku): This feature is built into Heroku. ✓

Employees have unique SSH keys: Verifies that any two workstations with the Vanta Agent installed share no SSH keys if the workstations are owned by different users. This test doesn't check Windows machines. ✓

C 1.2

2 CONTROLS

Asset disposal procedures utilized

COMPLETE

The company has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.

1 DOCUMENT

Proof of media/device disposal

Customer data deleted upon leaving

COMPLETE

The company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.

1 TEST

Deleting from a logging bucket requires MFA: Verifies that all AWS S3 buckets used as the destination for CloudTrail or S3 access logs require MFA to delete.

1 DOCUMENT

Customer data deletion record

SD - SOC 2

Supporting Compliance Documentation

SD - SOC 2

1 CONTROL

SOC 2 - System Description

COMPLETE

Complete a description of your system for Section III of the audit report

1 DOCUMENT

System Description (Section III)

Appendix A: Definitions

Bug bounty program: A crowdsourcing initiative that rewards individuals for discovering and reporting software bugs, especially those that could cause security vulnerabilities or breaches.

DDoS: Distributed denial of service. A DDoS attack is attack in which multiple compromised computer systems flood a target—such as a server, website, or other network resource—with messages or requests to cause a denial of service for users of the targeted resource.

Multifactor authentication (MFA): A security system that requires multiple methods of authentication using different types of credentials to verify users' identities before they can access a service.

Penetration test: The practice of testing a computer system, network, or web application to find vulnerabilities that an attacker might exploit.

Principle of least privilege: The principle of giving a user or account only the privileges that are required to perform a job or necessary function.

Protected data: Data that is protected from public view or use; includes personally identifiable information, sensitive data, HIPAA data, or financial data.

Sensitive data: Any information a reasonable person considers private or would choose not to share with the public.

SSH: Secure shell. A cryptographic network protocol for operating network services securely over an unsecured network.

SSL: Secure sockets layer. The standard security technology for establishing an encrypted link between a web server and a browser.

Appendix B: Document history

Vanta continuously monitors the company's security and IT infrastructure to ensure the company complies with industry-standard security standards. Vanta tests the company's security posture continuously, and this report is automatically updated to reflect the latest findings.

About Vanta

Vanta provides a set of security and compliance tools that scan, verify, and secure a company's IT systems and processes. Our cloud-based technology identifies security flaws and privacy gaps in a company's security posture, providing a comprehensive view across cloud infrastructure, endpoints, corporate procedures, enterprise risk, and employee accounts.

Vanta is based in San Francisco, California.