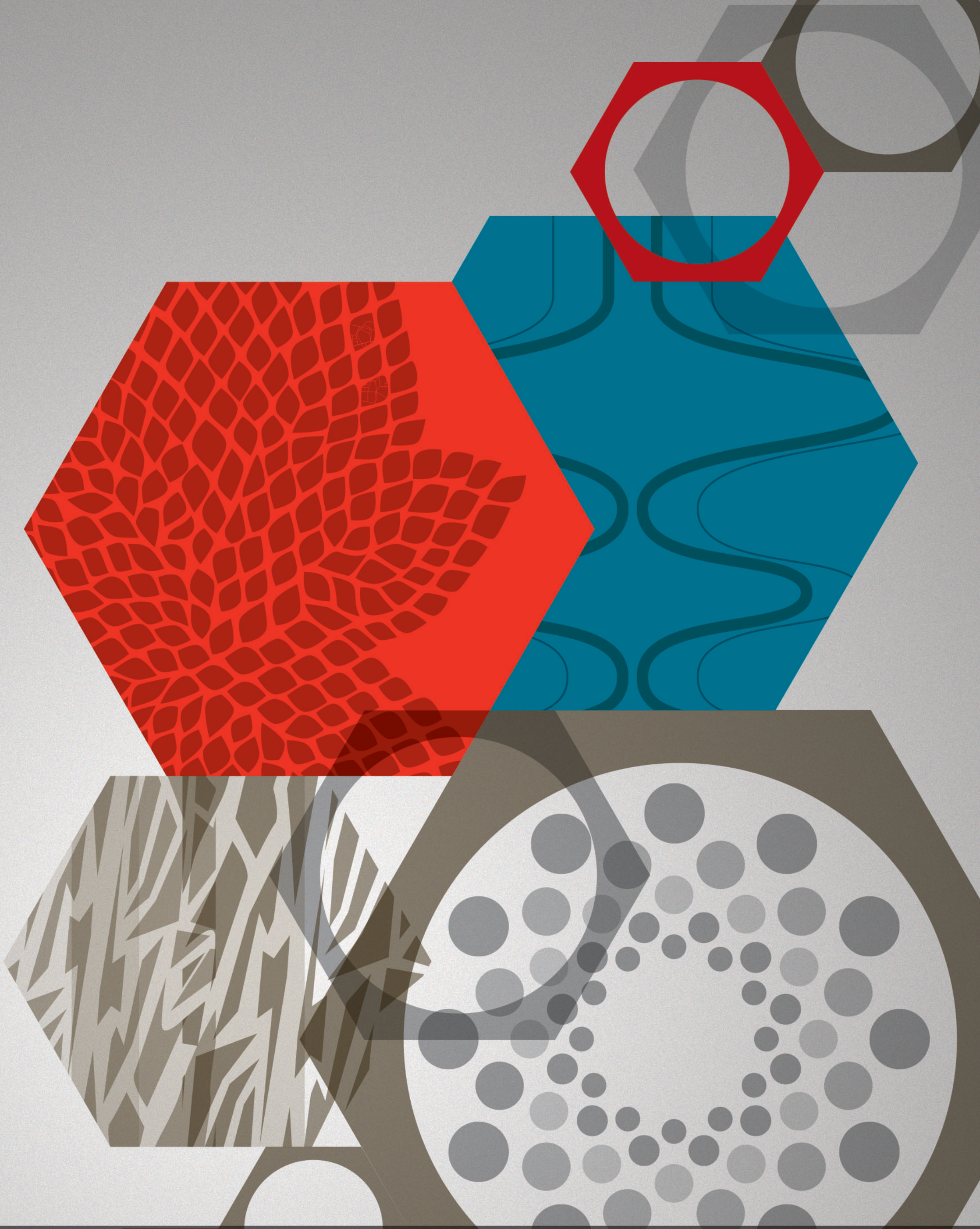

VARONIS COMPLIANCE BRIEF

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) 800-53 FOR FEDERAL INFORMATION SYSTEMS

CONTENTS

OVERVIEW

In 2002, Congress passed the Federal Information Security Management Act (FISMA), which requires federal organizations (and their contractors) to implement “information security protections commensurate with the risk and magnitude of the harm.” FISMA also requires the National Institute of Standards and Technology (NIST) to develop their own standards and guidelines for helping federal organizations improve their security. A list of these publications can be found on the NIST website.

The overall idea is that federal organizations first determine the security category of their information system based on FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems — essentially deciding whether the security objective is confidentiality, integrity, or availability.

And then the organization chooses from a set of baseline security controls in NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations. In complying with FISMA, NIST gives organizations flexibility in choosing the security controls in 800-53 based on their own security goals.

MAPPING NIST 800-53 CONTROLS TO VARONIS SOLUTIONS

The following table maps relevant 800-53 controls to specific Varonis solutions:

800-53 CONTROL FAMILY	DESCRIPTION	VARONIS SOLUTIONS
Identification and Authentication (IA)		
IA-2 Identification and Authentication (Users)	The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).	DatAdvantage software solution identifies and aggregates users, permissions, data and access event information from directories and file servers. Sophisticated analytics applied to the collected information show detailed data use and determine rightful access based on business need.
Access Control (AC)		
AC-2 Account Management	The organization … (c) Establishes conditions for group and role membership (d) Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account	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. **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)..
AC-6 Least Privilege	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	

800-53 CONTROL FAMILY	DESCRIPTION	VARONIS SOLUTIONS

Audit and Accountability (AU)

800-53 CONTROL FAMILY	DESCRIPTION	VARONIS SOLUTIONS
AU-2 Audit Events	The organization: a. Determines that the information system is capable of auditing the following events: information systems… b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;	**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
AU-6 Audit Review, Analysis, and Reporting	The organization: a. Reviews and analyzes information system audit records … b. Reports findings to appropriate personnel ..	
AU-10 Non-repudiation	The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed file copies, moves, or deletes.	

Configuration Management (CM)

800-53 CONTROL FAMILY	DESCRIPTION	VARONIS SOLUTIONS
CM-4 Security Impact Analysis	The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.	**Varonis DatAdvantage** provides actionable intelligence on where excess file permissions andgroup 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.

800-53 CONTROL FAMILY	DESCRIPTION	VARONIS SOLUTIONS
Risk Assessment (RA)		
RA-5 Vulnerability Scanning	The organization: a.Scans for vulnerabilities in the information system and hosted applications ... c. Analyzes vulnerability scan reports and results from security control assessments	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 that we find.
RA-2 Security Categorization	(a) Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;	
RA-3 Risk Assessment	a) Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;	
System and Information Integrity (SI)		
SI-4 Information System Monitoring	The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with ... b. Identifies unauthorized use of information systems ..	**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