VARONIS

National Institute of Standards and Technology SP 800-171

Varonis compliance mapping for NIST 800-171 SP, rev. 2: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Contents

Overview

In 2010, the U.S. government launched a framework of cybersecurity standards to address data security for private contractors. Rather than using the existing National Institute of Standards and Technology (NIST) SP 800-53, which is a series of security controls for internal federal agencies, NIST developed a shorter list of standards for government contractors to abide by, titled "NIST Special Publication (SP) 800-171: Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations." Because federal contractors are likely to process data that the federal government considers controlled unclassified information (CUI), the federal government requires these contractors to protect that data.

While NIST SP 800-171 is based heavily on and is consistent with NIST SP 800-53, private companies are given some flexibility in the actual implementation of the security controls. If contractors are already compliant with the popular ISO 27001 or the Framework for Critical Infrastructure Cybersecurity, it's easy to comply with NIST SP 800-171 as the frameworks are similar in nature. Appendix D of the NIST SP 800-171 standard provides a convenient mapping of the controls in publication to these other data security standards.

How Varonis maps to the NIST SP 800-171 framework

Here's how Varonis can help organizations achieve data security as expected by NIST SP 800-171:

NIST 800-171 checklist	How Varonis helps
3.1 Access controls	**How Varonis helps:**
3.1.1 Limit information system access to authorized users, and processes acting on behalf of authorized users.	By combining user and group information taken directly from Active Directory, LDAP, NIS, or other directory services with a complete picture of the file system, Varonis gives organizations a complete picture of their permissions structures. Both logical and physical permissions are displayed and organized, highlighting and optionally aggregating NTFS and share permissions. Flag, tag and annotate your files and folders to track, analyze and report on users, groups, and data.
3.1.5 Employ the principle of least privilege, including for specific security functions and	Varonis helps organizations not only define the policies that govern who can access, and who

privileged accounts.	can grant access to unstructured data, but it also enforces the workflow and the desired action to be taken (i.e. allow, deny, allow for a certain time period).
3.2 Awareness and training	**How Varonis helps:**
3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	Our Cyber Resiliency Assessment can help you stress-test your environment by simulating attacks on your regulated data and CUI. In doing so, we can help your security team learn by: • Assessing your threat detection capabilities against modern adversaries • Classifying sensitive data and measuring overexposure and non-compliant access • Documenting detection gaps, Zero-Trust posture, and remediation priorities • Preparing and educating your team to handle advanced incidents
3.3 Audit and accountability	**How Varonis helps:**
3.3.1 Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	Varonis helps organizations examine and audit the use of ordinary and privileged access accounts to detect and prevent abuse. With a continual audit record of all files, email, SharePoint, and Directory Services activity, Varonis provides visibility into users' actions. The log can be viewed interactively or via email reports. We can also identify when users have administrative rights they do not use or need and provide a way to safely remove excess privileges without impacting the business.
3.3.5 Correlate audit record review, analysis, and reporting processes for investigation, and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	Varonis can be configured to send real-time alerts on a number of actions, including the granting of administrative rights to a user or group. This allows the organization to detect, in real time, when privileged access has been granted erroneously and act before abuse

	occurs. Real-time alerts can also be triggered when administrative users access, modify, or delete business data.
3.3.6 Provide audit record reduction (collecting audit information into a summary format that is more meaningful to analysts) and report generation to support on-demand analysis and reporting.	Varonis continuously maps permissions and monitors data activity to identify excessive access, policy violations, and suspicious behavior — providing a full audit trail of activity for investigation and analysis. We use user entity and behavior analytics (UEBA) to identify risky behavior and deliver alerts that are meaningful, while filtering out the noise. Through detailed and intuitive dashboards, reports, and playbooks, admins can easily identify and report on where sensitive data is at risk and deliver these aggregated reports to auditors or internal analysts.
3.3.7 Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.	Varonis time stamps alerts based on the reported time stamp of the collector, processing the resource that triggered the alert.
3.3.8 Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	The Varonis platform allows users to create different RBAC roles, such as Varonis admin, and Varonis users (someone who can only view audit events but not manage the system).
3.3.9 Limit management of audit logging functionality to a subset of privileged users.	
3.4 Configuration management	**How Varonis helps:**
3.4.4 Analyze the security impact of changes prior to implementation.	Varonis provides actionable intelligence on where excess file permissions and group memberships can be safely removed without affecting normal business processes. DatAdvantage also provides the ability to model and simulate permissions changes in its sandbox so they can be tested without affecting the production environment.
3.6 Incident response	**How Varonis helps:**

3.6.3 Test the organizational incident response capability.	Our Cyber Resiliency Assessment can help you stress-test your environment by simulating attacks on your regulated data and CUI.
3.11 Risk assessment	**How Varonis helps:**
3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.	Varonis offers Compliance Risk Assessments and Data Risk Assessments tailored to your unique business needs and challenges. These services allow you to evaluate our data security platform for free in your own environment and using your own data. Once you are a Varonis customer, your account team will conduct quarterly business reviews with you to assess new or ongoing risks to your data and help mitigate them — and make the most of your investment with us.
3.12 Security assessment	**How Varonis helps:**
3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	Our Cyber Resiliency Assessment can help you stress-test your environment by simulating attacks on your regulated data and CUI.
3.14 System and information integrity	**How Varonis helps:**
3.14.5 Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.	Varonis provides innovative behavior analytics with privileged account detection by using behavior-based threat models to analyze and detect suspicious activity. Automatically analyze and detect suspicious activity and prevent data breaches — using deep analysis of metadata, machine learning, and advanced user behavior analytics (UBA). Our UBA threat models allow you to detect: • Insider threats • Outsider threats • Malware activity (including ransomware)

	• Suspicious behavior • Potential data breaches • Compromised assets
3.14.6 Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	Automatically analyze and detect suspicious activity and prevent data breaches — using a deep analysis of metadata, machine learning, and advanced user behavior analytics (UBA).
3.14.7 Identify unauthorized use of organizational systems.	Our threat models allow you to detect a wide range of threats, alerting you to compromised assets and anomalous data access. By doing so, we can identify unauthorized use of data stores and the files within them. Using AI that learns from your environment as well as pre-set rules, we define baseline normal behavior, and can identify threats such as insider threats or ransomware with a high level of accuracy.

Schedule a free Data Risk Assessment.

Varonis can help manage your security risk and comply with NIST 800-171 by implementing least-privilege access to your data, monitoring your data for potential threats, and automatically generating comprehensive audit records. To learn more about how Varonis can help you comply with NIST 800-171, sign up for a free Data Risk Assessment, during which you can try out our products with no commitment and with full support from our team.

Our complimentary assessment run by expert forensics and incident response analysts will help you find and classify data across on-premises and cloud data stores, measure and report on data exposure, and alert on suspicious access to your data.

Contact us

About Varonis

Varonis is a pioneer in data security and analytics, fighting a different battle than conventional cybersecurity companies. Varonis focuses on protecting enterprise data on-premises and in the cloud: sensitive files and emails; confidential customer, patient, and employee data; financial records; strategic and product plans; and other intellectual property.

The Varonis Data Security Platform detects insider threats and cyberattacks by analyzing data, account activity, and user behavior; prevents and limits disaster by locking down sensitive and stale data; and efficiently sustains a secure state with automation. With a focus on data security, Varonis serves a variety of use cases including governance, compliance, classification, and threat analytics. Varonis started operations in 2005 and has thousands of customers worldwide — comprised of industry leaders in many sectors including technology, consumer, retail, financial services, healthcare, manufacturing, energy, media, and education.