Varonis

Varonis SaaS Data Security Platform

SOC 3

Service Auditor’s Assurance Report

For the period

October 1, 2024, to September 30, 2025

Contents

KPMG

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 – Independent Service Auditor's Report

We have examined management's assertion that Varonis, during the period October 1, 2024, to September 30, 2025, 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 (with Revised Points of Focus – 2022). 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 criteria mentioned for security, availability and confidentiality.

Yours faithfully,

KPMG Somekh Chaikin

Somekh Chaikin

KPMG

Tel Aviv, Israel

December 21, 2025

Section II - Management Assertion Provided by Varonis

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

- Identifying the Varonis SaaS Data Security 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 October 1, 2024 to September 30, 2025, 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 (with Revised Points of Focus – 2022).

December 21, 2025

Section III - Description of Varonis SaaS 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 (Nasdaq: VRNS) is the leader in data security, fighting a different battle than conventional cybersecurity companies. Our cloud-native Data Security Platform continuously discovers and classifies critical data, removes exposures, and detects advanced threats with AI-powered automation.

Thousands of organizations worldwide trust Varonis to defend their data wherever it lives — across SaaS, IaaS, and hybrid cloud environments. Customers use Varonis to automate a wide range of security outcomes, including data security posture management (DSPM), data classification, data access governance (DAG), data detection and response (DDR), data loss prevention (DLP), database activity monitoring (DAM), identity protection, email security, and AI security.

Description of the Services Provided

Varonis SaaS is 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 on 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.

Principal Service Commitment and System Requirements

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

The organization's cloud infrastructure is deployed on Microsoft Azure (utilizing both SaaS and PaaS solutions) for hosting and operating the production, staging, and development environments. Varonis' commitment, to customers and other third parties, includes security, confidentiality, and availability. This is communicated and documented as part of the supplier relationship process. Our commitment for 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 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.

- 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. Cloud services provided, and risks to the services and customers are subject to risk assessment and application of suitable technical and organizational controls.

- Data centers which host, store, and/or process customer data comply with industry's best practices. This includes protecting information system equipment and cabling, entrance 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.

- 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, termination and any other changes in employment, as well as ongoing cybersecurity awareness training.

- 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).

- Maintaining contractual agreement between Varonis and customer wherein the customer requirements are specified, and Varonis states the level of service responsibilities and guarantees regarding availability, performance, handling of availability incidents and support levels.

- Implementing privacy by design within the systems and processes in such a way as to minimize risks to privacy and aims to process personally identifiable information (PII) in line with regulatory requirements.

Organizational Structure

Varonis has an established organization 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.

Functional areas of operations are listed below:

- **Executive Management** – Responsible for overseeing company-wide initiatives and activities, establishing, and accomplishing goals, overseeing objectives, and ensuring appropriate resource levels are available to meet business objectives.

- **DevOps** – Responsible for a diverse Varonis SaaS Data Security Platform environment. Design and development of DevOps tools and features, CI\CD pipelines and automation processes for configuration, deployment, monitoring, and maintenance of complex cloud environments.

- **Product Management (PM)** – Responsible for product planning and execution throughout the product life cycle. The PM gathers and prioritizes product requirements by conducting market research supported by visits and interaction with customers, prospects, and partners, as well as perform analyzes market trends and competitive landscape.

- **Information Security** – Provides leadership in developing, reviewing, and recommending direction for the Information Security Policy, Standards, and Guidelines, as well as responsible for the security monitoring, architecture, testing, governance, risk, and compliance.

- **Security Operations Center (SOC) team** – Part of the global Information Security team, and responsible for monitoring systems and investigating cybersecurity incidents, as well as developing operational playbooks and suggesting alert enhancements to improve threat detection capabilities.

- **Product Security** – Responsible for the secure software development lifecycle, secure design, security testing, and the security of the cloud-based production environment.

- **Human Resources** – Responsible for HR policies, practices, and processes including but not limited to talent acquisition, recruitment, Employee on boarding, Training and development, benefits, compensation, resignation process, and performance review.

- **Support** – Managing, monitoring, and supporting users for the cloud services environment.

- **Software Engineers** – Responsible for programming high-performance core applications, which are responsible to collect and move large amounts of data. Design, features, and modules of ownership in all aspects.

- **Architecture Team** – Responsible for designing software systems aligned with industry best practices and ensures that the threat model for the software and services is conducted and mitigated.

- **Internal Audit** – Independent, objective assurance and consulting activities designed to add value and improve an organization's operations. The team supports the organization to accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

Description of the Control Environment, Information Communication, Monitoring and Risk Management Process

A company’s internal control is a process – affected by the entity's boards of directors, management, and other personnel – designed to enable the achievement of objectives in the following categories: (a) reliability of Product Development, (b) effectiveness and efficiency of operations, and (c) compliance with applicable laws and regulations. The following section is a description of the components of internal control for Varonis.

Control Environment

The control environment sets the tone of an organization, influencing the control consciousness of its employees. It reflects the overall attitude, awareness, and actions of management and others concerning the importance of controls and the emphasis given to controls in the entity’s policies, procedures, methods, and organizational structure. Varonis executive management recognizes its responsibility for directing and controlling operations and for establishing, communicating, and monitoring control policies and procedures. Policy and procedures documents for significant processes that address system requirements and relevant updates are available on the internal shared drive.

Authority and Responsibility

Lines of authority and responsibility are clearly established throughout. The Varonis’ Board of Directors (the “Board”) meets periodically to review committee charters and corporate governance, which define their roles, responsibilities, member qualifications, meeting frequency, and other discussion topics. Meeting minutes of the annual meetings are recorded, which include participants and date the meeting occurred.

Each member of the Board possesses adequate, relevant experience, and is recognized as an individual of high integrity and good stature. The Board is actively involved in and scrutinizes the activities of Varonis’ functional groups and acts with respect to its fiduciary responsibilities. The Board is responsible for overseeing Varonis' corporate governance and has discretion to delegate a broad range of powers and decisions to the Management Committee to manage the entity and its daily business.

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

Management Philosophy and Operating Style

The control environment at Varonis entails the involvement and ongoing engagement of Executive and Senior Management (Management Team), chaired by the Chief Executive Officer ("CEO"), who has been delegated by the Board the responsibility to manage Varonis and its daily business. In its role, the Management Team assigns authority and responsibility for operating activities and establishes reporting relationships and authorization hierarchies. The Management Team designs policies and communications so that personnel understand Varonis' objectives, know how their individual actions interrelate and contribute to those objectives and recognize how and for what they will be held accountable. Communication exists between Executive and Senior Management so that both have information needed to fulfill their roles.

Integrity and Ethical values

Integrity and ethical values are essential elements of the control environment, affecting the design, administration, and monitoring of key processes. Integrity and ethical behavior are the products of Varonis' ethical and behavioral standards, how they are communicated, and how they are monitored and enforced in its business activities. They include management's actions to remove or reduce incentives/pressures, and opportunities that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of the entity's values and behavioral standards to personnel through policy statements and codes of conduct, and by the examples the executives set.

The Board 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 (the "Code of Conduct"), which is distributed to all employees. Specifically, employees and their immediate families are prohibited from using their positions with Varonis for personal or private gain, disclosing confidential information regarding clients, or taking any action that is not in the best interest of clients. Employees' personal securities transactions are governed by 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. Each employee is required to affirm periodically that he or she received, read, understood, and complied with the requirements set forth in the Code of Conduct and the Employee Handbook. Employee recertification status is monitored periodically for compliance.

Whistleblower program

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

Commitment to Competence

Varonis management defines competence as the necessary knowledge and skills required by employees to fulfil and accomplish tasks that define their roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for jobs and how those levels translate into the requisite skills and knowledge.

Accountability

Varonis employees and contractors are accountable for understanding and adhering to the guidance contained in the Security Policies, and any applicable supporting procedures.

Control Activities

Control activities are the policies and procedures that enable management directives to be conducted to address risks to the achievement of the entity's objectives. Varonis operating and functional units are required to implement control activities that help achieve business objectives associated with the reliability of financial reporting, the effectiveness and efficiency of operations, and compliance with applicable laws and regulations.

The controls activities are designed to address specific risks associated with Varonis operations and are reviewed as part of the risk assessment process. Varonis has developed formal policies and procedures covering various operational matters to document the requirements for performance of control activities. Controls are in place to put the policies into action in a timely manner. Competent personnel with sufficient authority perform the control activities with diligence and continuing focus. Policies and procedures are documented, reviewed, and approved on an annual basis by the management team and available to Varonis' employees within the Varonis internal portal. In addition, Responsibility, and accountability for developing and maintaining the policies are assigned to the relevant personnel and approved on an annual basis by the management team.

Information and Communication

Information and communication are integral components of Varonis' internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, information technology. At Varonis, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

The Varonis Community Portal offers detailed product information. Varonis' customers may access detailed service plans in the Community Portal.

Internally, Varonis offers their employees several methods for communication. All policies and procedures are available via the internal employee portal. Employees are informed regularly of service updates, delays as well as new products and services once they are made available.

With communication being critical to the provision of cloud services, Varonis ensures that customers are informed of information in a timely manner. This includes information about changes to services or availability, and security incidents relating to either their services or their account. Methods of communication with Cloud service customers are set out in contracts.

To support this, Varonis provides customers with key information before agreeing to contracts, during the exchange of contracts and throughout the lifecycle of the relationship. Availability of the SaaS Data Security Platform, including status and uptime, is published on the customer-facing website for customers. Varonis also established a Privacy Policy which discloses its confidentiality practices for customer data. The privacy policy is available on Varonis website to all customers. Customers are notified of material updates to the privacy policy.

Varonis communicates its commitment that security is a top priority for its customers and Varonis internal users through Varonis' portal. In addition, customers and Varonis internal users are offered multiple methods for contacting Varonis. Customers and internal users can contact Varonis via various methods to report issues on bugs, defects, availability, security, confidentiality, and privacy.

Varonis also communicates security, availability, confidentiality and privacy principles to the internal users through the on-boarding process and policies and procedures available on the internal website and shared folders. Varonis communicates commitments of security, availability, confidentiality and privacy principles to external audience via Trust & Security | Varonis.

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 following security policies apply to everyone, and enhance Varonis' security posture:

- Acceptable Use of Assets
- Asset Management
- Backup and Restore
- Business Continuity
- Change Management
- Secure System Hardening
- Cloud Security
- Compliance
- Cryptography
- Data Classification
- Data Disposal
- Endpoint Security
- Human Resources Security
- Identity and Access Management
- 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

Varonis is committed to and conducts its business activities lawfully and in a manner that is consistent with its compliance obligations. This includes legislative obligations, regulations, security standards, intellectual property rights, protection of records, independent review of information security, compliance with security policies and standards, contractual requirements, applicable privacy regulations industry codes and standards, as well as Varonis internal policies, standards, and procedures.

Risk Management

Varonis has 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. Company-wide risks are covered during the semi-annual enterprise risk assessment, performed by the Internal Auditor, and presented to senior management and the Audit Committee of the Board of Directors. As part of the risk management program, mitigation activities to reduce the risk levels are reviewed. The CISO conveys cyberthreats, and a mitigation plan is decided and followed.

Cyber Risk Assessments

Varonis perform regular technical risk assessments for software development, Varonis SaaS Data Security Platform, and corporate and cloud infrastructure (more details in the 'Security Testing' section). 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 the treatment plan.

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 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, 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 mutual Data Processing Addendum. We also require an NDA and security agreements.

Components of the Varonis SaaS Data Security Platform

Infrastructure

Varonis SaaS services utilize Microsoft Azure for cloud operations. The cloud platform is deployed in multiple Azure regions across the world (specifically East US 2, West Europe, Australia East, US South and Canada Central) Varonis provides software installations of Collector services, which the customer installs on its servers inside its data center.

System Boundaries

The Varonis SaaS infrastructure is deployed on Microsoft Azure (utilizing both SaaS and PaaS solutions) for hosting and operating the production, staging, and development environments. Varonis leverages the experience, resilience, and reliability of Microsoft Azure to scale quickly and securely to meet our current and future demands.

Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the system. Varonis SaaS Data Security Platform monitors various platforms, such as NetApp and Windows, as seen in the diagram below.

A Varonis Collector server installed on the customer's premises is responsible for:

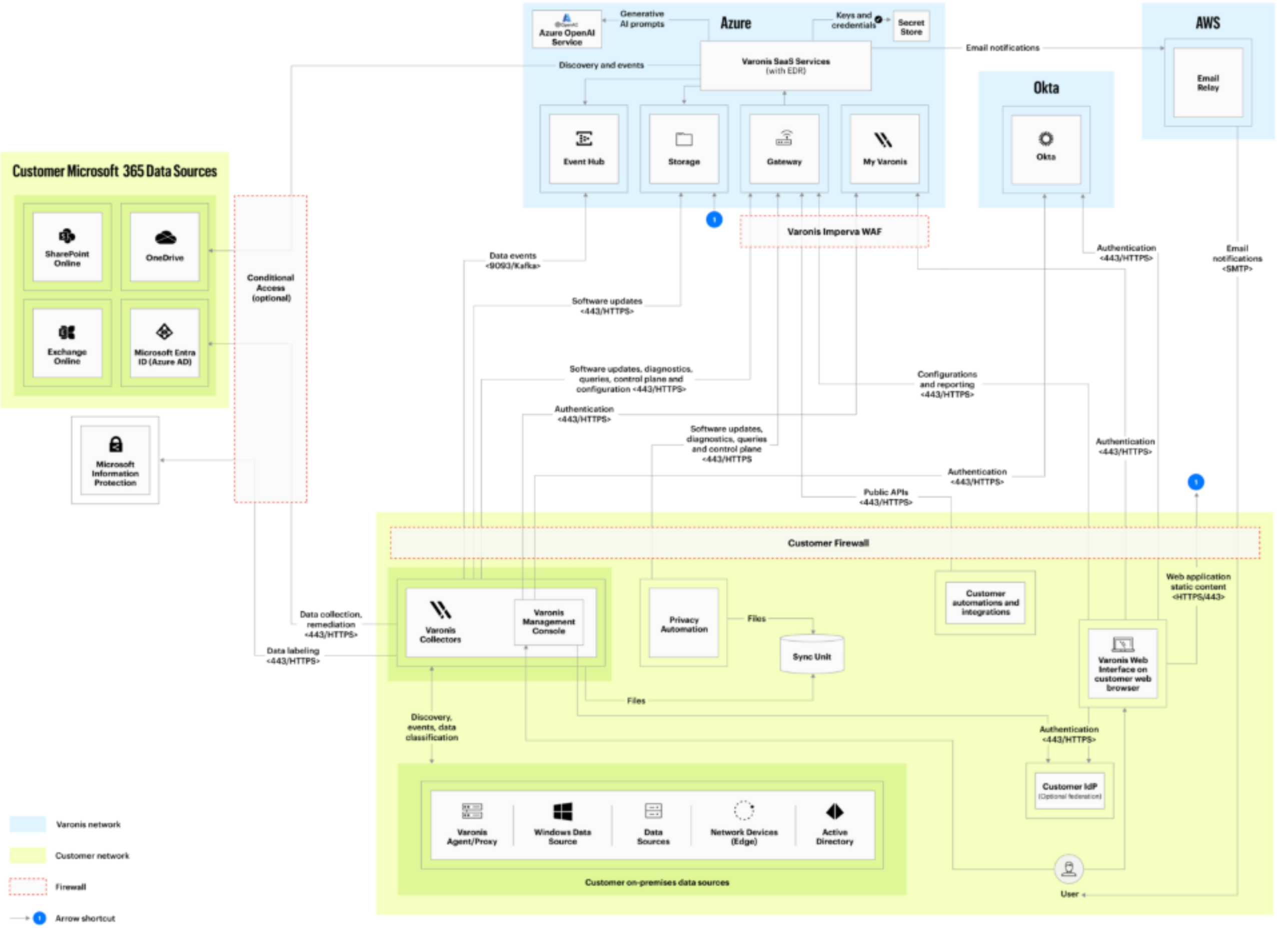
- Monitoring those platforms, gathering events, and telemetries
- Collecting and auditing user activity events and file server metadata
- Classifying files contents using rule packs that Varonis SaaS Data Security Platform provides
- Securely sending data to the cloud for analysis and processing
- Publishing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

Varonis Deployment Hub – Responsible for all on-premises deployment flows.

Varonis SaaS UI – Comprises the following applications:

- Varonis Management Console –For environment configuration.
- Varonis Web Interface –For query and data analysis.

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


Azure
Azure OpenAI Service
Generative AI prompts
Keys and credentials
Secret Store
Discovery and events
Varonis SaaS Services (with EDR)
Email notifications
AWS
Email Relay
Okta
Okta
Event Hub
Storage
Gateway
My Varonis
1
Varonis Imperva WAF
Customer Microsoft 365 Data Sources
SharePoint Online
OneDrive
Exchange Online
Microsoft Entra ID (Azure AD)
Conditional Access (optional)
Microsoft Information Protection
Data events <9093/Kafka>
Software updates <443/HTTPS>
Software updates, diagnostics, queries, control plane and configuration <443/HTTPS>
Authentication <443/HTTPS>
Software updates, diagnostics, queries and control plane <443/HTTPS
Configurations and reporting <443/HTTPS>
Authentication <443/HTTPS>
Authentication <443/HTTPS>
Authentication <443/HTTPS>
Email notifications <SMTP>
Public APIs <443/HTTPS>
1
Customer Firewall
Data collection, remediation <443/HTTPS>
Data labeling <443/HTTPS>
Varonis Collectors
Varonis Management Console
Privacy Automation
Files
Sync Unit
Files
Customer automations and integrations
Web application static content <HTTPS/443>
Varonis Web Interface on customer web browser
Discovery, events, data classification
Authentication <443/HTTPS>
Customer IdP (Optional federation)
Varonis Agent/Proxy
Windows Data Source
Data Sources
Network Devices (Edge)
Active Directory
Customer on-premises data sources
User
Varonis network
Customer network
Firewall
1
Arrow shortcut

Infrastructure and Software

Varonis SaaS Security Platform Application	Business Function
Azure Active Directory (Entra ID)	Azure identity and security management
Azure Service Fabric, functions, and batch	Azure virtual machines, Service Fabric, and batch for online and batch processing
Azure DNS	Name resolution service
Azure Storage	Azure Table, Azure Blob storage for event processing and data lake
Azure Monitoring and Grafana	Managing observability platform
Azure Event Hubs	Microsoft streaming platform to pass events from the on-prem part to the cloud
Azure Data Explorer (ADX)	Data ingestion and analysis service

Azure DevOps Pipelines and Repos, Terraform	CI/CD platform
Azure SQL	Managed SQL DB
Azure Firewall	Cloud-native network firewall
Azure Sentinel	Security information and event management system that provides real-time analysis of security alerts
Azure Defender	Security protection for Azure workloads
Azure Kubernetes Services	Running computer containers
Azure Data Bricks	Service for big data processing
Azure App Containers	Web Application hosting
Azure Service Bus	Azure Queuing system
Azure DevOps – For MDDR	Used as a ticketing system for Managed Data Detection and Response Service

Third-Party Cloud Services

Varonis SaaS relies on third-party services as part of its operations.

Varonis SaaS Security Platform Application	Business Function
Grafana	Monitoring of Varonis SaaS Platform
Imperva Web Application Firewall	Protects web applications by monitoring, filtering, and blocking traffic to and from a web service
Tenable	Cloud infrastructure vulnerability management, scans for internal and external network and web application vulnerabilities
Okta	Identity management solution
Let's Encrypt CA and Amazon Cert services	Certificate management solution
AWS SES	SMTP provider
Azure Open AI	AI model hosting and inference

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.

Data Processing

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

Data processing is completely isolated from the Varonis corporate network. Access is restricted only to the required employees, who must authenticate with multifactor authentication (MFA). Access is achieved under strict monitoring and auditing.

Description of the Information Systems Controls

Separation of Environments

All secrets, such as tokens for connecting to customer databases, are stored in an Azure Key Vault. 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.

Employee access to the Varonis SaaS Data Security Platform is restricted and fully audited and is only allowed on-demand to certain employees for a short period of time with manager approval, as described in the Access Authentication and Authorization section.

The Varonis SaaS Data Security Platform is completely separated from the staging and development environments with separate access control and a segmented network. Logical segregation is performed for each customer’s data and tenant. Separation is also performed between Varonis’ internal administration and resources used by customers.

Access Authentication and Authorization

Varonis has established and follows specific access control practices to protect information and information systems from unauthorized access, modification, disclosure, or destruction. Access to Varonis information systems is controlled by a centralized authentication, authorization, and accounting system. All staff are given network access in accordance with business access control procedures and requirements for access as defined by their roles.

A formal user registration and deregistration procedure for granting and revoking access to all information systems and services has been developed. The procedure includes an onboarding procedure and a procedure for terminating an employee's access, as part of the employee termination process.

Users are assigned to groups. When a user from that group requests access to the Varonis SaaS Data Security Platform, the request requires justification and needs to be approved by the business owner for each session. Access is limited by time, and is documented, logged, and monitored by the SOC.

Physical access to Varonis' facilities is granted by the authority of the facility manager and applied on a strict need-to-know basis.

Authentication

Individuals are positively authenticated and authorized before being granted access to any Varonis information and information assets. Varonis personnel access the corporate and Varonis SaaS Data Security Platform networks using a virtual private network (VPN). Remote access sessions also require two-factor authentication. Separate accounts are used for personal, corporate, and production functions.

Authorization

No account is granted access unless the account holders and their access has been approved. Access is based on the individual's roles and responsibilities and is limited to the minimum access right necessary to perform an assigned job function (the principles of least privilege and need-to-know).

Access is reviewed on a quarterly basis and approved by the business owners to ensure that the level of access is current, necessary, and appropriate. Such access reviews are documented.

Varonis SaaS Data Security Platform Access

Access to cloud production is limited based on the principles described in the sections above. The access is approved by request, is regularly monitored by Varonis' Security Operations, and is restricted to a minimal number of users.

Customer Access

Customer employees authenticate cloud services through the Internet using the TLS functionality of their web browser, federated by the customer, or federated through the customer identity provider supported by the system. Customer employees must supply a valid user ID and password to gain access to customer cloud resources. Passwords must conform to password configuration requirements configured on the virtual devices using the virtual server administration account.

Password Policy

Passwords must conform to defined password standards and are enforced through parameter settings in their identity provider. These settings are part of the configuration standards and force users to change passwords at a defined interval, disable the user ID's ability to access the system and components after a specified number of unsuccessful access attempts, and mask workstation screens, requiring reentry of the user ID and password after a period of inactivity. Accounts are forced to change passwords upon initial sign-on.

Privileged Access

Privileged user accounts are strictly controlled. Their use is logged, monitored, approved, and regularly reviewed. The use of group identities is only permitted where they are suitable for the work carried out (e.g., service accounts).

Encryption

Data is encrypted at rest and in transit. Varonis uses strong ciphers with longer keys and FIPS-compliant ciphers where possible. Used ciphers and algorithms are regularly monitored to ensure deprecated versions are not used.

- Data at rest - Databases and Virtual machines are encrypted at rest.
- Data in transit sent over public networks and internally within the Varonis SaaS is encrypted using TLS Service-to-Service communication within boundaries is also encrypted using TLS.

Network Security

Network security controls are implemented to ensure the isolation of different zones and prevent unauthorized attempts to penetrate Varonis' internal cloud security infrastructure. Similar controls are also in place for third-party cloud service vendors. The Varonis SaaS environment is also protected by a web application firewall.

Security Testing

Varonis conducts rigorous security testing using various tools, techniques, and methods.

- A security design review is conducted for features involving security aspects.
- Changes are tested in an isolated and controlled environment prior to implementation to minimize the effect on the relevant business process, to assess its impact on operations and security, and to verify that only intended and approved changes were made. A peer programmer, who is not responsible for the change, conducts a code review on each change. Once the code review has been completed, the change is submitted to Quality Assurance (QA) for testing.
- Development changes are tested based on documented test plans, which are developed by a Business Analyst and/or Quality Assurance personnel.
- Assessment and remediation (according to the policy) are conducted on third-party, open-source, and other components identified as vulnerable.
- Automated security tests are continuously run as part of the CI/CD process.
- External and internal penetration testing is conducted on the software solution, including the OWASP Top 10 controls, at least once a year, or prior to any major version release.
- Functional security testing in the QA phase (manual or automated) that covers the designed controls and aligns with the application security verification processes (ASVS).
- Automated network and application vulnerability testing is conducted by third-party vendor software.
- Automated and manual reviews of product logs and telemetries are conducted to detect functional and security issues.

Vulnerability Scanning and Monitoring

Varonis SaaS is periodically scanned for vulnerabilities by the following solutions:

1. Vulnerability management software
2. Software Composition Analysis (SCA) tool to detect components with found vulnerabilities
3. Dynamic Application Testing (DAST) tool

Findings are handled according to a well-defined SLA, which is in line with industry's best practices and standards.

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 lifetime, they are securely destroyed to ensure that data is not recoverable.

Secure Software Development Cycle (SSDLC)

Varonis is committed to information security at every level of the organization. It is based on industry-leading best practices and adopts a thorough secured software development lifecycle policy (SSDLC).

Our policy includes:

1. SCA—Software composition scanning for vulnerable components.
2. Security design and threat modeling reviews.
3. Secured code reviews—Performed by developers to detect and remediate possible security issues.
4. Secured development training—Performed annually for most developers in R&D.
5. Automated security testing—Part of the CI/CD process.
6. Security vulnerability handling procedure and SLA.
7. Periodic internal penetration testing—Performed by security experts.
8. Periodic external penetration testing—Performed by an external certified company.
9. Identification and tracking of application security issues and threat mapping and developing appropriate mitigations.
10. Each new feature goes through security architecture review, which includes threat mapping. Applicable controls are included in the feature design and development.

Software Testing and Validation Process

Varonis has an established Secure Software Development Lifecycle (SSDLC) process. The Varonis SaaS Data Security Platform applies both automatic and manual validation and quality assurance (QA) from the early stages of development. Each code change must first pass code review. Then, automatic tests are performed on the code change: Each change passes unit testing and component testing. Then a set of automatic system tests are run to verify all major flows are functioning well. In addition, functionality is constantly tested manually where automation does not exist. Once all relevant tests pass (automatic and manual), there is another round of end-to-end (E2E) testing on the overall system to verify and approve deployment to production.

Change Management

Software development and change management at Varonis include development and production changes to Varonis SaaS solutions.

Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are documented and approved by the management team within the change management solution.

Varonis’ management establishes direction and high-level objectives for change management and control. By implementing a defined change management process and policy, Varonis demonstrates increased agility in responding predictably and reliably to new business demands. The process ensures that proposed changes are reviewed, authorized, evaluated, and released in a controlled manner, and that the status of each proposed change is monitored. To fulfill this, the processes below are followed:

1. **Risk Management**—Risks related to changes are evaluated before the change is made. Proper precautions are taken to reduce the probability of the related risks.

2. **Approval**—All changes are approved by the business owner prior to production. Approval of changes is based on formal acceptance criteria, i.e., the change request was made by an authorized user, the impact assessment was performed, and the proposed changes were evaluated.
3. **Testing**—Where technically possible, changes are tested in an isolated and controlled environment prior to implementation to minimize the effect on the relevant business process, to assess its impact on operations and security, and to verify that only the intended and approved changes were made. The testing includes peer review.
4. **Implementation**—Deployment is only undertaken after appropriate testing and approval by stakeholders.
5. **Roll back**—Where applicable, procedures for aborting and recovering from unsuccessful changes are documented.

Change Documentation

The change control process is formally defined and documented. At a minimum, the change control documentation includes the following:

- Submission date
- Start date and end date
- Description of the change
- Change requester
- Change urgency
- Impacted components
- Change approvers
- Change implementer
- Change status

Emergency Changes

An emergency change is usually a response to an outage or failure that needs an urgent fix. Due to the nature and urgency of these emergency changes, documentation of such changes can be done after the change has already been made. Emergency changes still require business owner approval prior to implementation.

Change Monitoring

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 alignment of automation tools where appropriate.

The changes are monitored once they are rolled out to the production environment. Deviations from design specifications and test results are documented and escalated to the solution owner for verification.

Human Resource Policies and Procedures

Human resource (HR) policies and practices relate to hiring, onboarding, orienting, training, evaluating, counseling, promoting and compensating employees, and termination procedures. The competence and integrity of employees are essential elements of controlling the environment. The organization's ability to recruit and retain enough competent and responsible employees is dependent to a great extent on its HR policies and processes.

The HR policies and processes of Varonis are designed to: identify and hire competent employees, provide employees with the training and information they need to perform their jobs, evaluate the performance of employees to verify their ability to perform job assignments, and through performance evaluation, identify opportunities for growth and job performance improvement.

Formal written job descriptions are developed and maintained for each position. Each job description is reviewed and updated as needed by a manager responsible for overseeing employees with that description. Changes to formal written job descriptions are submitted to HR for review and approval. Formal written job descriptions are also prepared for contractors who work under the direct supervision of Varonis' management.

Occupational descriptions clearly articulate the job qualifications, required degrees/certifications, responsibilities, and placement in the chain of command with respect to supervisors and subordinates. Varonis' Human Resource (HR) department plays a key role in the development of its information security program by staff hiring and termination, formulating policies and procedures, and facilitating employees, awareness, training, education, and professional development.

New Hire Process

Managers within the respective functional groups of the organization determine the need for additional resources and submit formal job requisitions to senior management for approval. Once requisitions have been approved by the appropriate individual(s), HR begins sourcing for the available position. HR screens potential candidates and sends selected résumés to the respective managers. The relevant manager and HR conduct interviews, and potential offers are submitted to the appropriate authority within the organization for approval.

Individuals offered a position at Varonis are subject to background checks (as appropriate for each country with respect to local laws and regulations) as a condition of their employment in the company. The background check for employees includes substantiation of educational credentials, previous employment, and criminal records, as applicable. Prospective employees complete an employment application and sign waivers to release information for the background check. In addition, it is the policy of Varonis to request employment references to determine whether the candidate is well-qualified and has the potential to be productive and successful during his or her tenure.

In each location, employees receive data packages containing an overview of Varonis' HR policies and procedures. These offer packages include the offer letter or employment contract, the Code of Conduct, and privacy policy. Employees are asked to sign to confirm that they have read these materials.

Vendor employees and non-employee personnel who are granted wide access to Varonis assets or facilities must sign an access and use agreement, the terms being like the Code of Conduct, prior to being granted access to Varonis assets or facilities.

Varonis conducts background verification checks on all candidates for employment in accordance with relevant laws, regulations, and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.

Verification checks are subject to all relevant privacy, protection of personal data and/or employment-based legislation, and where permitted, may include the following:

- Availability of satisfactory character references, e.g., one business and one personnel.
- A check (for completeness and accuracy) of the applicant's resume.
- Confirmation of claimed academic and professional qualifications.
- Independent identity verification (passport or similar document).
- Additional detailed checks, such as checks of criminal records.

Employees are obliged to agree and sign the terms of their employment contract, which states theirs and the company's responsibilities for information security, privacy, and confidentiality.

During Employment

All employees receive appropriate Information Security and Privacy Awareness Training and regular updates in related statutes and organizational policies and procedures relevant for their role. All employees are required to complete security and privacy awareness training on an annual basis.

Varonis' Information Security department works with HR to provide periodic security awareness materials to Varonis' employees through emails and posters, as well as announcements on significant changes to security, availability, confidentiality, and privacy. Other awareness training materials include phishing campaigns. Varonis has established a sanction policy to address non-compliance with Varonis' security policies, and disciplinary actions are taken in the event of violation.

Access Provisioning/De-provisioning

Upon hire, employees are assigned to a position in the HR management system. Prior to the employees' start date, Employees are required to sign Varonis confidentiality agreement. New hire signs an additional privacy addendum and if background checks are not permitted in their country of employment, they also undergo reliability tests. Terminated employees' access is revoked as soon as possible. Quarterly access reviews are conducted as an additional layer of access control to make sure only active employees are granted access.

Performance Evaluation

Varonis has a continuous performance management process, which provides feedback for employees and managers through regular 1:1 meeting as well as Goal Plans within the Human Resources Information System (HRIS). Varonis also has an annual performance review process in place to review annual accomplishments, provide constructive feedback, identify opportunities for improvement, and development for all Varonis employees. The annual performance reviews allow 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 supports alignment between employee efforts and the organization's goals.

Physical Access

Varonis recognizes the significance of physical security controls as a key component in its overall security program. Employee Data Center Access. Microsoft Azure provides physical data center access only to approved employees. All employees who need data center access must first apply for access and provide valid business justification. These requests are granted based on the principle of least privilege, where requests must specify to which layer of the data center the individual needs access and are time-bound. Requests are reviewed and approved by authorized personnel, and access is revoked after the requested time expires. Once granted admittance, individuals are restricted to areas specified in their permissions.

Facilities Physical Security

Physical access protection mechanisms include entrances controlled by access cards and surveillance cameras as well as environmental security controls. Employees must not share badges with anyone. Access rights are granted according to a need-to-know. Access rights are promptly removed for terminated employees, or for personnel no longer requiring access to the facility where the information system resides. Access rights are reviewed and approved periodically by the facility manager, and guests must sign in and are accompanied by an employee when in Varonis physical areas.

Incident Response

Varonis has implemented incident response policies and procedures to detect, investigate, and response to security incidents. These procedures guide Varonis' personnel in reporting and responding to information technology incidents. Additionally, these implemented procedures help Varonis to identify, response, and report on system, security, and privacy breaches. The organization's incident response phases are aligned with industry best practices and are as follows:

- Preparation –establishes policies and procedures to effectively manage incidents and enables efficient communication methods both before and after an incident.
- Detection and Analysis – Identifies and validates security incidents.
- Containment, Eradication, and Recovery - These phases addresses:
  - How to isolate systems that have been affected
  - Restoration of services
- Lesson Learned – Recommendations on how to handle future incidents and if necessary, what process needs to be revised.

The Incident Response plan contains procedures to address various cyber-security scenarios that may occur. Furthermore, the plan includes a communication process for stakeholders at each phase. Varonis also has cyber insurance in place and remains up to date to cover any business liability for data breaches and loss of availability in the event of a cyber incident.

Endpoint Security

Anti-Malware

Anti-malware solution is installed on employees' endpoints to detect and prevent infection of unauthorized or malicious software. Antivirus reports are sent to relevant stakeholders on a regular basis. Additionally, Varonis uses a real-time anti-malware solution to protect its servers located at the external data centers and its private computers against viruses, worms and other forms of malicious code that may cause damage.

Software Approval and Monitoring Process

The installation of applications and software is restricted to authorized individuals. Software is fully controlled before it is implemented on the network. Processes are in place to detect changes to software and configuration parameters that may indicate unauthorized or malicious software. Antimalware software is implemented and maintained to provide for the interception or detection and remediation of malware. Software that is noncompliant with the company standards is detected and identified. Detection policies and procedures are defined. Detection tools are implemented on infrastructure and software to identify anomalies in operation or unusual activity on systems. Procedures include a defined governance process for security event detection and management, including the provision of resources, use of intelligence sources to identify newly discovered threats and vulnerabilities, and logging of unusual system activities. Anomalies are identified and handled by the relevant Varonis team.

Other Endpoint Security Controls

- **Patch Management** – The vulnerability and Threat management policy requires security patches to be installed in a timely manner. All devices are scanned for vulnerabilities and then patches are deployed by the IT department.
- **Secure Configuration** – Hardening policy is developed for servers and network devices.
- **Mobile Device Management** – A Mobile Device Management (MDM) solution is deployed for all Varonis' corporate and authenticated devices, which includes encryption, password protection, session time out, auditing and more production data is not accessible via smartphones or IoT devices.
- **Restrictions on the use of removable media** – Media such as USB drives are restricted of being used and monitored by the SOC.

Business Continuity and Disaster Recovery

Varonis Business Continuity plan outlines measures to avoid disruptions to customers and partners. The proposal plan includes impact analysis and risk assessment to help identify critical functions and processes.

The business continuity plan also includes the following topics:

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

Backup and Restore

Varonis has documented policies in place to guide personnel in system backup. The organization ensures availability and integrity of customer data by conducting regular periodic backups and restore tests.

The backup policy also contains provisions on backup systems and configurations and all necessary data required to maintain continual operation.

- Backups are stored encrypted
- Backup data is stored in a location at a distance from the data's principal storage location
- Access to backups is restricted to a minimal number of authorized employees
- Varonis uses at least daily differential backup and a weekly full backup for Varonis SaaS application database
- Varonis transactional log backups are performed based on business needs to meet their objectives
- All data is retained according to Varonis' Privacy Policy
- Backup monitoring
- Varonis monitors backups and infrastructure capacity within the Varonis SaaS Data Security Platform environment
- Alerts are triggered by the cloud operation team when capacity reaches a defined threshold

Additional Criteria for Availability

High availability eliminates single points of failure and helps to ensure continuous operations or uptime for an extended period. Load balancing is used to distribute traffic across multiple servers. Varonis uses Azure availability zones with 3 distinct data centers with independent electricity, Internet connectivity and power supply. Data is replicated over wide area network (WAN) link across those data center within the availability zones. 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.

Support Services

Support

Varonis' customer support procedures are designed to handle and resolve issues and requests in a timely manner. This includes issues that are internally identified, and issues submitted by customers. Varonis' support is provided via the support platform and support hotline. Response time to customers' issues is defined in the SLA agreement. The agreement is communicated to the customers as part of the contract.

Ticketing and Management

Varonis opens a ticket when an issue is raised by a customer or when an issue is proactively identified. Varonis uses an application to manage, classify, and ticket the customer support-related issues. Tickets are classified by level of urgency and assigned to the appropriate support tier for resolution.

Escalation Process

Varonis' goal is to resolve issues efficiently. Issues are tracked and updated in the ticket system. The escalation process is defined and documented by Customer Support. Tickets are escalated as deemed necessary to the infrastructure or engineering teams. Service interruptions are communicated to clients using email based on the escalation procedures and SLA notification thresholds.

Internal Audits

Varonis has an internal audit team which performs audits and assessments in variety of areas on an ongoing basis. Identified issues are reported to management and the Audit Committee, and corrective actions are taken when necessary. Preventative strategies are put in place to limit the recurrence of identified deficiencies.

External Audits

Varonis is committed to ensuring compliance with industry standards including but not limited to:

- ISO/IEC-27001:2022
- ISO/IEC-27017:2015
- ISO/IEC-27018:2019
- ISO/IEC-27701:2019
- NIST 800-53