Varonis

DatAdvantage Cloud Platform

ISAE 3000 (SOC 3)

Service Auditor’s Assurance Report

For the period

November 1, 2023, to October 31, 2024

Contents

Section I - Management Assertion Provided by Varonis

We have prepared the attached description of DatAdvantage Cloud Platform ('The System') for the time period of November 1, 2023, to October 31, 2024 (the 'Description') based on the criteria in items (a)(i)–(ii) below, which are the criteria for a description of a service organization's system in paragraph 1.34 of the AICPA Guide Reporting on Controls at a Service Organization Relevant to Security, Availability, Confidentiality and Privacy (the 'Description criteria'). The Description is intended to provide with information about DatAdvantage Cloud Platform and to meet the criteria for "2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy" issued by the Association of International Certified Professional Accountants (AICPA).

We confirm, to the best of our knowledge and belief, that:

A. The Description fairly presents The System for the period November 1, 2023, to October 31, 2024, based on the following Description criteria:
    I. The Description contains the following information:
        1. The types of services provided.
        2. The components of the system used to provide the services:
            a) Infrastructure: the physical and hardware components of a system (facilities, equipment, and networks);
            b) Software: the programs and operating software of a system (systems, applications, and utilities);
            c) People: the personnel involved in the operation and use of a system (developers, operators, users, and managers);
            d) Procedures: the automated and manual procedures involved in the operation of a system; and
            e) Data: the information used and supported by a system (transaction streams, files, databases, and tables).
        3. The boundaries or aspects of the system covered by the Description;
        4. How the system captures and addresses significant events and conditions;
        5. The process used to prepare and deliver reports and other information to customers and other related parties;
        6. If information is provided to, or received from, subservice organizations or other parties; how such information is provided or received; the role of the subservice organization and other parties; and the procedures performed to determine that such information and its processing, maintenance and storage are subject to appropriate controls;
        7. For each principle being reported on, the applicable trust services criteria and the related controls that must be designed and operated effectively to meet those criteria, including as applicable:
            a) Complementary user-entity controls contemplated in the design and operation of the service organization's system.
        8. For subservice organizations presented using the carve-out method, the nature of the services provided by the subservice organization; each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria;
        9. Any applicable trust services criteria that are not addressed by a control and the reasons; and
        10. Other aspects of the service organization's control environment, risk assessment process, information and communication systems, and monitoring of controls that are relevant to the

services provided and the applicable trust services criteria.

II. The Description does not omit or distort information relevant to the service organization's system while acknowledging that the Description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.

B. Subject to the information outlined in point c) below, the controls stated in the Description were suitably designed and operated effectively for the period November 1, 2023, to October 31, 2024, to meet the applicable trust services criteria. This assumes that the subservice organizations applied, for the specified period, the types of controls expected to be implemented and operated at the subservice organization and incorporated in the design of the system.

SOMEKH CHAIKIN
KPMG Millennium Tower
17 Ha'arba'a Street
Tel Aviv, 6473917, Israel

TEL +972 3 684 8000
Fax +972 3 684 8444
Website www.kpmg.co.il

Section II – Independent Service Auditor's Assurance Report Provided by KPMG

Private and confidential

The Board of Directors

Varonis

November 17, 2024

Dear Directors,

ISAE 3000 (SOC 2) Type II Independent Service Auditor's Assurance Report.

In accordance with our engagement letter dated March 30, 2021, we have examined the accompanying Description in Section III of the controls in place at the service organization called Varonis Systems Inc. ('Varonis') and carried out procedures to enable us to form an independent opinion on whether Varonis's management has fairly described DatAdvantage Cloud Platform throughout the specified period of November 1, 2023, to October 31, 2024 (the 'Description'), and on the design and operation of controls stated in the Description to meet criteria for the Security, Confidentiality, Privacy and Availability Principles set forth in the TSP section 100, Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy (AICPA, Technical Practice Aids) ('applicable trust services criteria'). Our opinion is set out below and should be read and considered in conjunction with this report in full.

Varonis Management's responsibilities

In this report, references to Varonis's "management" means the directors of Varonis and those employees to whom the directors of Varonis have properly delegated day-to-day conduct over matters for which the directors of Varonis retain ultimate responsibility.

Management of Varonis is responsible for (1) preparing its statement and the system description, (2) having a reasonable basis for its statement, (3) selecting the criteria to be used and stating them in the statement, (4) specifying the controls that meet the applicable trust services criteria and stating them in the Description, and (5) designing, implementing, and documenting controls that are suitably designed and operating effectively to provide reasonable assurance that the applicable trust services criteria will be achieved.

Service Auditor's responsibilities

Our responsibility is to express an independent opinion to Varonis based on the procedures performed and evidence obtained, as to whether (1) Varonis's management Description fairly presents the controls that were designed and implemented throughout the specified period, and the aspects of the controls that may be relevant to a user organization's internal control, as it relates to an audit of the Security Principle within Varonis's statement, (2) the controls included in the Description were suitably designed throughout the specified period to provide reasonable assurance that the required trust services criteria would be met if the described controls were complied with satisfactorily, and (3) such controls were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the required trust services criteria were achieved during the specified period.

Framework Applied

Our work was performed based on the framework set out by the International Auditing and Assurance Standards Board (IAASB), International Standard on Assurance Engagements (ISAE 3000).

SOMEKH CHAIKIN
KPMG Millennium Tower
17 Ha'arba'a Street
Tel Aviv, 6473917, Israel

TEL +972 3 684 8000
Fax +972 3 684 8444
Website www.kpmg.co.il

Our Independence and Quality Control

We comply with the Code of Ethics for Professional Accountants issued by the International Ethics Standards Board for Accountants. Accordingly, we maintain a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements and professional standards (including independence, and other requirements founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality, and professional behavior) as well as applicable legal and regulatory requirements.

Scope of work

An assurance engagement to report on the description, design, and operating effectiveness of controls at a service organization involves performing procedures to obtain evidence about the disclosures in the service organization's Description of its system, and the design and operating effectiveness of controls. The procedures selected depend on the service auditor's judgment, including the assessment of the risks that the Description is not fairly presented, and that controls are not suitably designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the applicable trust services criteria were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the Description based on the Description criteria and the suitability of design and operating effectiveness of those controls to meet the applicable trust services criteria.

We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Limitations of Controls at a Service Organization

Varonis management's Description is prepared to meet the needs of their auditors. Also, because of their nature, controls at a service organization may not prevent or detect all errors or omissions in service operations or related reporting. Also, the projection of any evaluation of the effectiveness of the controls to meet the applicable trust services criteria to future periods is subject to the risk that the system may change or that controls at a service organization may become inadequate or fail.

The relative effectiveness and significance of specific controls at Varonis, and their effect on assessments of control risk at the user organization is dependent on their interaction with the controls and other factors present at the user organization. We have performed no procedures to evaluate the effectiveness of controls at the user organization.

Opinion

Our opinion has been formed on the basis of the matters outlined in this report. In our opinion, in all material respects, based on the criteria identified in Varonis's statement on Section II and III and the applicable trust services criteria:

A. The Description fairly presents The System that was designed and implemented throughout the period of November 1, 2023, to October 31, 2024.
B. The controls stated in the Description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the described controls were complied with satisfactorily throughout the period of November 1, 2023, to October 31, 2024; and
C. The controls tested, which were those necessary to provide reasonable assurance that the applicable trust services criteria were achieved, operated effectively throughout the period of November 1, 2023, to October 31, 2024.

SOMEKH CHAIKIN
KPMG Millennium Tower
17 Ha'arba'a Street
Tel Aviv, 6473917, Israel

TEL +972 3 684 8000
Fax +972 3 684 8444
Website www.kpmg.co.il

About this report including disclosure

This report is made to and has been prepared solely for the management of Varonis, as a body, on the terms agreed and recorded in our Engagement Letter. In this report, by "management" we mean the directors of Varonis and those employees to whom the directors of Varonis have properly delegated day-to-day conduct over matters for which the directors of Varonis retain ultimate responsibility.

This report was designed to meet the agreed requirements of Varonis and particular features of our engagement determined by Varonis's needs at the time.

The information contained in this report is confidential and shall not be released, duplicated, published, or disclosed in whole or in part, or used for other purposes, without our prior written consent or as permitted by our engagement letter.

Intended users and purpose

This report and Description of tests of controls and results on section IV are only to be disclosed to User Entities who have a sufficient understanding of the following:

- The nature of the service provided by the service organization;
- How the service organization's system interacts with user entities, subservice organizations, and other parties;
- Internal control and its limitations;
- Complementary user-entity controls and how they interact with related controls at the service organization to meet the applicable trust services criteria;
- The applicable trust services criteria; and
- The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks.

The above understanding is necessary to enable the User Entities to consider the matters stated including the basis of our consent to disclosure and their ability to rely on this report, along with other information including information about controls implemented by customers themselves, when assessing the risks in relation to User Entities' operational systems. This report is not to be used by anyone other than these specified parties.

Any party other than Varonis or its management, as a body, who obtains access to this report or a copy and chooses to use and rely on this report (or any part of it) will therefore do so at its own risk. To the fullest extent permitted by law, we do not accept or assume responsibility to anyone other than Varonis and its management, as a body, for our work, for this report, or for the opinions we have formed.

SOMEKH CHAIKIN
KPMG Millennium Tower
17 Ha'arba'a Street
Tel Aviv, 6473917, Israel

TEL +972 3 684 8000
Fax +972 3 684 8444
Website www.kpmg.co.il

Yours faithfully,

KPMG

Tel Aviv, Israel

November 17, 2024

Section III - Description of Varonis DatAdvantage Cloud Platform

Company Overview and Background

Varonis Systems, Inc. ("Varonis") started operations in 2005 and services numerous leading firms in various sectors, including financial services, public, healthcare, industrial, insurance, energy and utilities, technology, consumer and retail, media and entertainment, and education.

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 email, as well as confidential customer, patient, and employee data. Our services also protect financial records, strategic product plans, and other proprietary information 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, in a way that 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.

Description of the Services Provided

The Varonis DatAdvantage Cloud a cloud-hosted data security platform for protecting and governing enterprise data. Companies use Varonis DatAdvantage Cloud to discover mission-critical data, ensure only the right people have access, and detect threats before they come breaches. Varonis integrates with a wide array of data repositories, applications, and infrastructure to give customers a holistic view of their data. Varonis can be used to address these important use cases:

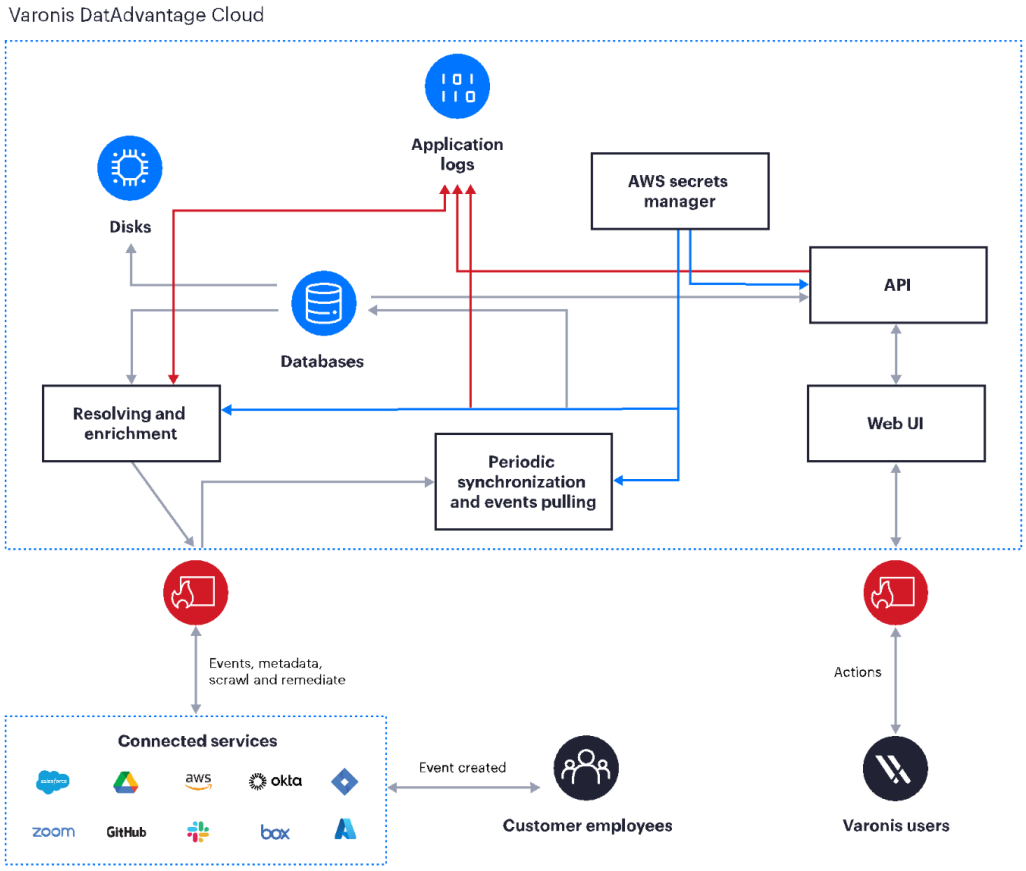
- **Detecting insider threats and cyberattacks**: Varonis DatAdvantage Cloud detects threats to data, including insider threats and external cyberattacks with a live-updating library of pre-built threat models based on attack techniques and vulnerabilities used by real-world adversaries.
- **Pinpointing data exposure**: Varonis DatAdvantage Cloud automatically classifies sensitive data, highlights where information is exposed externally or internally, and helps teams prioritize remediation efforts.
- **Limiting the blast radius of an attack**: Varonis DatAdvantage Cloud analyzes where there is unnecessary access to data and drastically reduces the damage from insider threats and cyberattacks.
- **Fixing misconfigurations**: Varonis DatAdvantage Cloud provides SSPM capabilities to analyze and fix misconfigured SaaS applications, discovering shadow instances, or spotting vulnerabilities that could put data at risk.
- **Achieving compliance**: Varonis' vast library of classification rules can discover sensitive data related to GDPR, CCPA, HIPAA, and more. The permissions analysis and continual monitoring Varonis provides gives auditors a real-time pulse on compliance.

Infrastructure

Varonis' DatAdvantage Cloud infrastructure is deployed on Amazon AWS (utilizing both SaaS and Platform as a Service [PaaS] solutions) for hosting and operating 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 of its customers.

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

System Boundaries



Varonis' DatAdvantage Cloud infrastructure is implemented in Amazon AWS and uses Okta as the identity provider for customer access and authentication. The Varonis solution leverages the capabilities, resilience, and reliability of Amazon AWS to scale quickly and securely to meet our customers' current and future demand.

Separation of environments

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

Network Infrastructure

Robust network infrastructure is essential for reliable and secure real-time data communication between the various Varonis cloud service components. To provide sufficient capacity, Varonis' network infrastructure relies on platforms provided by Amazon AWS and other software providers. To ensure appropriate network security levels, 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. All secrets, such as tokens for connecting to customer databases, are stored in the Amazon AWS Secrets Manager. Varonis uses. Varonis has multiple security zones to differentiate services of

various sensitivities and different service principles to isolate secrets. The keys that are under Varonis' responsibility (e.g., the password for tenant databases) are periodically rotated.

The sections below describe the network and hardware infrastructure, software, and information security elements that Varonis delivers as part of the platform, database management system security, and application controls.

Data Center Security

Varonis relies on Amazon AWS's global infrastructure, including the facilities, network, hardware, and operational software, all of which support the provisioning and use of basic computing resources and storage. These facilities comply with industry standards of security and reliability, thereby enabling Varonis to provide its services in an efficient and stable manner.

Software

The Varonis application includes the following primary service components:

- Virtual machines, Kubernetes, Logging, and monitoring
- Firewall and web application firewall
- Change management tool
- Storage service
- Key management system
- Identity and security management
- Programmable communication application program interfaces (APIs) for messaging
- Database applications
- Simple Mail Transfer Protocol (SMTP) provider
- Security information and event management
- Incident management platform
- Certificate management solution
- Managing observability platform
- Domain Name System (DNS) service
- Relational and graph databases
- Automated deployment, scaling, and management of containerized applications
- Build and deploy automation
- Caching service
- Event streaming platform
- Messaging service

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

Access Control and User and Permissions Management

Varonis' users are provided with the minimal access rights required to carry out their duties (known as "least privilege" access). Employees are assigned to a specific group upon hire. Only employees 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 requests access to production, the request must be approved by the business owner for each session. Access is limited by time and then documented, logged, and monitored by the security operations center. Employees accessing Varonis DatAdvantage Cloud Platform and the corporate network are required to use a two-factor authentication mechanism and a virtual private network (VPN). Logical and physical access is revoked from resigned employees upon termination.

Customer access is authenticated in the system either by logging in with username and password or federated by the customer through the customer's identity provider, which is supported by the system.

Quality Testing

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

Data

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 company's 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.

Metadata and data classifications are uploaded for further analysis to Varonis DatAdvantage Cloud. The data is gathered and stored in protected storage for further analysis and to identify immediate or potential risks in the customer's environment. This information is easily viewed on the Varonis DatAdvantage Cloud dashboard, including any alerts that are produced. All customer data is stored and transferred in encrypted form.

People

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

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

Change Management

All changes to Varonis' services follow a structured process to ensure appropriate planning and execution. This structured process requires communication, 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 and by peers. Releases are tested by QA before deployment.

Security Testing

Various sets of security testing are performed on the cloud infrastructure and applications. Testing includes, but is not limited to, penetration testing that is performed by both an internal red team and on an annual basis by a reputable third-party vendor, vulnerability scanning, software composition scanning, code reviews, and other automated scans.

Encryption

Varonis uses Transport Level Security (TLS) to encrypt and provide integrity to all data when transmitting data over public networks. Encryption is for data at rest stored on virtual machines, databases, data backups and all other storage types. Communication between the boundaries is encrypted.

Human Resources processes

New Hire

Individuals offered a position at Varonis are subject to background checks (as appropriate for each country and taking into account local laws and regulations) as a condition to their employment in the company. In each location, employees receive data packages containing an overview of Varonis' Human Resources policies and procedures. These packages include the offer letter or employment contract, NDA, and the Varonis Code of Conduct. Employees are asked to sign their offer/employment contract to confirm that they have read these materials and agree to be bound by their terms. New hires are also required to sign a privacy addendum. If background checks are not permitted in their country of employment, they undergo a reliability test.

Performance Evaluation

Varonis has a continuous performance management process that provides feedback to employees and managers through regular 1:1 meetings and Goal Plans in HR. Varonis also has an annual performance review process in place to review accomplishments, provide constructive feedback, identify opportunities for improvement, and ensure the ongoing development of all Varonis employees. The annual performance reviews enable managers to provide ratings for the direct reports on their team, employees to provide self-evaluations, and end with a year-end conversation between the managers and employees. This process is designed to align the employee's efforts and the organization's goals.

Whistleblower Program

Varonis has an anonymous whistleblower program in place for employees to report any violation without fear of dismissal or retaliation. Reported issues are investigated and acted on in a timely manner. Information regarding how to report any violation is outlined in the Varonis Code of Business Conduct and Ethics policy.

Organizational Structure

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

Authority and Responsibilities

Lines of authority and responsibility are clearly established throughout the company. Varonis' Board of Directors meets periodically to review committee charters and corporate governance that define their roles,

responsibilities, member qualifications, meeting frequency, and other discussion topics. Minutes of the annual meetings are recorded and include the names of the participants and the date the meeting occurred.

The Board of Directors and management recognize their responsibility to foster a strong ethical environment within Varonis to determine that its business affairs are conducted with integrity and in accordance with high standards of personal and corporate conduct. This responsibility is characterized and reflected in the Varonis Code of Business Conduct and Ethics, which is distributed to all employees. Specifically, employees are prohibited from using their positions at Varonis for personal or private gain, disclosing confidential information regarding customers or taking any action that is not in the best interest of the customers. Employees' personal securities transactions are governed by a corporate policy and employee account trades are reviewed to monitor adherence to Varonis' policy. All employees are required to maintain ongoing compliance with all policies, standards, and procedures of the Code of Conduct and with lawful and ethical business practices, whether they are specifically mentioned in the Code of Conduct or not. All employees are required to affirm annually that they received, read, understand, and comply with the requirements set forth in the Code of Conduct and the Employee Handbook. Employee recertification status is monitored periodically for compliance.

Audit Committee

The Audit Committee is responsible for overseeing and monitoring the integrity of Varonis' consolidated financial statements, the company's compliance with legal and regulatory requirements as they relate to financial reporting or accounting matters, and the company's internal accounting and financial controls. The Audit Committee also oversees and monitors Varonis' independent auditor's qualifications, independence, and performance; provides the Board of Directors with the results of its monitoring and recommendations; provides the Board of Directors with the additional information and materials it deems necessary to ensure the Board of Directors is aware of significant financial matters that require the Board's attention; and oversees Varonis' internal audit function.

Communication

Varonis values transparent communication—both internally and externally. Varonis communicates with prospects, customers, and employees through several methods including, without limitation, the corporate website, which includes our privacy policy and public ways to report product flaws or security issues, a customer portal, which contains product release notes and other critical product information, and an internal employee portal which offers information about policies and procedures.

Varonis' security approach and compliance certifications are documented and communicated to customers on the Trust & Security page, in the company's agreements, and as part of the description of services provided online.

Risk Management

Varonis has developed a risk management policy that includes risk identification, analysis, communication and reporting, treatment, and monitoring. The risk management program implements a structured security plan. Each risk is evaluated by the likelihood and impact it may cause, and the treatment plan is an ongoing effort by all Varonis departments.

Enterprise Risk Management Program

The security and privacy risk management program has several levels and is conducted periodically by external and internal auditors. High-level risks are covered during the annual enterprise risk assessment performed by the internal auditor and are presented to the company's senior management. The Chief Information Security Officer (CISO) conveys cyber threats, and a mitigation plan is then decided upon and implemented.

Cyber Risk Assessments

Varonis performs routine technical risk assessments for software development, cloud production, and corporate and cloud infrastructure. Expert third-party consultants also perform ongoing assessments. The Information Security Department, led by the CISO, monitors the progress of such efforts until all substantial risks are remediated. The CISO and senior management propose remediation plans, and the security steering committees decide on the treatment plan to be adopted.

Third-Party Risk Management

Engagements with third-party suppliers undergo a security risk assessment. It is incumbent upon Varonis to ensure that vendors are capable of delivery and aware of inherent security risks. The vendor is thoroughly vetted for security and posture. We assure our customers that their data is protected and evaluate the risk by thoroughly reviewing third parties' security, compliance, and privacy practices. Whenever customer data is shared with a new third party, our customers are notified, and the vendor list is updated. High-risk third parties that hold customer data undergo periodic reviews. Each engagement with potential disclosure of PII requires a privacy assessment and signing of a Data Processing Addendum. We also require a Non- Disclosure Agreement (NDA) and security agreements.

Privacy Management

Varonis is committed to complying with all applicable data protection laws and regulations and maintaining appropriate procedures and work instructions as part of its privacy information management system. The privacy program is aligned with global privacy standards, including the EU's GDPR.

Varonis implements a privacy-by-design strategy that 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 in its agreements with its partners, subcontractors, and other relevant third parties (customers, suppliers, etc.). Varonis has a designated Data Protection Officer who guides Varonis on all data privacy concerns, risk management, and other related legal matters.

Security and Privacy Awareness Training

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

Company Information Security Policies

Varonis has established Information Security policies that ensure that its community of users are properly informed of their role and responsibilities based upon their level(s) of access to Varonis systems. This policy also defines the role of each end-user in helping to safeguard sensitive and confidential information systems from internal and external threats.

These policies include:

- Acceptable use of assets
- Access control
- Asset management
- Backup and restore
- Business continuity
- Change management
- Cloud security
- Compliance
- Cryptography
- Data classification
- Data disposal
- Endpoint security
- Human Resources security
- Incident response

- Information security awareness, education, and training
- Information transfer
- Logging and monitoring
- Mobile device management
- Network security
- Passwords
- Physical and environmental security
- Privacy management
- Records retention and data disposal
- Risk management
- Secure software development lifecycle
- Supplier relationships
- Teleworking and remote access
- Vulnerability and Threat management

Availability Procedures

High availability eliminates single points of failure to ensure continuous operations and extended uptime. Load balancing is used to distribute traffic across multiple servers. High availability and load balanced arrays are in place for production systems to help mitigate the effect of a system error. Additionally, Varonis implemented a web application firewall to protect against denial-of-service attacks and reduce the risk of web application threats.

Business Continuity Plan

Varonis' Business Continuity Plan outlines measures to avoid disruptions to customers and partners. The plan 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, including systems, suppliers, and users. The Business Continuity Plan also includes the following topics:

- DatAdvantage Cloud production infrastructure
- Corporate infrastructure
- Critical suppliers
- Cyber incident response
- Pandemic preparedness

Backup

The database and storage are hosted on Amazon AWS. A daily backup is performed using an automated application. In case of failure, a notification is sent to the operations team. Production databases utilize AWS availability zone capabilities. Additionally, a complete replica is stored at a separate region.

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. Furthermore, the plan includes roles and responsibilities, and the communication process for stakeholders at each phase.

Asset Management

Company assets are tracked and managed throughout the asset lifecycle. Each asset has an owner assigned to it, 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.

Endpoint Security

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

Monitoring

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

Principal Service Commitment and System Requirements

Varonis' commitments to customers include security, confidentiality, availability, and privacy. Commitments are communicated and documented within agreements, the Trust & Security page, and as part of the supplier relationship process. Our commitments to our customers include, but are 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.
- Controlled physical, logical, and remote access to sensitive information 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 in transmission over public networks. Encryption is also enabled on databases, data at rest, data backups, and communication between segmented boundaries.
- Network segregation to enforce separation between production, staging, testing, and other cloud-based and internal infrastructure environments.
- Minimum standards of security for the development, provision, and use of Varonis cloud services require that the security, confidentiality, availability, and privacy of assets within Varonis cloud services are protected. Risks to the services and to customers are subject to a risk assessment and to the application of suitable technical and organizational controls.
- Data centers that host, store, and/or process customer production data must comply with industry best practices. This includes protecting information system equipment and cabling, entrance controlled by access card, surveillance cameras, providing emergency power, shutoff, lighting, fire alarms, protection from water and fire, and maintaining temperature and humidity controls.
- A retention policy that complies with applicable legal, regulatory, and contractual requirements. This includes deleting customer data upon request or automatically based on lifecycle policies that are communicated to the customer.
- The Human Resources department (HR) ensures successful operations and delivery of effective security controls. This includes implementing security measures prior to employment, during employment, at termination, and as otherwise required during any other changes in employment status, as well as providing ongoing cybersecurity awareness training to the company's employees.
- Backup procedures designed to ensure the continued availability and accessibility of information and to minimize the cost of a disruption (e.g., operational error, disaster, or sabotage that causes damage to, or destruction of, information).
- Maintaining a service level agreement (SLA) between Varonis and its customers wherein Varonis' responsibilities and the customer's cooperation requirements are specified. Within such SLA, Varonis upholds certain obligations regarding the availability of its service, and maintaining support levels, depending on the severity of the error.

- Implementing privacy by design within the systems and processes, which is intended to minimize risks to privacy rights and to process personally identifiable information (PII), in keeping with regulatory requirements.
- An established business continuity and disaster recovery plan that provides an overview of the activities necessary to coordinate the recovery of critical business customer functions and managing and supporting recovery in the event of a disruption or disaster.