Varonis DatAdvantage Cloud
Security and Privacy Standards and Practices
Contents

Our Approach to Security .......................................................................................................................... 3
How We Secure Our Environment ........................................................................................................... 5
Our Operational Security ....................................................................................................................... 11
How We Keep Your Data Secure ........................................................................................................... 14
How We Secure Our Staff ..................................................................................................................... 15
How We Secure Our Solution ................................................................................................................. 16
How We Identify, Protect, and Respond to Threats ................................................................................ 20
Our Risk Management and Compliance Programs .................................................................................. 22
How to Connect with Us .......................................................................................................................... 25
Our approach to security

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

Philosophy

Organizations are adopting cloud solutions for the flexibility and productivity gains they offer. The 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 that customers can trust in our solutions and practices.

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

We have experienced teams that operate in all fields of information security:

- **CISO** – Leads the global security teams and is responsible for the internal infrastructure and cloud production security programs. The CISO also directs and oversees the development and review of the 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 Architect** – 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 awareness, 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.

- **DevOps** – Responsible for implementation of security protocols, and remediation of vulnerabilities.

- **Security Research and Forensics Team** – Identifies new security issues in monitored platforms and helps advance functionality to improve customer experiences.

### 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 from the ground up. We develop software using tried-and-true features and frameworks. We design characteristics by consulting with our vendors regarding the best and safest way to implement their components using standardized security controls.

A good software product is constantly evolving; therefore, risk and threat management is critical to uncovering security issues and tracking them across teams for execution. Leveraging tools such as Common Vulnerability Scoring System (CVSS) scoring allows us to assess and prioritize any problems.

Access Control and Management

Provisioning

Varonis has defined processes for provisioning user access. New hires are granted access to resources based on their role in the company. Following the Role-Based Access Control (RBAC) security paradigm allows us to achieve and maintain least privilege with strong identity security. Any access changes to permissions require business owner approval.

Customer Data

Customer data is managed, processed, and stored with relevant protection and other regulatory controls. We use a range of technologies to manage separate access between tenants, and access control.
All customer data is classified as Confidential per the Varonis Global Classification Policy. Data is gathered and protectively stored to identify immediate or potential risks within the customer’s environment.

Only essential employees can request access to production data, and each access requires manager approval and a business justification. Access also has time limitations and is constantly monitored by the SOC teams. Multi-factor authentication (MFA) is also mandatory for each session.

Access Reviews

All production accounts are reviewed and approved periodically by the business owners to ensure the appropriate level of access and permissions.

Passwords

Varonis has a defined password policy that follows industry best practices and vendor recommendations. Our Access Authorization process covers provisioning, reviews, and passwords (Figure 1).

Figure 1: Access Authorization
Secured Data Flow

Backend processes access customers’ services (such as Box, AWS, G-Suite, etc.) and fetch events and metadata of objects such as files, folders, users, groups, etc. All gathered information is stored in tenant-specific databases and access to those databases is not shared between tenants. It is then shown in the Web UI to authenticated users, who also can only access the specific tenant they are logged into.

API Security

API access is authenticated and authorized before returning any data sets. API is limited to Graph QL queries only. Connectivity requires that the user is configured in the system (SSO or MFA). Connectivity includes the tenant, user, and password or a token from an external identity provider. In this way, separation is maintained from customer to customer.
Authentication

Authentication is performed using OAuth 2.0, with API credentials stored and hashed within the DatAdvantage Cloud premises (Figure 3).

Federated Login Flow (aka SSO)

For non-federated users, we store password hashes created with industry accepted hashing algorithms.
Building Security into Our Network Architecture

Varonis uses role-based security architecture. Users of the system must be identified and authenticated before use of any system 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 engaged in the work activities or by an employee from another department.

Each hardware platform and software system has defined configuration standards. A security architect develops these standards, which are also updated annually or on an as-needed 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.

Securing Access to Our Networks through DatAdvantage

Each user at Varonis is assigned to a specific group. Those assigned to the production group can request access to production. The business owner must grant access for each production session. The SOC team monitors access. Each session is approved for a limited time and must be documented and logged.

To safely access DatAdvantage and AWS (Amazon Web Services) resources:

- A two-factor authentication mechanism is required for employees to access DatAdvantage Cloud.
- A generated token which expires periodically is required to access AWS resources such as SQS (Simple Queue Service) or internal API services.

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 that security updates are 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.
Our operational security

Managing Configurations and Changes

Changes within all our environments are subject to a structured change management procedure. New changes require a risk assessment, security team and business owner approval, as well as documentation, tests, a fallback plan, and customer notification where necessary. As with all our processes, the change management procedure is subject to annual external audits (SOC 2 and ISO 27000 series).

Testing of Changes

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 of 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.

Communication of Changes

Varonis provides customers notification and information regarding upgrades as well as changes to the cloud service that could adversely affect their cloud environment.

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 is anonymized.
- The use of customer data for testing purposes is prohibited.
Logging and Monitoring

Varonis has comprehensive logging and monitoring of its IT infrastructure and cloud-based security solution to detect and react to inappropriate access to 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, 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 proposal includes impact analysis and risk assessment to help identify critical functions and processes. We also have BC plans for the following:

- Corporate infrastructure
- Critical suppliers
- 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.

Backups

Varonis has documented policies in place to guide personnel in system backup and recovery activities. The organization ensures availability and integrity of customer data by conducting regular periodic backups. Customer data is saved at the Amazon US East region or EU Central region. Data is encrypted at rest using AES (Advanced Encryption Standard) 256-bit encryption.

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.

The cloud hosting services supporting Varonis DatAdvantage Cloud are provided by AWS and monitored by Varonis’ Information Security department.

**Third-Party Data Center Access**

Third-party access is requested by approved AWS employees, who must apply for third-party access and provide a valid business justification. These requests are granted based on the principle of least privilege, where requests that are time-bound must specify to which layer of the data center the individual needs access. These requests are 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. Anyone granted visitor badge access must present identification when arriving on site and are signed in and escorted by authorized staff.

**Varonis’ Facilities Physical Security**

Physical access protection mechanisms include entrances controlled by access card 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 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 physical presence (guards and company personnel).
How we keep your data secure

Encryption

Customer data in transit over public networks is encrypted using Transport Layer Security (TLS) with Perfect Forward Secrecy (PFS). 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 DatAdvantage Cloud utilizing VPN (Virtual Private Networks) and multi factor authentication. 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 boundary (internet facing services are exposed though TLS

Data encryption at rest is enforced on all tenants and servers by AWS by default.

Key Management

Varonis uses Amazon Secret Manager (ASM) for secret and credential management. The process is inspected and verified internally by AWS as part of their existing validation processes. Access restrictions are applied to ASM, and no access is provided to users. All attempts to access parts of the infrastructure, including the ASM, require permissions unavailable to the system user. Any attempts to access the infrastructure are audited and alerted.

Data Centers

We selected Amazon, the Leader in Gartner’s Magic Quadrant for Cloud Infrastructure and Platform Services (CIPS). Varonis DatAdvantage Cloud is hosted in multiple availability zones in the Amazon U.S. East or EU Central data centers certified by various security industry standards. For more information, please click here.
Tenant Separation

Logical security is implemented to avoid compromise of data or tenant of other customers. Separate roles, secrets, and databases exist for each customer. Secrets and passwords are rotated frequently and stored with access restricted on a per-tenant basis.

- All secrets, such as tokens for connecting to customer databases, are stored in AWS Secrets Manager. Separate roles are used to access each tenant’s secrets.
- Employee access to production is restricted and only allowed on-demand to certain employees for a short period of time by manager’s 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.

Varonis protects customer data in services such as AWS, Box, etc. Customers have a responsibility to ensure only relevant people can access Varonis’ SaaS Platform, and that permissions are set according to the customer’s access control policy.

The diagram below illustrates the shared responsibilities of managing customers’ data.

![Diagram of Shared Responsibility](image-url)

Figure 5: Shared Responsibility
Data Retention

Customer Data will be deleted at the request of the customer, or automatically based on lifecycle 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?”)

How we secure our staff

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 lifecycle 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 code of conduct.
- Users are assigned only relevant accounts and permissions
- 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.
- 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 on-going 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.

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

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
How we secure our solution

Secure Design through SSDLC Framework

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

Illustrated in Figure 6 below, the approach has the following six phases:

- **Planning and Requirements** - This is a fundamental and critical phase of the process where 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 need 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 these 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 original design & security requirements. The application is not ready to be deployed unless test results are satisfactory and 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** - System reaches end of life and is removed from operation and disposed of in accordance with regulatory and security requirements.
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 vulnerabilities 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.
- **Container Assessment** – Examines the current application architecture, business practices, and development workflows as they relate to container workflow processes.
- **Open-Source Assessment** – Scans for vulnerabilities in an artifact repository.
- **Web Security Assessment** – 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.
- **Configuration Monitoring** – We monitor the configuration of our environments against established configuration baselines.
- **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 timeframes for resolving security issues of different severities in our products.
Incident Response

Varonis has a structured and consistent framework for the central coordination, monitoring, and response for 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 (IR) 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. Company-wide 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 cyberthreats, 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.

Regulatory Compliance Certifications

Varonis is certified for the following:

- **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** – Trust Services Criteria for Security, Availability, Confidentiality and Privacy

Conclusion

Varonis has nearly 30 security policies in place, covering various security domains in our documentation and aligns policies with various ISO standards (27001, 27017, 27018, and 27701), NIST 800-53, AICPA (American Institute of Certified Public Accountants), and other privacy regulations. 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 maintains appropriate procedures in our privacy information management system (PIMS). Our privacy program aligns with global privacy standards, including the EU’s General Data Protection Regulation (GDPR).

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

- Website Users & Marketing Privacy Policy
- Software Privacy Policy
- Data Processing Addendum for SaaS (Software as a Service) Clients

Our main Data Privacy principles:

- Data Retention and Minimization – We only collect essential information and retain it for the shortest period necessary.
- 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.

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, as well as Varonis internal policies, standards, and procedures. Varonis’ senior management is committed to ensuring compliance with industry standards including but not limited to:
- ISO 27001
- NIST 800-53
- ISO 27017
- ISO 27018
- ISO 27701
- AICPA requirements (SOC 2 requirements)
- General Data Protection Regulation (GDPR).

Varonis verifies compliance to these 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 keep sharpening 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 government’s requests for data, we also maintain our customers’ confidentiality in compliance with the law.

**How to connect with us**

Report a Security Issue
soc@varonis.com

Privacy Inquiries
privacy@varonis.com