Service Organization Controls (SOC) 3 Report

Report on description of system DatAdvantage Cloud Platform Services by Varonis limited to Security, Availability, Confidentiality, and Privacy Trust Principles For the period May 1, 2021, to November 01, 2021

1. Independent Service Auditor's Report

To the Management and Board of Directors of Varonis Systems, Inc. ("Varonis")

Opinion

We have been engaged to report on management's statement that during the period May 1, 2021, to November 01, 2021, Varonis maintained effective controls over the Varonis DatAdvantage Cloud platform to provide reasonable assurance that:

- The system was available for operation and use, as committed or agreed
- The system was protected against unauthorized access
- Information designated as confidential was protected by the system as committed or agreed

This is based on the AICPA and CPA security, availability, confidentiality, and privacy criteria set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria) (applicable trust services criteria). Varonis management is responsible for this statement. Our responsibility is to express an opinion based on our engagement. Management's description of the aspects of the Varonis system covered by its statement is attached.

Varonis uses subservice organizations, namely AWS, for third-party co-location data centers for providing data center hosting services. The statement indicates that certain applicable trust services criteria can only be met if controls at the subservice organizations are suitably designed and operating effectively. Our examination did not extend to controls of subservice organizations and we express no opinion on those controls.

Our assurance engagement involved: (1) obtaining an understanding of Varonis relevant controls over the security, availability, confidentiality, and privacy of the Varonis DatAdvantage Cloud Platform; (2) testing and evaluating the operating effectiveness of the controls; and (3) performing such other procedures as we considered necessary in the circumstances.

We believe that our engagement provides a reasonable basis for our opinion. Because of the nature and inherent limitations of controls, Varonis's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent or detect and correct error or fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions. In our opinion, management's statement referred to above is fairly stated, in all material respects, based on the AICPA and CPA trust services security, availability, confidentiality, and privacy criteria.

KPMG Somekh Chaikin

2. Assertion of Varonis Management

The management of Varonis makes the following statement pertaining to the Varonis DatAdvantage Cloud platform. Varonis maintained effective controls over the Varonis DatAdvantage Cloud platform's system, during the period May 1, 2021, to November 01, 2021, based on the AICPA and CPA Trust Services availability, security, and confidentiality criteria set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria) to provide reasonable assurance that:

- The system was available for operation and use, as committed or agreed
- The system was protected against unauthorized access
- Information designated as confidential was protected by the system as committed or agreed

The attached description of the Varonis DatAdvantage Cloud platform's system identifies those aspects of the system covered by our statement. Varonis uses subservice organizations, namely AWS, for third-party co-location data centers for providing data center hosting services. Certain applicable trust service criteria can be met only if controls at the subservice organizations are suitably designed and operating effectively. The controls expected to be in place at the subservice organizations are included in the accompanying description of Varonis DatAdvantage Cloud platform relevant to Security, Confidentiality and Availability. This statement relates only to the controls of Varonis and excludes the controls of subservice organizations.

Varonis Systems Inc.

December 12, 2021

3. Varonis Description of its System and Controls

Company Overview and Background

Varonis started operations in 2005 and services numerous leading firms in the financial services, public, healthcare, industrial, insurance, energy and utilities, technology, consumer and retail, media and entertainment, and education sectors.

Varonis is a pioneer in data security and analytics, fighting a different battle than conventional cybersecurity companies. Varonis focuses on protecting enterprise data, which includes sensitive files and emails, as well as confidential customer, patient, and employee data. Our services also protect financial records, strategic product plans, and other intellectual property from unauthorized access by nefarious actors.

The Varonis Data Security Platform detects cyberthreats from both internal and external actors by analyzing data, account activity, and user behavior, and thereby prevents and limits disaster by locking down sensitive and stale data, and efficiently sustains a secure state with automation.

Varonis products address additional important use cases including data protection, data governance, zero trust, compliance, data privacy, classification, and threat detection and response.

Products and Services

Varonis DatAdvantage Cloud platform offers security teams a single control point for identifying sensitive data and where it's exposed, reducing risk by understanding and rightsizing privileges, and monitoring for suspicious or inappropriate behavior across SaaS apps.

Principal Service Commitment and System Requirements

Our commitment to our customers includes but is not limited to:

- An established global risk management process to identify, monitor and manage risks for the entire organization, business units, and all supplier relationships.
- Physical, logical, and remote access to sensitive information that is controlled to reduce the likelihood of a security incident. Varonis has established and follows specific access control practices to protect information and information systems from unauthorized access, modification, disclosure, or destruction.
- Secure data transmission protocols to encrypt data when transmitting over public networks. Encryption is also enabled on databases, data at rest, data backups, and communication between segmented boundaries.
- Minimum standards of security for the development, provisioning, and use of our cloud services requires that the security, confidentiality, availability, and privacy of assets within our cloud services are protected and preserved to at least the same level as assets within our own infrastructure. Cloud services provided, and risks to the services and to customers, are subject to a risk assessment and application of suitable technical and organizational controls.
- Data centers which host, store, and/or process customer production data comply with industry best practices. This includes protecting information system equipment and cabling, entrances controlled by access card, surveillance cameras, providing emergency power, shutoff, and lighting, fire alarms, protection from water and fire, and maintaining temperature and humidity controls.

- Backup procedures to ensure the continued availability and accessibility of information and minimize the cost of a disruption (e.g., operational error, disaster, or sabotage that causes damage to, or destruction of, information).
- An established business continuity and disaster recovery plan that provides an overview of the activities necessary to coordinate the recovery of critical business functions needed to manage and support recovery in the event of a disruption or disaster.
- Implementing privacy by design within our systems and processes in order to minimize risks to privacy and process personally identifiable information (PII) in line with regulatory requirements.

Organizational Structure

Varonis has an established organizational structure with defined roles and responsibilities. Roles and responsibilities are segregated based on functional requirements. Varonis has an organization chart that outlines lines of reporting. The organization chart is updated in real time to reflect any changes.

People

Varonis employees involved in the development, operation, security, or support of the DatAdvantage Cloud platform are grouped in the following primary areas:

- Executive Management
- DevOps
- Professional Services
- Product Management
- Information Security
- Product Security
- Human Resources
- Support
- Software Engineers
- Internal Audit

Data

Through the application programming Interface (API), the customer defines and controls the data they load into and store in the Varonis production network. Such data contains access logs and configuration logs. Data is accessed remotely from the Varonis customer portal via the internet. Varonis has deployed secure data transmission protocols to encrypt data when transmitting over public networks. Encryption is also enabled on databases at rest and on data backups.

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulatory requirements, with specific requirements formally established in customer contracts. This data is managed and stored in a range of database technologies, and procedures are in place to manage separate access between tenants, periodic backups, and access control.

Software

DatAdvantage Cloud is a software as a service (SaaS) solution. The Varonis application includes the following service components:

- Logging
- Network Protection
- Vulnerability Management
- Change Management
- Version Control
- Database applications
- Single Sign On(SSO)
- Patch Management automation
- Messaging application
- Storage Service
- Key Management System
- Security Information and Event Management
- Communication programmable application program interfaces (APIs) for messaging

Overview of Varonis Internal Control Environment

Company Policies

Formal written organization-wide information security policies for the principles and processes within the organization are developed and communicated so that personnel understand Varonis objectives. The assigned policy owners review and approve the policy on an annual basis, and responsibility and accountability for developing and maintaining the policies are assigned to relevant Varonis teams.

Access Control, User and Permissions Management

Varonis users are provided with the minimal access rights required to carry out their duties – known as 'least-privilege' access. Varonis users are assigned to a specific group upon hire. Users who are assigned to the production group can request access to production. Their access is reviewed periodically by the business owners. When a user from that group is requesting access to production, the request must be approved by the business owner for each session. Access is limited by time, documented, logged, and monitored by the Security Operations Center (SOC). Employees accessing DatAdvantage Cloud are required to use a two-factor authentication mechanism.

Logical and physical access is revoked from resigned employees upon termination.

Services accessing AWS resources such as Amazon Simple Queue Service (SQS) or databases and internal API services are required to use a generated token, which is changed periodically.

Customer employee access is authenticated in the system either by logging in with an applicable user assigned ID or federated by the customer or federated through the Customer Identity Provider supported by the system.

Separation of environments

All secrets, such as tokens for connecting to customer databases, are stored in AWS Secrets Manager. Separate roles are used to access each tenant's secrets. Tokens that are the responsibility of Varonis, e.g., the password for tenant databases are periodically rotated.

The Production environment is completely separated from the staging and development environment with separate access control and segmented network.

Physical Security

Varonis maintains a physical security policy that aligns with industry best practices. The policy details procedures for securing offices globally, access restrictions to buildings and offices, badge access, periodic review of entry, and continuous workplace monitoring.

Our partner data centers, Amazon AWS, is SOC 2 compliant. The SOC 2 report addresses various physical security and environmental controls that are tested annually. The Varonis security team reviews certificates and attestations reports annually to ensure a consistent level of protection.

Change Management

All changes to Varonis services follow a structured process to ensure appropriate planning and execution. This structured process requires communication, the documentation of important process workflows and personnel roles, and the alignment of automation tools where appropriate.

Software changes are tested in the development environment, committed to a source code management system, and reviewed through automated testing or by peers. Releases are tested by QA, before deployment or at least once a week.

Software Testing and Validation Process

The Varonis Validation and Quality Assurance (QA) team is involved from the early stages of development. Automatic tests are performed using a dedicated tool to validate the code quality. Code review is mandatory in order to continue

the Secure Software Development Lifecycle (SSDLC) process. A successful test status is mandatory in order to continue in the SDLC process and deploy a version to the production environment.

Privacy Management

Varonis is committed to comply with all applicable national data protection laws and regulations and maintaining appropriate procedures and work instructions as part of its privacy information management system (PIMS). The privacy program is aligned with global privacy standards, including the EU's General Data Protection Regulation (GDPR).

Varonis implements a privacy by design strategy which limits the scope and scale of data collection and processing as much as possible, to limit risks to sensitive data.

Varonis is committed to upholding contractual terms related to privacy and data protection agreed with its partners, subcontractors, and other relevant third parties (customers, suppliers, etc.). Varonis has a designated Data Protection Officer (DPO) who guides Varonis on all data privacy concerns, risk management, and legal or ethical matters.

Security and Privacy Awareness Training

Varonis employees undergo an information security and privacy awareness training upon joining the company, as well as annually thereafter, in conformance to the Varonis information security policy. The training ensures that each group of employees receives security training according to its technical knowledge and needs.

Description of the Production Environment

Infrastructure

Varonis DatAdvantage Cloud infrastructure is deployed on Amazon Web Services (AWS) (utilizing both SaaS and PaaS solutions) for hosting and operating the production, staging, and development environments. Varonis leverages the experience, resilience, and reliability of AWS to scale quickly and securely to meet the current and future demands.

Each boundary of the system has specific security controls applicable to it. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the system.

Production Environment

The Varonis production environment is hosted in Amazon Web Services (AWS) Virtual Public Cloud, located globally. The facilities comply with standards of Varonis security and reliability that enable Varonis to provide its services in an efficient and stable manner.

Network Infrastructure

Robust network infrastructure is essential for reliable and secure real-time data communication between the Varonis cloud service components. To provide sufficient capacity, the Varonis network infrastructure relies on platforms provided by Amazon Web Services (AWS). To ensure appropriate network security levels, Varonis security standards and practices are backed by a multi-layered approach, aimed at preventing security breaches, and ensuring confidentiality and availability.

Security and Architecture

Varonis provides a secure, reliable, and resilient SaaS platform that has been designed from the ground up based on industry best practices. The sections below addresses the network and hardware infrastructure, software, and information security elements that Varonis delivers as part of this platform, database management system security, application controls, and intrusion detection monitoring software.

Data Center Security

Varonis relies on the Amazon Web Services global infrastructure, including the facilities, network, hardware, and operational software that support the provisioning and use of basic computing resources and storage.

Security Testing

Various sets of security testing are performed on the cloud infrastructure and applications. Testing includes but is not limited to, Web application vulnerability scan, configuration scanning, open-source component scanning, other automated scans, and penetration tests which are performed on an annual basis by a reputable third-party vendor.

Incident Response

Varonis has implemented incident response policies and procedures to detect, investigate, and respond to security incidents. These procedures guide Varonis personnel in reporting and responding to information technology incidents that affect the security, availability, and confidentiality of the system. The Incident Response plan contains procedures to address various cybersecurity scenarios that may occur. This includes roles and responsibilities, and the communication process for stakeholders at each phase.

Data Encryption

Varonis has deployed secure data transmission protocols to encrypt data when transmitting over public networks. Encryption is also enabled on databases at rest and on data backups. Communication between the boundaries is encrypted. External Zone boundaries (internet facing services) are exposed through TLS (Transport Layer Security).

Asset Management

Company assets are tracked and managed throughout the asset lifecycle. Assets are assigned owners to ensure there is an individual responsible for securing the asset. The tracked assets include production components as well as employee devices that may contain personal data. When assets reach end of life, they are securely destroyed to ensure that data is not recoverable.

Availability Procedures

Backup

Varonis database and storage are hosted at AWS. A daily backup is performed using an automated application. In case of failure, a notification is sent to the operations team. Varonis production databases utilize AWS Multi Availability Zone capabilities. Additionally, a complete replica is stored at the additional region.

Restoration

Restoration tests are performed regularly. Test includes a full restore to a separate database server and bringing up the database to verify data integrity and accessibility.

Business Continuity Plan (BCP)

The Varonis Business Continuity plan outlines measures to avoid disruptions to customers and partners. The proposal includes impact analysis and risk assessment to help identify critical functions and processes. Customer support and resiliency are top priorities. The plan includes a strategic continuity plan for customer support and cloud-based solutions, including all systems, suppliers, and users. The DatAdvantage Cloud platform is hosted in multiple availability zones.

Testing of resiliency and disaster recovery is fully automated and performed daily.

The business continuity also includes the following topics:

- Corporate infrastructure
- Critical suppliers
- Cyber Incident Response
- Pandemic preparedness

Endpoint Security

Devices issued to company personnel must meet minimum security criteria that includes full disk encryption, screen lockout policy, running anti-malware and other security software, and being kept up to date with security patches.

Monitoring Usage

Varonis uses a suite of monitoring tools to monitor its service. Alerts are sent to relevant stakeholders by an internal communication tool, based on predefined rules. The notifications are reviewed and processed according to their level of urgency.

Subservice Organizations (Sub processors)

The cloud hosting services provided by AWS were not included within the scope of this examination. See the Complementary Subservice Organization Controls section below for more details.

Complementary User Entity Controls

Varonis controls related to the DatAdvantage Cloud platform cover only a portion of the overall internal controls for each user entity of this platform. It is not feasible for the Trust Services criteria related to the DatAdvantage Cloud platform to be achieved solely by Varonis. Therefore, each user entity's internal control must be evaluated in conjunction with Varonis controls described in this report, taking into consideration the related complementary user entity controls expected to be implemented and operating effectively, and shown in the table below.

#	Complementary User Entity Control
1.	User Entity should contact Varonis support team before performing maintenance or changes to prevent availability issues.
2.	User Entity can access the Varonis service only through the interfaces and protocols provided or authorized by Varonis.

User Entity Responsibilities

The Varonis system is designed with the assumption that certain responsibilities are managed by the users of the system. Customer controls are expected to be in operation at user entities to complement Varonis controls. The procedures listed below are the responsibility of users of the system.

#	User Entity Responsibilities
1.	Varonis Dashboard Multi Factor Authentication (MFA) login enforcement
2.	Varonis Dashboard user management – creating, removing, and updating user access
3.	Varonis webhook API is integrated with certified 3rd party platform(s)
4.	Varonis webhook data is accessible to certified personnel only
5.	Varonis integration(s) to 3rd party applications in accordance with necessary compliance

Subservice Organizations carved-out controls: Amazon Web Services (AWS)

The following table presents the applicable Trust Services criteria that are intended to be met by controls at AWS, alone, or in combination with controls at Varonis, and the types of controls expected to be implemented at AWS to meet those criteria. The subservice organization is SOC 2 certified and is not included in the scope of this report.

Control Activity Expected to be Implemented by AWS	Applicable Trust Services Criteria
AWS is responsible for managing logical access to the underlying network, virtualization management, and storage devices for its infrastructure as a Service (IaaS) cloud hosting services where Information systems reside.	CC5.1 – CC5.4, CC5.6
AWS is responsible for implementing controls to detect and address vulnerabilities impacting the infrastructure components supporting the cloud services utilized by Varonis.	A 1.1, CC 7.1 – CC 7-5
AWS is responsible for implementing and maintaining environmental protections.	A 1.2
AWS is responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers.	CC5.5
AWS is responsible for providing and maintaining the environmental security systems (fire detection and suppression systems, UPS systems, generators, air conditioning units) at the data center facilities.	A1.2