VARONIS COMPLIANCE BRIEF

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY 800-171 FOR NONFEDERAL ORGANIZATIONS

CONTENTS

OVERVIEW

Rather than using the existing NIST 800-53, which is a series of security controls for internal federal organizations, the US government in 2010 instead launched a separate standard to address data security for private contractors. The National Institute of Standards and Technology (NIST) 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, addresses data security for the private sector — contractors of federal agencies.

While NIST 800-171 is based heavily on and is consistent with 800-53, private companies are given some flexibility in the actual implementation. If they already have in place the popular ISO 27001 or the new Framework for Critical Infrastructure Cybersecurity, they can still comply with 800-171: appendix D of the 800-171 standard provides a convenient mapping of its controls to these other data security standards.

MAPPING NIST 800-171 CONTROLS TO VARONIS SOLUTIONS

The following table maps relevant 800-171 controls to specific Varonis solutions:

800-171 CONTROL FAMILY	DESCRIPTION	VARONIS SOLUTIONS
3.1 Access Controls	3.1.1 Limit information system access to authorized users, processes acting on behalf of authorized use	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 DatAdvantage** 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 privileged accounts.	**Varonis DataPrivilege** helps organizations not only define the policies that govern who can access, and who 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).
3.3 Audit and Accountability	3.3.1 Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.	**Varonis DatAdvantage** 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 file, email, SharePoint, and Directory Services activity, DatAdvantage provides visibility into users' actions. The log can be viewed interactively or via email reports. DatAdvantage can also identify when users have administrative rights they do not use or need and provides a way to safely remove excess privileges without impacting the business.
	3.3.5 Correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.	**Varonis DatAlert** 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.

800-171 CONTROL FAMILY	DESCRIPTION	VARONIS SOLUTIONS
3.4 Configuration Management	3.4.4 Analyze the security impact of changes prior to implementation.	**Varonis DatAdvantage** 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.
3.11 Risk Assessment	3.11.2 Scan for vulnerabilities in the information system and applications periodically and when new vulnerabilities affecting the system are identified.	The **Varonis IDU Classification Framework** gives organizations visibility into the content of data, providing intelligence on where sensitive data resides across its file systems. By integrating file classification information into the **Varonis Metadata Framework**™, and presenting it in the **DatAdvantage** interface, the Varonis IDU Classification Framework enables actionable intelligence for data governance - including prioritized reports showing where sensitive content is highly concentrated and over-exposed, and an audit trail of all Active Directory activity, Varonis gives you context around the sensitive content.
3.14 System and Information Integrity	3.14.5 Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed. 3.14.6 Monitor the information system, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	**Varonis DatAlert Analytics** 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 cryptolocker) • Suspicious behavior • Potential data breaches • Compromised assets

ABOUT VARONIS

Varonis is a leading provider of software solutions that protect data from insider threats and cyberattacks. Varonis empowers enterprises to stop ransomware in its tracks, discover where sensitive data is overexposed, prioritize vulnerable and stale data, and lock it down without interrupting business. Varonis builds context around the content of data and activity; automates threat detection with predictive threat models built on advanced analytics, user behavior, and machine learning; and monitors critical assets for suspicious activity, including unusual access to sensitive data, abnormal user behavior and file activity to protect against potential exploitation.

All Varonis products are free to try for 30 days. Our systems engineering team will get you up and running in no time.

FAST AND HASSLE FREE

Our dedicated engineer will do all the heavy-lifting for you: setup, configuration, and analysis - with concrete steps to improve your data security.

FIX REAL SECURITY ISSUES

We'll help you fix real production security issues and build a risk report based on your data.

NON-INTRUSIVE

We won't slow you or your system down. We can monitor millions of events per day without impacting performance.

START YOUR FREE TRIAL