VARONIS

Varonis Security Standards and Practices

Contents

This whitepaper describes the current state of Varonis' security as of August 2023, which is subject to change with future feature and product launches.

Formed in 2005, Varonis' customers include leading firms in the financial services, healthcare, industrial, insurance, energy and utilities, technology, consumer and retail, media and entertainment, and education sectors.

Our approach to security

Philosophy

Organizations are adopting cloud solutions for the flexibility and productivity they offer, but increased efficiency can bear increased risk. At Varonis, we take our software development and security practices seriously. We refine and share our security practices so customers can trust our solutions and approach.

Varonis is a pioneer in data security and analytics specializing in data protection, threat detection and response, and compliance. Varonis adopts a risk-based approach for its information security management system (ISMS). This approach requires identifying, assessing, and appropriately mitigating vulnerabilities and threats to information assets. Deploying an ISMS reduces the risk of unauthorized, accidental, or intentional information disclosure, modification, or destruction.

Our team

Our experienced teams operate in all fields of information security:

- **CISO** — Leads the global security teams and is responsible for internal infrastructure and cloud production security programs. The CISO also directs and oversees the development and review of information security policies, standards, and guidelines.
- **Security operations center (SOC) team** — Point of contact for security incidents. Using a tiered structure, our global SOC teams are responsible for monitoring systems and investigating cybersecurity incidents. They also develop operational playbooks and suggest alert enhancements to improve threat detection capabilities.
- **Product security group** — Leads the secure software development life cycle (SSDLC) program. This program is responsible for designing, testing, and implementing security controls across all Varonis product lines, including cloud-based production environments.
- **Governance, risk, and compliance (GRC) team** — Responds to customers' inquiries and assessments. They are also responsible for the security awareness program, risk management, external security audits, and the compliance program.
- **Corporate security architect** — Defines the security requirements of our internal infrastructure, network, and cloud-based IT solutions.

- **Development, security, and operations (DevSecOps) team** — Responsible for implementing security protocols and remediating vulnerabilities.
- **Security research and forensics team** — Identifies new security issues in monitored platforms and helps define the product roadmap to ensure emerging threats coverage.

Continually improving our security program

We understand that a good security program requires ongoing efforts, constant evaluation, and updates to improve infrastructure and cloud offerings. We regularly conduct internal and external assessments and perpetually update and improve our policies so that existing controls comply with what we believe are the highest security, privacy, and compliance standards.

How we secure our environment

Secure design

At Varonis, security is built into all systems, projects, and processes. In addition, security requirements are embedded in all stages of software development.

Quality software is built on a solid foundation. We believe that every new software component should be designed with security in mind from the ground up. We develop software using tried-and-true features and frameworks. We design characteristics by consulting with our vendors about the best and safest way to implement their components while using standardized security controls.

A good software product is constantly evolving, and therefore, risk and threat management is critical to uncovering security issues and tracking them across teams for execution. Leveraging tools such as the common vulnerability scoring system allows us to assess and prioritize any problems.

We bake security into design from the beginning — every design is reviewed for security and safety hazards and appropriate mitigations are created. Identified threats are used as a basis for further security testing.

Customer 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 users 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 SaaS Data Security Platform

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.[1]

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.

Varonis DatAdvantage Cloud

Varonis DatAdvantage Cloud works exclusively for cloud data sources, such as Salesforce, Google Suite, Box, etc.

For these data sources, Varonis does not require installing a Collector server, and the full data is retrieved by DatAdvantage Cloud from the data sources for classification.

The data is not stored in the cloud, and after data classification, the data is discarded. Metadata and classifications are stored in the cloud to enable their analysis by the customers.

Access control and management

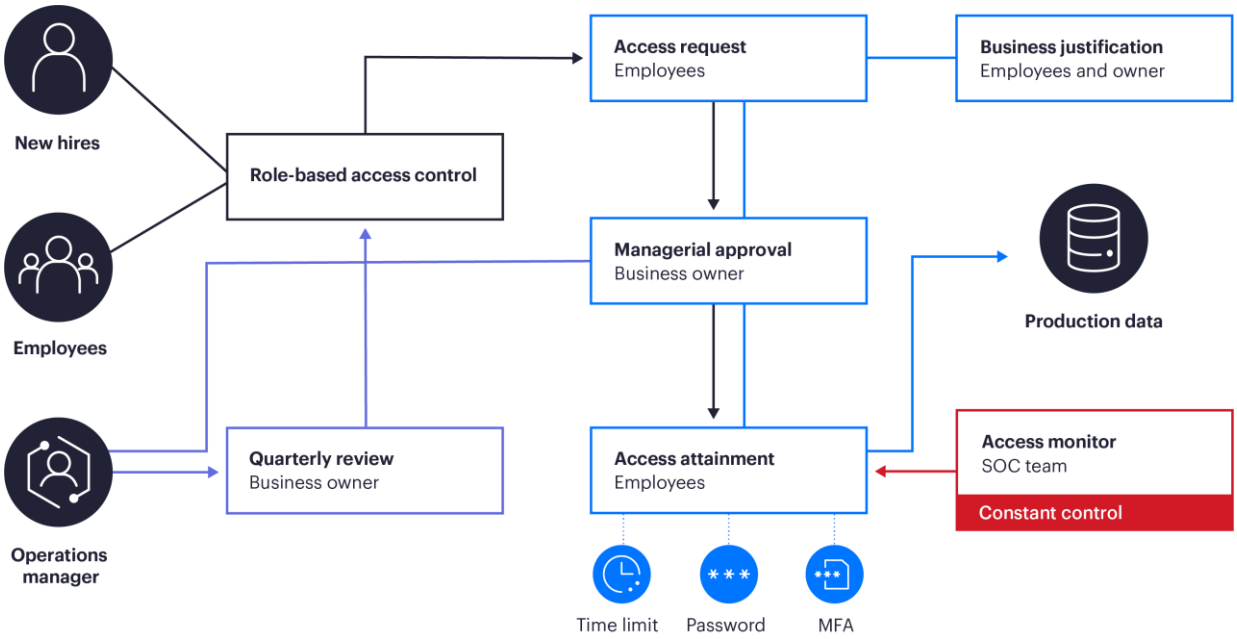
Securing production access

Varonis has defined processes for provisioning user access. New hires are granted access to resources based on their role in the company (i.e., role-based access control (RBAC)) and the least privilege principle. Only essential employees can request access to the production environment. Each access requires business owner approval and documented business

[1]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.

justification. Access is also audited, has time limitations, and is constantly monitored by the SOC teams. Multifactor authentication (MFA) is also mandatory for each session.

Figure 1: Access authorization



Access reviews

All production accounts are reviewed and approved periodically by the business owners to ensure the accounts have the appropriate level of access and permissions. Varonis personnel use strong authentication with MFA to access the production environment.

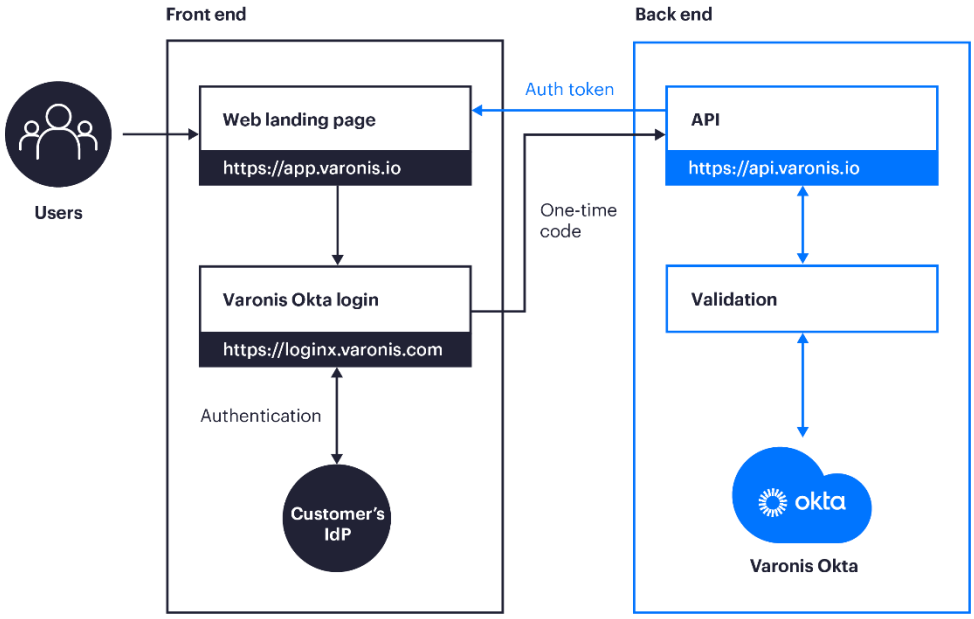
Passwords

Varonis' cloud services have a defined password policy that follows industry best practices and vendor recommendations. Our access authorization process covers provisioning, reviews, and password strength.

User authentication and federation

Authentication is performed using OAuth 2.0. Either Varonis' IDP (Okta) can be used, or customers can configure federation with their IDPs. The latter enables customers to control login policies such as MFA, password complexity, lockout policy, source IP addresses, and more.

Figure 2: Federated authentication workflow



Secured architecture and data flow

Back-end processes access customers' cloud services and on-premises data stores (such as NetApp filers) and fetch events and metadata of objects such as files, folders, users, groups, etc. All gathered information is stored with per-tenant partitioning, enforcing no cross-tenant access. The information is then shown in the web UI only to authenticated users, who can only access the specific tenant they are logged in to. All data is encrypted in transit, both externally and internally.

Figure 3: Varonis SaaS architecture

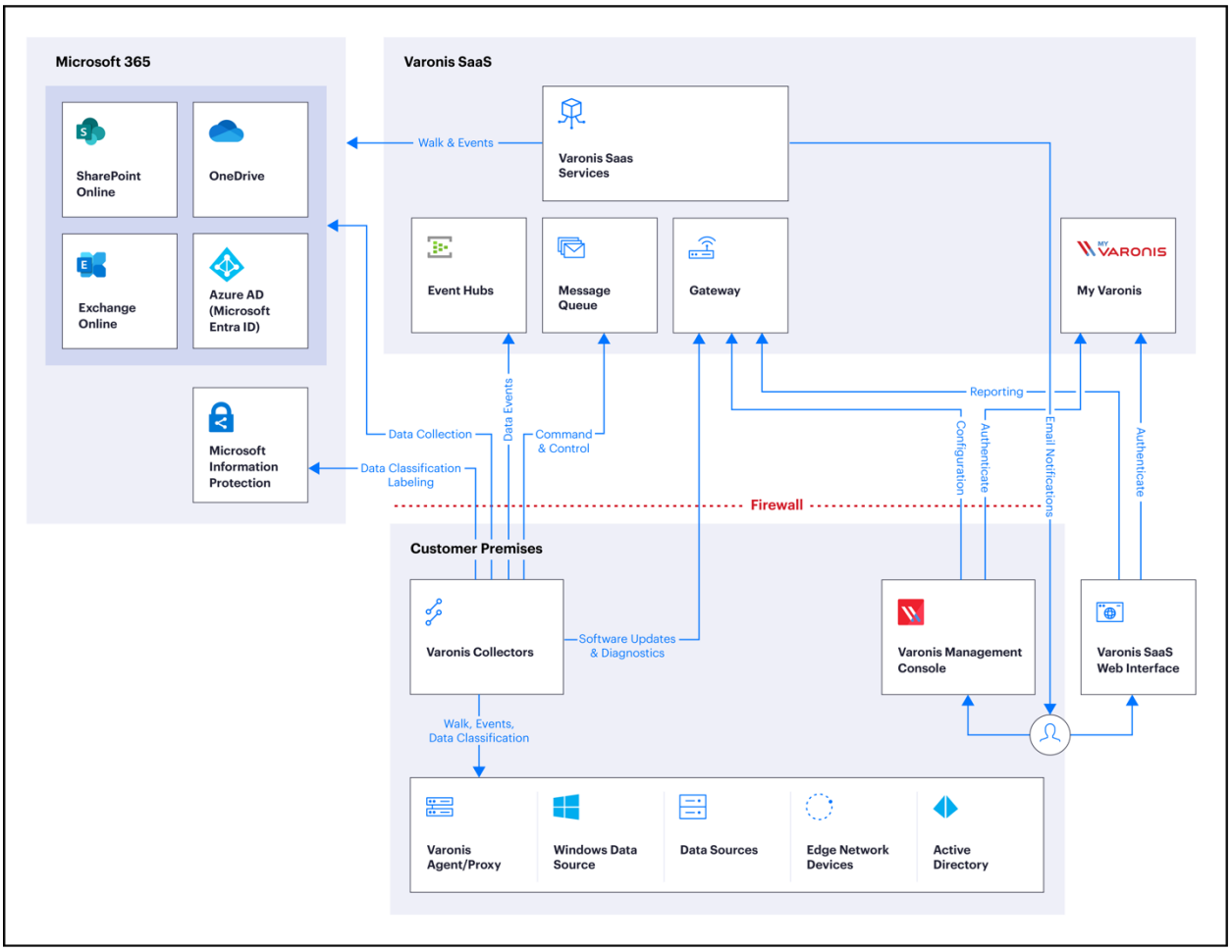
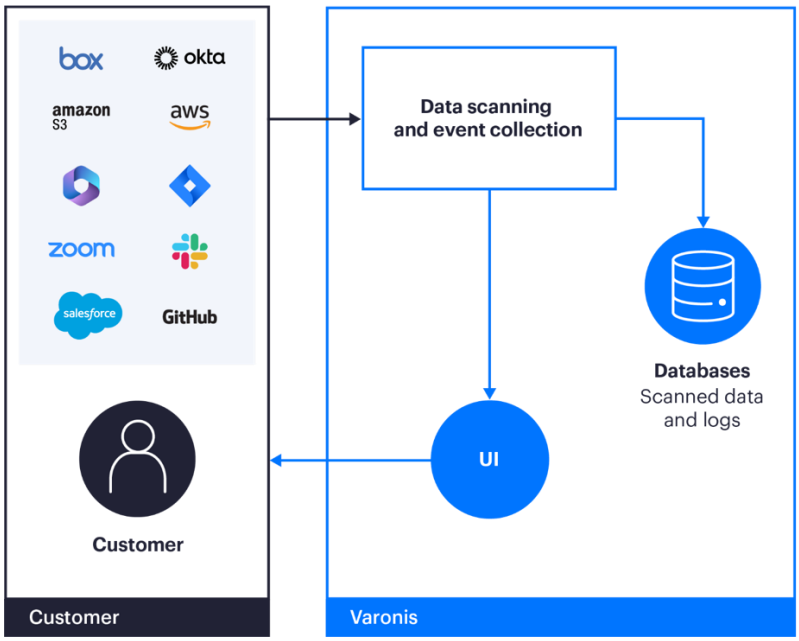


Figure 4: DatAdvantage Cloud architecture



API permissions

Varonis supports assignment of users to roles. Varonis implements RBAC so that each API call verifies that the user who accesses the back-end API via the UI has a required role assigned.

Building security into our network architecture

Users of the system must be identified and authenticated according to the assigned user role before they can use any resources. A native security system and add-on software products provide resource protection; these systems and software products identify and authenticate users and validate access requests by comparing the user's authorized roles in access control lists. Monitoring is performed by uninvolved personnel, such as a supervisor not involved in the work activities or by an employee from another department.

Each system has defined configuration standards. A security architect defines these standards, which are also updated annually and on a per-need basis. Prior to implementation, configuration standards are reviewed and approved by the lead security and lead system architect.

All resources are managed in the asset inventory system and each asset is assigned an owner. Owners are responsible for approving access to the resource and for performing periodic reviews of access by role.

Network security

We secure our external and internal networks with various technologies and monitoring tools, and secured network architecture:

- Internal segmentation is performed for different services.
- High availability and load balancing arrays are in place for production systems to help mitigate the effect of system errors.
- Web application firewall is in front of our cloud-based solutions and corporate infrastructure, with enforced rules to block web malicious attacks and sanctioned countries.
- Microsoft Azure and Amazon AWS public cloud infrastructure provide overall network protection against DDoS. Network security attacks and alerts are monitored continuously by the security operations center.

Securing our endpoint devices

Endpoint security is a pivotal mechanism of Varonis' in-depth security defense approach.

We use the following techniques to minimize threats to our endpoints:

- **Protection from malware** — Within our corporate infrastructure, the Varonis security team has deployed anti-malware and endpoint detection, in addition to response solutions on our internal servers that are monitored by the SOC team.
- **Patch management** — Our patch management policy requires security updates be installed promptly. All devices are continuously scanned for vulnerabilities.
- **Configuration management** — We have developed a hardening policy for our corporate servers.
- **Mobile device management** — We have an MDM (mobile device management) solution for all our corporate and authenticated devices, including encryption, password protection, session time-out, auditing, and production data not accessible via smartphones or internet of things (IoT) devices.
- **Monitoring** — Our SOC team continuously monitors our assets and responds to any anomalous, suspicious, or malicious activity from servers and endpoint devices. The SOC receives alerts from various security systems. The team is constantly improving threat detection capabilities and partners with our service providers to fine-tune our rules and proactively hunt for new detection and response methods.

Our operational security

Managing configurations and changes

Changes within all our environments are subject to a structured change-management procedure. They undergo design and impact analysis and are continuously monitored. As with all our processes, the procedure is subject to annual external audits (SOC 2 and ISO/IEC 27000 series).

Software code changes

Our CI/CD processes are fully integrated into our production changes. These processes include a peer programmer code review (by someone who is not responsible for the change) and approval of each change committed. New developed code is then going through several processes of quality assurance, such as regression, unit, security, and integration testing. The candidate builds then undergo manual and automatic tests, which are based on documented test plans. When tests are completed, the new candidate build is reviewed and approved by the relevant manager. We apply the same process for multi-tenant applications. All changes are logged and documented in a version control system.

Infrastructure and other changes

We established a documented process for all other types of changes, which include impact analysis, security team and business owner approval, documentation, tests, a fallback plan, and customer notification when necessary.

Communication of changes

Varonis provides customers notification and information regarding upgrades and changes to the cloud service that could adversely affect their cloud environment. All software update packages are distributed as part of upgrades and contain a digital signature.

Testing data

We abide by the following practices when testing data:

- The use of regulated data for testing purposes is prohibited.

- If personally identifiable information (PII) or other confidential information is used for testing purposes, all sensitive details and content are anonymized.
- The use of customer data for testing purposes is prohibited.

Logging and monitoring

Varonis' comprehensive logging and monitoring of its IT infrastructure and cloud-based security solution detects and reacts to inappropriate access of and/or use of information systems or data. We collect detailed audit logs from all cloud offerings and corporate infrastructure environments. Our security operations center and cloud operations teams monitor logs and use automated notifications and playbooks for performance issues or security incidents.

Business continuity and disaster recovery management

Customer support and resiliency are Varonis' top priorities. Our business continuity (BC) plan outlines measures to avoid disruptions to our customers and partners. The continuity plan includes impact analysis and risk assessment to help identify critical functions and processes. We also have BC plans for the following:

- Corporate infrastructure
- Working remotely
- Cyber incident response
- Pandemic preparedness

Our cloud environments are monitored by the cloud operations and incident response teams. We have an established process to notify customers of any down time.

High availability architecture

As part of our high availability, our cloud production infrastructure and services are fully redundant, to avoid single point of failures and downtime.

Cloud hosting resiliency features

Microsoft Azure and Amazon AWS services are providing resilient cloud hosting services by default, with redundant data centers, power supply, internet links, and more. Physical and logical controls are in place to ensure that customer data is highly available and able to be recovered in

case of data loss or corruption. Our cloud providers perform ongoing tests of the resiliency of data centers to continuously improve the overall security architecture and validate that they meet the highest security standards.

Monitoring

The cloud infrastructure is continuously monitored by our engineers, and securely designed to detect and immediately respond to any failure. Customer logs are stored in the same data centers as data itself, in order to provide quick resolution and avoid downtimes. We also established a process to notify customers in case of downtime. Availability controls are annually tested during the SOC 2 and ISO27000 audits.

Customers can use https://varonisprod.statuspage.io/ to subscribe to proactive communications about outages.

Backup and restore

Varonis has documented policies in place to guide personnel in system backup and recovery activities. We ensure availability and integrity of customer data by conducting regular daily backups and periodic restoration tests. Customer data is saved at the Amazon AWS and Microsoft Azure data centers and replicated to a distant availability zone by default. We use infrastructure-as-a-code to automatically build our data servers. This also allows rebuilding of the infrastructure quickly in case of a disaster.

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 SOC 2 compliant partner data centers address various physical security and environmental controls. We review the compliance certificates and attestations reports annually to ensure a consistent level of protection.

Third-party data center access

We use Amazon AWS and Microsoft Azure as service providers for our cloud-based solutions. Both organizations have sufficient physical access control systems and security staff using surveillance, detection systems, and other electronic means to secure their data centers.

Physical security of Varonis' facilities

Physical access protection mechanisms include entrances controlled by access cards and surveillance cameras, as well as other environmental security controls. Employees must have ID badges on their persons when in Varonis premises, and badges are not to be shared with anyone else. Access rights are granted according to a least privileged model. Access rights are promptly removed for terminated and transferred personnel, 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. Varonis facilities are monitored and secured using surveillance cameras and locks, identification cards, and a physical presence (guards and company personnel).

How we keep your data secure

Encryption

Customer data in transit over public networks is encrypted using — at a minimum — transport layer security (TLS) 1.2 or later (TLS 1.1 can be supported for backward compatibility). Varonis uses strong ciphers with longer keys and FIPS-compliant ciphers where possible. We also regularly monitor used ciphers and algorithms to make sure deprecated versions are not used.

Authorized employees are able to access Varonis cloud solutions using VPN (virtual private networks) and MFA. Varonis implemented secure data transmission protocols to encrypt data when transmitting over public networks. Encryption is also enabled on databases at rest and on data backups. Communication between the boundaries is encrypted. External zone boundaries (internet-facing services) are exposed through TLS.

Data encryption at rest is enforced on all tenants and servers by our cloud service providers by default. Data is encrypted at rest using advanced encryption standard 256-bit encryption.

Key management

Varonis uses Azure Key Vault solutions for secret and credential management. Access restrictions are applied to vaults, and no access is provided to users. All attempts to access parts of the infrastructure, including the Key Vaults, require permissions unavailable to the system user. Any attempts to access the infrastructure are audited.

Data centers

We selected Amazon AWS for DatAdvantage Cloud, and Microsoft Azure for Varonis SaaS, both of which are leaders in Gartner's Magic Quadrant for Cloud Infrastructure and Platform Services. Varonis SaaS and DatAdvantage Cloud are hosted in multiple availability zones in the U.S. Our data centers are certified by various security industry standards.

Multi-tenancy security

Logical security is implemented to create tenant separation and avoid compromising the data or tenants of other customers.

- Separate roles, secrets, and database partitions exist for each customer.
- All secrets, such as tokens for connecting to customer databases, are stored in managed Key Vault solutions. Separate roles are used to access each tenant's secrets.
- Employee access to production is restricted and only allowed on demand to certain employees for a short period of time by manager approval, as described in the access authentication and authorization section.
- The production environment is completely separated from the staging and development environment, with separate access control and a segmented network.

Sharing the responsibility for managing customer data

Varonis' system is designed to have shared responsibilities that are managed by the users of the system. Customer controls are expected to be in operation at user entities to complement Varonis controls.

Customers are responsible for:

- Ensuring a strong password policy
- Connecting their identify provider to enforce:
  - Single sign-on
  - Authentication
  - MFA
  - Password policy
- Configuring federation of customer's IDP with My Varonis
- Ensuring timely removal of user accounts for employees when user access is no longer required
- Securing on-premises components
  - Ensure a patch management process
  - Restricted access to the on-premises components
  - Disk encryption
  - Anti-malware/EDR solution with frequent signature updates and monitoring of alerts
  - Continuous monitoring of the relevant system components
- Configuring application roles to your employees based on the least privileged access model
- Securing initial tenant accounts with a strong password policy
- Secured integration with monitored platforms
  - Use strong secrets for data source access
  - Periodic secret rotation
  - Use only encrypted connectivity for data source access
- The selection of tenant geolocation

Data retention

Customer data will be deleted at the request of the customer, or automatically based on life cycle policies that are communicated to the customer. Customer data retention is explained within the software privacy policy (under the section “How long do we retain the information we collect?”)

HR security practices

In addition to technical means, information security requires human enforcement and application. Our human resource (HR) security practices address the controls that mitigate employee security risks. Our employment life cycle policy includes all HR security topics and applies to all employees, staff role changes, and local subcontractors.

Hiring

- Where applicable by law and per Varonis' policy, background verification checks are performed on all candidates for employment and contractors.
- Additional verification checks are required for sensitive roles and employees with privileged access or access to customer data.
- Employees are required to sign a non-disclosure agreement (NDA) and review security policies and our code of conduct.
- Users are assigned only relevant roles and permissions.

During employment

- All employees undergo security and privacy training annually. The program includes CISO-instructed current industry threat landscape and periodic phishing simulations.
- Developers perform periodic role-based security training.
- Access permissions are reviewed and modified with any role changes.

Account termination

- Varonis has procedures to revoke all logical and physical access and requires the return of all Varonis-supplied computing devices after employee termination.
- The HR department initiates the termination process, which triggers the immediate actions required from the relevant departments.

Security awareness training

All employees receive appropriate security and privacy awareness training, in addition to regular updates to organizational policies and procedures as relevant for their role.

Security training of employees is the responsibility of the security team. It is an ongoing program by which all employees must be consistently trained in security issues which are relevant to their functions and positions within the company.

The training must be relevant to each employee at the employees' functional level and consists of:

- General security training for all employees
- Privacy training for an employee with access to PII
- Secure code training for developers

Other requirements:

- Employee guidelines are distributed and uploaded to the intranet portal.
- Updates or newsletters are sent to employees as decided by the CISO.
- New employees must read and sign the education package.
- Annual review and confirmation of relevant security policies for each employee is required.

How we secure our solution

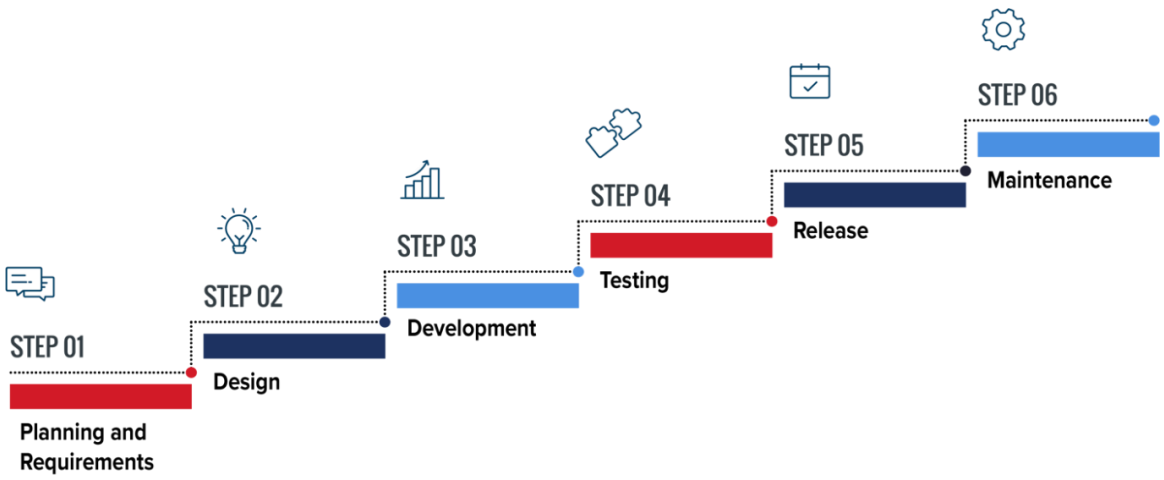
Secure design through SSDLC framework

Varonis adopted the SSDLC framework as part of its holistic development approach. This proven approach focuses on adding security to the standard SDLC (software development life cycle policy) and incorporating security as a major component of every phase of the SDLC. Using this methodology empowers Varonis to build secure applications and IT systems more quickly, reducing the costs of rework and identifying and addressing potential security issues upfront, making this method a viable investment for organizations.

Illustrated in Figure 5 below, the approach has the following six phases:

- **Planning and requirements** — This is a fundamental and critical phase of the process, during which the organization's needs for the intended system are identified with substantial feedback and interaction from/with customers. At this stage, pertinent information about the purpose of the system and expectations are collected and used to determine the feasibility of the product or service. At the end of this stage, all ambiguities are resolved, and features of the intended solution are formally documented.
- **Design** — Gather requirements (business, functional, and mandatory security) to incorporate into design. Define what should happen, by way of functional requirements, and what should not, by way of security requirements.
- **Development** — Determine the best approach to meet stakeholder needs by identifying alternatives and making the decision to purchase or custom build the system or service per specified requirements. Use established secure coding guidelines as well as code reviews that double-check that guidelines have been followed correctly for both codes written from scratch and when leveraging existing code from open sources.
- **Testing** — Conduct pre-release testing against the original design and security requirements. The application is not ready to be deployed unless test results are satisfactory, and the customer provides formal acceptance.
- **Release** — Go-live, operate, maintain, and modify. Plan for modifications to application functionality based on feedback in the form of future releases, upgrades/updates, and system enhancements.
- **Maintenance** — During the maintenance phase, Varonis provides updates to the software to fix security vulnerabilities. After the maintenance phase is over, Varonis will not usually stop providing security unless there is an exceptional situation at hand.

Figure 5: Varonis SSDLC model



Code analysis

Varonis uses both manual and automated secure code review techniques to examine its application's source code. The goal of this examination is to identify any existing security flaws or vulnerabilities. During our code review, developers specifically look for logic errors, examine implementation, and check style guidelines, among other tasks. During the automated code review, Varonis uses commercial tools to automatically review the source code of the application, using a predefined set of rules to look for inferior code.

How we identify, protect, and respond to threats

Security testing

At Varonis, we rigorously and continuously evaluate our security posture by testing our products, services, and infrastructure security controls and processes. We scan for vulnerabilities and misconfigurations and remediate issues promptly.

A summary of our security testing methods is as follows:

- **Penetration testing** — In addition to running automated scanners, we conduct testing using external and internal penetration testing teams. Test results are available upon request under a confidentiality agreement.
- **Internal security testing** — Our product team performs security testing on specific functionalities.
- **Web security assessment** — This identifies vulnerabilities in web services or web-based applications.
- **Manual processes** — Each commit of a new code is checked and approved. The product security team reviews the source code for quality and security. After verification, we proceed to the subsequent phases of testing using automated processes.
- **Network scans** — These scans help us identify active services, open ports, and applications running across our environment, plus any vulnerabilities at the network level.
- **External asset discovery** — We continually review the latest tools available and integrate them into our systems if we believe that they will enhance our vulnerability detection capabilities.
- **Customer reports and tickets** — We welcome notifications and respond promptly when a vulnerability is identified by one of our users.
- **Bug fix policy** — We have a documented bug fix policy that defines the time frames for resolving security issues of different severities in our products.

Vulnerability disclosure program

Varonis partners with HackerOne to maintain our public vulnerability disclosure program (VDP). Our VDP encourages HackerOne's massive network of security researchers to evaluate our assets and report any discovered vulnerabilities to our team for remediation. We foster relationships with the community to proactively identify new threats and improve security for our customers, partners, suppliers, employees, and overall company. More information about our vulnerability disclosure program can be found here.

Incident response

Varonis has a structured and consistent framework for the central coordination and monitoring of — and response to — all security-related events and incidents. Our security operations center continuously supervises events from all environments, correlates and merges logs, and creates automated and documented playbooks for various incident types. The threat intelligence team actively collects information from external resources. Our incident response plan includes step-by-step instructions for handling suspicious events or aggregation of events, including:

- Detection and analysis
- Categorization
- Containment
- Eradication
- Recovery
- Lessons learned

We test our response plans periodically with a red team and a blue team. As highly qualified and experienced security professionals and forensic experts, our IR team is trained to detect and respond quickly to any security incident.

Our IR plan includes notification workflows. If a customer's data or tenant is involved in an incident, the stakeholders are notified promptly. Once the investigation is complete, an after-action meeting is held to discuss process improvements and avoid future incidents.

Our risk management and compliance programs

Risk management programs

Varonis has a risk management policy and practice that includes risk identification, analysis, communication and reporting, treatment, and monitoring. Each risk is evaluated by the level of potential impact, and the treatment plan is an ongoing effort by all relevant Varonis departments.

Enterprise risk management program

Our security and privacy risk management programs have several components. Companywide risks are covered during the annual enterprise risk assessment, performed by the internal auditor, and presented to senior management and the audit committee of the board of directors. The CISO conveys cyber threats, after which time a mitigation plan is created and followed.

Cyber risk assessment

We conduct regular technical risk assessments for software development, cloud production, and corporate and cloud infrastructure. The security department 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

As with all other processes, engagements with third-party suppliers undergo a security risk assessment. Varonis ensures that vendors, who are thoroughly vetted for security and posture, are capable of delivery and aware of inherent security risks. We assure our customers that their data is protected by thoroughly reviewing third parties' security, compliance, and privacy practices. Whenever data is shared with a new third party, our customers are notified, and the vendor list updated. High-risk third parties that hold customer data undergo periodic review. 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.

Compliance with laws, regulations, and standards

The security standards that Varonis maintains are scoped for all our cloud solutions. Our compliance program constantly evolves to keep cloud infrastructure, policies, and standards updated with industry best practices. This compliance also includes regular independent external audits to ensure security, privacy, and compliance controls and procedures.

Varonis has nearly 30 security policies in place, covering various security domains in our documentation and aligns policies with various ISO/IEC standards (27001, 27017, 27018, and 27701), NIST 800-53, AICPA (American Institute of Certified Public Accountants), and other privacy regulations.

Regulatory compliance certifications

Varonis is certified for the following certifications.

- **ISO/IEC 27001:2013** is the best-known standard that provides ISMS requirements.
- **ISO/IEC 27017:2015** provides guidelines for information security controls applicable to the provision and use of cloud services.
- **ISO/IEC 27018:2019** establishes commonly accepted control objectives, controls, and guidelines for implementing measures to protect PII, per the public cloud computing environment's privacy principles listed in ISO/IEC 29100.
- **ISO/IEC 27701:2019** is a privacy-oriented standard that specifies requirements for establishing, implementing, maintaining, and continuously improving a privacy information management system (PIMS). ISO 27701 is based on the conditions, control objectives, and controls of ISO 27001. This standard creates a strong integration point for aligning security and privacy controls and supporting global privacy standards, such as the California Consumer Privacy Act (CCPA), EU General Data Protection Regulation (GDPR), and New York SHIELD Act.
- **SOC 2 Type 2** is the trust services criteria for security, availability, confidentiality, and privacy conclusion.
- **CSA Star Certification** confirms that Varonis successfully completed CSA's STAR Level 1 security self-assessment.
- **Cyber Essentials** is a U.K.-government backed program that helps protect organizations against a range of common cyberattacks.
- The **Texas Risk and Authorization Management Program (TX-RAMP)** is a program that provides a review of security measures taken by cloud products and services that transmit

data to Texas state agencies. Varonis SaaS and DatAdvantage Cloud received provisional certification via third-party audit/attestation review from TX-RAMP.

Our policy program requires an annual review, a process for improvements, and CISO and senior management evaluation. Employees are required to read the policies at regular intervals. Varonis policies are available for review within the company portal.

Privacy policies and practices at Varonis

We take privacy seriously. Varonis is committed to data protection laws and regulations and maintains appropriate procedures in our PIMS. Our privacy program aligns with global privacy standards, including GDPR and CCPA.

We recognize the need for appropriate protection and management of personal information that you provide to us. Varonis has the following policies and practices in place:

- Privacy Whitepaper
- Software Privacy Policy
- Data Processing Addendum for SaaS Customers

Our main data privacy principles are:

- **Data retention and minimization** — We only collect essential information and retain it for the shortest period necessary.
- **Purpose limitation** — We limit the processing of data to that which is adequate, relevant, and necessary for the identified purpose.
- **Data processing addendum** — All relevant third-party processors must comply with Varonis' policies and terms.
- **Data subject rights** — We have a process in place to handle all relevant data subject requests promptly.
- **Breach notification** — Our incident response policy includes a privacy breach workflow requiring all relevant stakeholders to be notified promptly.
- **Training** — All employees are trained in our privacy policies and procedures to increase awareness and comply with GDPR and other privacy regulations.
- **Privacy assessment** — All third parties with access to PII undergo a privacy assessment.

Data residency

During the onboarding process, customers can select the geolocation of their tenant. Below are the data center hosting locations for our cloud offerings:

Cloud offering	DatAdvantage Cloud	Varonis SaaS Data Security Platform
Cloud hosting provider	Amazon AWS	Microsoft Azure
US data center	East US	East US 2
EU data center	EU Central	West Europe
CA data center		Canada Central
AU data center		Australia East
UK data center		UK South

Internal and external audit

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 standards, and Varonis internal policies, standards, and procedures.

Varonis verifies compliance to standards through various methods, including but not limited to periodic security assessments, business tool reports, and internal and external audits.

We perform comprehensive security audits through well-known audit firms at least annually. Additional internal audits are performed in areas that are deemed “high risk” and are reported to the audit committee of the board of directors of Varonis. Audit outputs are all fed into a continuous improvement cycle which helps us continually sharpen the overall security program.

Law enforcement and government requests for data

Varonis has a defined process that incorporates our legal department to ensure that while we comply with law enforcement and the government's requests for data, we also maintain our customers' confidentiality in compliance with the law.

Your privacy matters to us

We are committed to protecting your data privacy and rights. We are also committed to responsible stewardship of the data under our control and perpetrate compliance with all applicable data protection laws that regulate the collection, use, and disclosure of data and privacy.

How to connect with us

Report a vulnerability
https://hackerone.com/varonis

Report a security issue
soc@varonis.com

Privacy inquiries
privacy@varonis.com

Requests to cease processing or deletion of personal information

dl-privacy-request@varonis.com