Varonis

Varonis SaaS Data Security Platform

ISAE 3000 (SOC 3)

Service Auditor’s Assurance Report

For the period

August 1, 2023, to July 31, 2024

Contents

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 I - Management Assertion Provided by Varonis

We, as management of, Varonis ("the Company") are responsible for:

- Identifying the Varonis SaaS Platform ("the system") and describing the boundaries of the system.
- Identifying our principal service commitments and system requirements.
- Identifying the risks that would threaten the achievement of the principal service commitments and service requirements that are the objectives of our system.
- Identifying, designing, implementing, operating, and monitoring effective controls over the Varonis platform (system), to mitigate risks that threaten the achievement of the principal service commitments and system requirements.
- Selecting the trust services categories that are the basis of our assertion.

We assert that the controls over the system were effective throughout the period August 1, 2023, to July 31, 2024, to provide reasonable assurance that the principal service commitments and system requirements were achieved, based on the criteria relevant to security, availability and confidentiality set forth in the AICPA's TSP Section 100 2017 Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016).

Varonis Inc

August 19, 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

Section II – Independent Service Auditor's Report

To the Management and board of directors of Varonis:

We have examined management's assertion that Varonis, during the period August 1, 2023, to July 31, 2024, maintained effective controls to provide reasonable assurance that:

- The System was protected against unauthorized access, use, or modification
- The System was available for operation and use, as committed or agreed
- Information within the System designated as confidential is protected as committed or agreed

Based on the criteria for security, availability, and confidentiality in the American Institute of Certified Public Accountants' TSP Section 100 (2017), Trust Services Principles and Criteria, for Security, Availability, Processing Integrity, Confidentiality, and Privacy. This assertion is the responsibility of Varonis' management. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included:

(1) Obtaining an understanding of Varonis ' relevant to security, availability, confidentiality, and Privacy controls.

(2) Testing and evaluating the operating effectiveness of the controls.

(3) Performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Because of inherent limitations in controls, error or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that the validity of such conclusions may be altered because of changes made to the system or controls, the failure to make needed changes to the system or controls or a deterioration in the degree of effectiveness of the controls.

In our opinion, Varonis management's assertion referred to above is fairly stated, in all material respects, based on the mentioned criteria for security, availability and confidentiality.

Yours faithfully,

KPMG

Tel Aviv, Israel

August 19, 2024

Section III - Description of Varonis SaaS Data Security Platform

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.

Description of the Services Provided

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

- **Detecting insider threats and cyberattacks** Varonis provides behavior-based threat detection that uses machine learning to alert on abnormal user or device behavior. Additionally, Varonis provides a live-updating library of pre-built threat models based on attack techniques and vulnerabilities used by real-world adversaries.
- **Pinpointing data exposure**: Varonis 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 safely automates permissions changes to eliminate unnecessary access and drastically reduce the damage from insider threats and cyberattacks.
- **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.

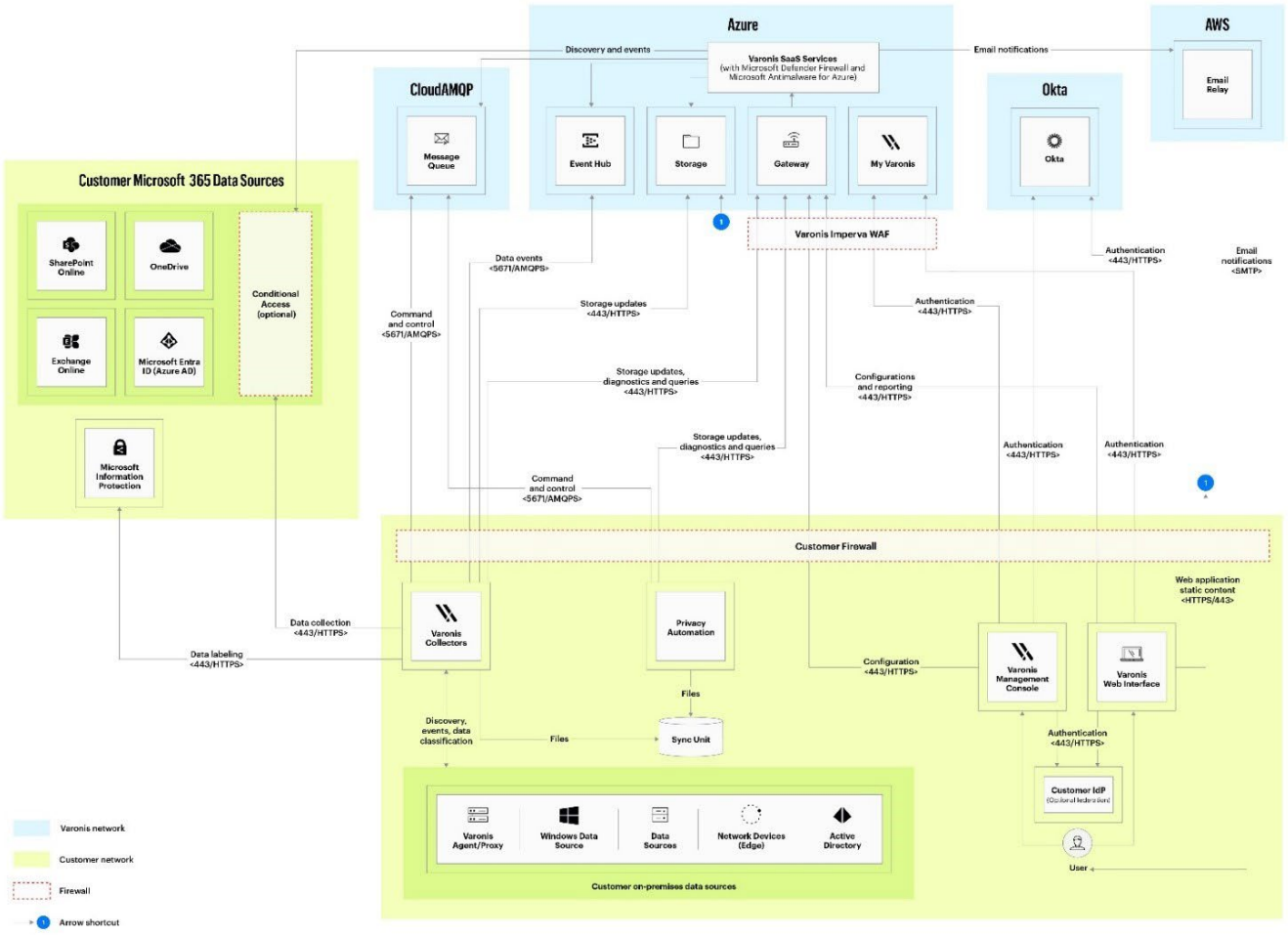
Infrastructure

Varonis' Software as a Service (SaaS) infrastructure is deployed on Microsoft Azure (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 Azure 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' SaaS infrastructure is implemented in Microsoft Azure and uses Okta as the identity provider for customer access and service level agreement authentication. The Varonis solution leverages the capabilities, resilience, and reliability of Microsoft Azure to scale quickly and securely to meet our customers' current and future demands.



Varonis monitors various platforms such as NetApp and Windows as seen in the diagram above. A Varonis Collector server installed on-premises is responsible for

- Monitoring those platforms gathering events and telemetries
- Collecting and auditing user activity events and file server metadata
- Classifying file contents using rule packs that Varonis provides
- Securely sending data to the cloud for analysis and processing
- Publishing DatAlert alerts

Varonis' Deployment Hub is responsible for all on-premises deployment flows. Varonis' SaaS user interface comprises the following applications:

- Varonis Management Console - for environment configuration
- Varonis Web Interface - for query and data analysis

Secured ports are used for both the Varonis Collector and the Deployment Hub when transferring data internally and externally.

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 Varonis cloud service components. To provide sufficient capacity, Varonis' network infrastructure relies on platforms provided by Microsoft Azure 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 Microsoft Azure key vault. Varonis uses Azure-managed identities to perform periodic security principal password rotation. 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 Microsoft Azure'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, Service Fabric, and batch for online and batch processing
- Message broker
- Logging and monitoring
- Firewall and web application firewall
- Change management
- Blob 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
- Certificate management solution

- Managing observability platform
- Domain Name System (DNS) service
- Event hubs
- Structured Query Language (SQL) Server

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, Microsoft Azure, 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. 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 SaaS 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 an applicable user-assigned ID or federated by the customer or 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

Varonis differentiates between data and metadata:

1. Customer metadata includes user IDs and names, group names, folder and file names, email subjects, domains, and IP addresses that user's access.

2. Customer data includes both file and email contents. All customer metadata is classified as "confidential" per the Varonis Global Classification Policy. Customer data is securely stored and monitored to identify immediate or potential risks within the customer's environment.

Varonis technology crawls data sources, classifying customer data. Customer data is then retrieved and processed by the Collector servers installed inside the customer network only. Varonis SaaS Data Security Platform does not store customer data in the cloud*.

Metadata and data classifications are uploaded into SaaS for further customer use. 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, including any alerts that are produced, is easily viewed on the Varonis SaaS dashboard. All customer metadata is always stored and transferred in encrypted form.

*Customers could enable the optional "File Analysis" role in the cloud, which allows customer users with an approved File

Analysis role to retrieve specific files via SaaS. without storing them.

People

The Varonis employees involved in the development, operation, security, or support of the Varonis SaaS 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 or by peers. Releases are tested by QA before deployment.

Varonis assigns customers to different "rings" so that software and configuration changes are gradually phased into production, one ring at a time; there is a delay between each ring release, thus minimizing impact in case of incorrect changes.

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

Hew Hire

Individuals offered a position at Varonis are subject to background checks (as appropriate for each country and considering 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 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 and their immediate families 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 Trust & Security, 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 (see security testing for more information). 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 which limits the scope and scale of data collection and processing only to the minimum extend required, to limit risks to sensitive data. All personally identifiable information (PII) is collected and maintained for specifically stated purposes only.

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 Policies

- Acceptable-Use of Assets
- Access Control
- Asset Management
- Backup and Restore
- Business Continuity
- Change Management
- Secure System Hardening
- Cloud Security
- Legal 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:

- Corporate infrastructure
- Critical suppliers
- Cyber incident response
- Pandemic preparedness

Backup

The database and storage are hosted on Microsoft Azure. A daily backup is performed using an automated application. In case of failure, a notification is sent to the operations team. Production databases utilize Azure 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.