

CONTENTS

Overview	1
Traditional/Manual ApproachES.....	1
Varonis Approach.....	2
About The Varonis Metadata Framework	5
Varonis Data Governance Suite.....	6
Varonis DatAdvantage for Windows	
Varonis DatAdvantage for UNIX/Linux	
Varonis DatAdvantage for SharePoint.....	6
Varonis DataPrivilege.....	7
Varonis Data Classification Framework.....	8
Learn More	8

Access Auditing With Varonis

OVERVIEW

Varonis DatAdvantage contains detailed information on every file access event, stored in a normalized database that is easily searched and sorted to answer questions such as:

- Who has been accessing this folder?
- What data has this user been accessing?
- Who deleted these files?
- Where did those files go?

TRADITIONAL/MANUAL APPROACHES

Most IT departments can't answer questions about what actually happened to files—who accessed them, deleted them, moved them, where they went, etc. This is because native windows auditing is resource intensive, voluminous, and cryptic, and therefore rarely enabled.

To enable native windows auditing for file access, first activate audits of successful object access attempts via the local or domain security policy settings.

Next, each folder's auditing settings (known as the SACL) must be modified to include those users you wish to audit. These are enabled in Properties->Security->Advanced->Auditing. If you want to audit all access events by everyone, add the everyone group, and select Success>Full Control.

Once auditing is enabled, events will show up in the security event container. The events must be opened up individually to inspect their contents, or exported. They are difficult to decipher, but not impossible. There is some filtering ability if you know which user you're interested in, but not for directory name, file type, delete events, etc.

Enabling auditing on Solaris requires making use of the BSM Security Auditing command, bsmconv. Reading the results requires outputting them with the command, auditreduce.

Linux 2.6 Kernel auditing involves configuring auditd, and using the command, ausearch to analyze the results.

VARONIS APPROACH

Varonis does not require windows auditing, BSM, or Linux 2.6 Kernel auditing to be enabled; Varonis has written a file system filter to capture these events on windows servers, Solaris, and Linux servers. The filter consumes negligible CPU time and RAM, and does not write to disk on the monitored systems. Varonis also collects audit information from SharePoint, EMC Celerra, and Netapp filers. (For Netapp filers and EMC Celerra DataMovers, Varonis uses their native operating system mechanisms— fpolicy on Netapp, CEPA or Windows analog auditing on Celerra).

Access activity is aggregated, normalized, analyzed, and stored in the Varonis Metadata Framework, and is accessible via the Varonis DatAdvantage and DataPrivilege Interfaces, and reports.

The DatAdvantage GUI allows you to search by directory, by user, by group, by file type, by activity type (open, create, delete, modify, move, etc.), and more, with virtually unlimited combinations, as well as and/or groupings.

For example, to determine who has deleted data in a directory, simply double click the directory, group by Operation type, and expand the Object Removed Events to see a list of all file delete events:

The screenshot shows the Varonis DatAdvantage interface. On the left is a directory tree with 'finance' selected. The main window displays a search query: 'Date between 12/1/2008 12:00:00 AM and 1/14/2009 11:59:59 PM AND Show data from Equals 'File-system events' AND Directory Starts with 'c:\finance''. The results are grouped by 'Operation Type', with 'Object removed (17)' expanded. Below is a table of the results:

Time	File Server / Do...	Operation On	Operation Ty...	Change Description	Operation By	File Type
12/4/2008 12:38:...	FileServer	c:\finance\Econo...	Object removed		Root-Domain\Ann Schoenberger	xls
12/1/2008 10:20:...	FileServer	c:\finance\Control...	Object removed		Root-Domain\Erin Manning	doc
12/1/2008 10:20:...	FileServer	c:\finance\Control...	Object removed		Root-Domain\Erin Manning	doc
12/1/2008 4:44:0...	FileServer	c:\finance\Control...	Object removed		Root-Domain\Erin Manning	DOC
12/1/2008 4:44:0...	FileServer	c:\finance\Control...	Object removed		Root-Domain\Erin Manning	DOC
12/1/2008 10:20:...	FileServer	c:\finance\Control...	Object removed		Root-Domain\Erin Manning	doc
12/2/2008 9:53:0...	FileServer	c:\finance\Control...	Object removed		Root-Domain\Margaret Coakley	DOC
12/1/2008 10:20:...	FileServer	c:\finance\Control...	Object removed		Root-Domain\Erin Manning	doc
12/2/2008 11:09:...	FileServer	c:\finance\Control...	Object removed		Root-Domain\Margaret Coakley	DOC
12/2/2008 11:08:...	FileServer	c:\finance\Control...	Object removed		Root-Domain\Anne Thornton	DOC
12/2/2008 11:52:...	FileServer	c:\finance\Control...	Object removed		Root-Domain\Anne Thornton	DOC
12/1/2008 11:49:...	FileServer	c:\finance\Control...	Object removed		Root-Domain\Anne Thornton	doc
12/2/2008 10:53:...	FileServer	c:\finance\Control...	Object removed		Root-Domain\Anne Thornton	doc
12/1/2008 12:10:...	FileServer	c:\finance\Control...	Object removed		Root-Domain\Anne Thornton	DOC
12/2/2008 10:46:...	FileServer	c:\finance\Econo...	Object removed		Root-Domain\Ann Schoenberger	xls
12/2/2008 4:50:0...	FileServer	c:\finance\Control...	Object removed		Root-Domain\Erin Manning	doc
12/3/2008 4:15:0...	FileServer	c:\finance\Econo...	Object removed		Root-Domain\Eric Adler	xls

To see what a user has been accessing, just double-click on the user:

The screenshot shows the Windows Event Viewer interface. On the left, the 'Users and Groups' pane is expanded to show the user 'melissadonovan'. The main pane displays a search query: 'Query: User Equals 'CORP\Melissa Donovan' AND Directory name Equals 'C:\Share\legal\Corporate\IP' AND Time between 10/4/2009 12:00:00 AM and 8/11/2010 11:59:58 PM AND Show data from Equals 'File-system events''. Below the query is a table of search results.

Time	File Server / Do...	Operation On	Operation Type	Change Description	Operation By	File Type
10/21/2009 7:22:...	corpfs02	C:\Share\legal\Co...	File opened		CORP\Melissa Donovan	doc
10/17/2009 7:22:...	corpfs02	C:\Share\legal\Co...	File opened		CORP\Melissa Donovan	doc
10/15/2009 7:23:...	corpfs02	C:\Share\legal\Co...	File opened		CORP\Melissa Donovan	doc
11/3/2009 7:21:0...	corpfs02	C:\Share\legal\Co...	File opened		CORP\Melissa Donovan	doc
11/5/2009 7:21:0...	corpfs02	C:\Share\legal\Co...	File opened		CORP\Melissa Donovan	doc
10/20/2009 3:03:...	corpfs02	C:\Share\legal\Co...	File opened		CORP\Melissa Donovan	doc
10/29/2009 7:21:...	corpfs02	C:\Share\legal\Co...	File opened		CORP\Melissa Donovan	doc
11/4/2009 7:22:0...	corpfs02	C:\Share\legal\Co...	File opened		CORP\Melissa Donovan	doc
10/30/2009 7:21:...	corpfs02	C:\Share\legal\Co...	File opened		CORP\Melissa Donovan	doc
10/14/2009 7:22:...	corpfs02	C:\Share\legal\Co...	File opened		CORP\Melissa Donovan	doc
11/2/2009 5:45:0...	corpfs02	C:\Share\legal\Co...	File opened		CORP\Melissa Donovan	doc
10/28/2009 12:0...	corpfs02	C:\Share\legal\Co...	File opened		CORP\Melissa Donovan	doc
10/27/2009 9:14:...	corpfs02	C:\Share\legal\Co...	File opened		CORP\Melissa Donovan	doc
10/13/2009 2:39:...	corpfs02	C:\Share\legal\Co...	File modified		CORP\Melissa Donovan	txt
10/13/2009 2:39:...	corpfs02	C:\Share\legal\Co...	Object added		CORP\Melissa Donovan	txt
10/15/2009 7:23:...	corpfs02	C:\Share\legal\Co...	File modified		CORP\Melissa Donovan	txt

Events can be examined in greater detail by double-clicking:

The screenshot shows the 'Details' pane for a specific event. The event details are as follows:

- Time:** 10/13/2009 2:39:00 PM
- File Server / Domain:** corpfs02
- Operation On:** C:\Share\legal\Corporate\IP\letter to network solutions confirming jude's identity.txt
- Operation Type:** Object added
- Operation By:** CORP\Melissa Donovan
- File Type:** txt
- Event Count:** 1
- Last Occurrence:** 10/13/2009 2:39:00 PM
- IP Address/Host:** (empty)

Once you find what you're looking for you can export it right to Excel from Tools>Log>Export to Excel.

The second method is to simply run one of the Varonis DatAdvantage built-in reports, *User Access Log*, specifying a user or group, folder, file, or any combination of numerous available parameters. This report (as with all DatAdvantage reports) can be run on demand, or scheduled to run and be delivered via email or share distribution automatically. The output lists detail for each file access event:

Time	File Server / Domain	Object Type	Operation On	Operation Category	Operation Type	Operation By
10/17/2009 09:42:00 AM	corpfs02	File	C:\Share\legal\Corporate\License Agreements\nikon (sdk+bdk) v-08.doc	Added	Object added	CORP\Melissa Donovan
10/28/2009 12:29:00 PM	corpfs02	File	C:\Share\legal\Corporate\License Agreements\t3g technology co. ltd.(sdk+bdk).txt	Accessed	File modified	CORP\Melissa Donovan
10/30/2009 09:18:00 AM	corpfs02	File	C:\Share\legal\Corporate\License Agreements\Veraz Networks Ltd. (SDK) (V3).txt	Accessed	File modified	CORP\Melissa Donovan
11/04/2009 09:24:00 AM	corpfs02	File	C:\Share\legal\Corporate\License Agreements\nextream france sa (sdk+bdk) v-14 (for menahem's review).doc	Accessed	File opened	CORP\Melissa Donovan
10/14/2009 01:32:00 PM	http://sharepoint	File	/legal (Legal)/Shared Documents/Corporate/License Agreements/miritek (sdk).doc	Accessed	File opened	CORP\Melissa Donovan
10/19/2009 01:02:00 PM	http://sharepoint	File	/legal (Legal)/Shared Documents/Corporate/License Agreements/innoteletek (sdk+bdk amendment) (added products).doc	Accessed	File modified	CORP\Melissa Donovan
10/21/2009 12:09:00 PM	http://sharepoint	File	/legal (Legal)/Shared Documents/Corporate/License Agreements/diebold incorporated (sdk) (4).doc	Accessed	File opened	CORP\Melissa Donovan
10/22/2009 02:10:00 PM	http://sharepoint	File	/legal (Legal)/Shared Documents/Corporate/License Agreements/olympus (sdk+bdk) v-05 (clean).doc	Accessed	File modified	CORP\Melissa Donovan

ABOUT THE VARONIS METADATA FRAMEWORK

Ongoing, scalable data protection and management require technology designed to handle an ever-increasing volume and complexity—a metadata framework.

Four types of metadata are critical for data governance:

- User and Group Information – from Active Directory, LDAP, NIS, SharePoint, etc.
- Permissions information – knowing who can access what data in which containers
- Access Activity – knowing which users *do* access what data, when and what they've done
- Sensitive Content Indicators – knowing which files contain items of sensitivity and importance, and where they reside

The Varonis metadata framework non-intrusively collects this critical metadata, generates metadata where existing metadata is lacking (e.g. its file system filters and content inspection technologies), pre-processes it, normalizes it, analyzes it, stores it, and presents it to IT administrators in an interactive, dynamic interface. Once data owners are identified, they are empowered to make informed authorization and permissions maintenance decisions through a web-based interface—that are then executed—with no IT overhead or manual backend processes.

The Varonis Data Governance Suite will scale to present and future requirements using standard computing infrastructure, even as the number of functional relationships between metadata entities grows exponentially. As new platforms and metadata streams emerge, they will be seamlessly assimilated into the Varonis framework, and the productive methodologies it enables for data management and protection.

VARONIS DATA GOVERNANCE SUITE

Varonis provides a complete metadata framework and integrated product suite for governing unstructured data on file servers, NAS devices and (semi-structured) SharePoint servers. Varonis DatAdvantage, DataPrivilege, and the Data Classification Framework provide organizations the ability to effectively manage business data through actionable intelligence, automation of complex IT tasks, and sophisticated workflow management.

Varonis DatAdvantage for Windows

Varonis DatAdvantage for UNIX/Linux

Varonis DatAdvantage for SharePoint

DatAdvantage provides a single interface through which administrators can perform data governance activities.

- Visibility
 - Complete, bi-directional view into the permissions structure of unstructured and semi-structured file systems:
 - Displays data accessible to any user or group, and
 - Users and groups with permissions to any folder or SharePoint site
 - User and group information from directory services is linked directly with file and folder access control data
- Complete Audit Trail
 - Usable audit trail of every file touch on monitored servers
 - Detailed information on every file event in a normalized database that is searchable and sortable
 - Data collection performed with minimal impact to the file server and without requiring native Windows or Unix auditing
- Recommendations and Modeling
 - Actionable intelligence on where excess file permissions and group memberships can be safely removed without affecting business process
 - Model permissions changes without affecting production environments
- Data Ownership Identification
 - Statistical analysis of user activity effectively identifies business owners of data
 - Automated reports involve data owners in data governance processes
 - Facilitates round-trip data owner involvement via DataPrivilege

VARONIS DATAPRIVILEGE

DataPrivilege automates data governance by providing a framework for users and data owners to be directly involved in the access review and authorization workflows. A web interface for data owners, business users, and IT administrators automates data access requests, owner and IT authorization of changes, automated entitlement reviews, and business data policy automation (e.g. ethical walls). A complete audit trail ensures that data governance policies are in place and being adhered to.

- Automated Entitlement Reviews
 - Data owners are provided scheduled entitlement reviews with recommendations for access removal (generated by DatAdvantage)
 - Reviews can be scheduled based on business policy
- Access Control Workflow
 - Users can request access to data and group resources directly, providing explanation and duration
 - Data owners and other stakeholders are automatically involved in authorization process
 - Permissions changes are carried out automatically once approval requirements are met
 - Permissions revocations are carried out automatically on their assigned expiration
- Business Policy Implementation
 - Multiple levels of authorization provide automated implementation of business and IT data governance policy
 - Ethical wall functionality enforces data access policies
- Complete Self-Service Portal
 - Data Owners can view and manage permissions on their data and groups without requiring elevated access privileges, if desired
 - Data Owners can view access activity and statistics about their data, if desired
- Complete Audit Trail and Reporting
 - All workflow events are recorded for audit and reporting which can prove the enforcement of governance practices
 - Authorizations, Entitlement reviews, and other management reports provide evidence of process adherence

Varonis Data Classification Framework

The Varonis Data 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—from either the included classification engine or from a third-party classification product—alongside the rest of the Varonis metadata in the DatAdvantage interface, DCF enables actionable intelligence for data governance, including a prioritized report of those folders with the most exposed permissions AND containing the most sensitive data.

- Actionable Intelligence
 - Classification information provides visibility into business-critical content from within the Varonis IDU
 - Organizations can see where their most sensitive data is over-exposed along with actionable recommendations on where that access can be reduced
- Extensible Architecture
 - The provided data classification engine provides a powerful and flexible method for classifying sensitive data through regular expressions and dictionary searches.
 - The Data Classification Framework can also integrate content classification data from third-party classification and DLP products, extending the ability of both
 - Intelligent, fast
 - True incremental scanning is attained with DatAdvantage real-time knowledge of all file creations and modifications—only new data is classified
 - Produces rapid-time-to-value results that have a clear remediation path or “next step”
 - Produces results dramatically faster than traditional approaches
- Leverages existing infrastructure
 - Can use either its built-in classification engine or those already deployed
 - Uses the unique meta-data layer created by the Varonis Intelligent Data Use (IDU) Framework
 - Builds on the foundation of the Varonis IDU Framework, with no need for additional servers or storage
 - Results flow into Varonis DatAdvantage and Varonis DataPrivilege (*future*)
- Easy, powerful classification rules
 - Rules match a combination of content AND meta-data conditions (e.g. creator, accessing user, permissions sets)
 - Prioritization based on Varonis metadata (e.g. scan the most exposed folders first)
 - Files are searched for keywords, phrases and/or regular expression patterns
 - Dynamic/auto-updated dictionary matching capabilities

Learn More

Phone: 877-292-8767

sales@varonis.com

www.varonis.com/products