



WHITEPAPER

3 Ways Varonis Helps You Fight Insider Threats

Contents

Overview	3
1. Rapid Detection and Response	10
2. Data Lockdown	11
3. Data Cleanup	12
Summary	13
Get a Personalized Risk Assessment	17

Overview

Insider threats keeping your executives up at night? They'll probably always be worried, and rightly so, but there are things you can do to help them get a little shuteye, and get in a few extra winks for yourself, while you're at it.

First, while insiders use data, they build up a profile – what kinds of data they use, how much, when, and from which devices. Just like your credit card company builds a profile of your spending habits to spot fraud, automation can build a profile of insider data habits to spot signs that someone may be abusing their access.

Second, why should insiders have so much access in the first place? Risk assessments show that, on average, 20% of all folders are accessible to every employee or contractor, usually by mistake. A lot of this data turns out to be sensitive – almost half of organizations have at least 1,000 sensitive files open to every insider. All it takes is one sensitive file to ruin a lot more than a few nights' sleep. If you're worried about insider threats, why allow insiders more access to data than they absolutely need, especially when there's a very practical alternative?

Third, data has a shelf life, but it stays on the shelf a lot longer than it needs to. On average, 71% of data hasn't been touched in months, or longer. Stale data doesn't add much value, but it adds to your risk, and wastes storage that probably isn't free. Getting stale data out of harm's way and onto cheaper storage should be a set it and forget it kind of thing.

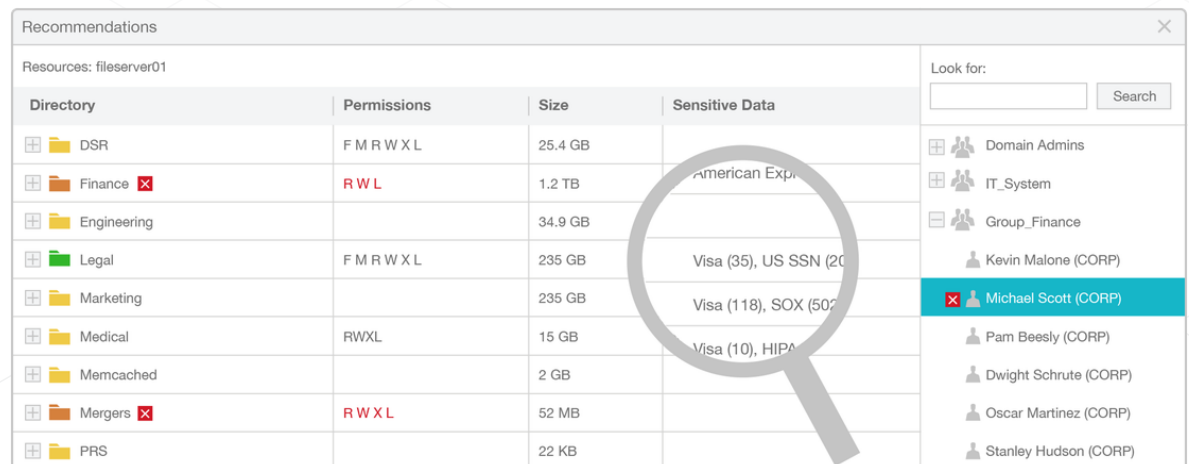
Here's how Varonis helps with all three areas ►

1

Rapid Detection and Response

Varonis DatAdvantage captures more information about how users interact with data than any other technology – it analyzes file system activity on platforms that provide adequate auditing through their API's, like those from Netapp and EMC and in Office365, and uses file system filters to capture metadata for platforms where native auditing is lacking, like Windows, Unix, Exchange, and SharePoint.

Varonis DatAdvantage also collects critical Active Directory events, like logon events and group changes, and with Varonis Edge, telemetry from DNS servers, web proxies and VPN concentrators. DatAdvantage also collects permissions/access control list information, and with the Data Classification Engine, looks inside files to discover sensitive information, like personal data, medical records and financial information.



Recommendations

Resources: fileserver01

Directory	Permissions	Size	Sensitive Data
DSR	F M R W X L	25.4 GB	
Finance	R W L	1.2 TB	American Express
Engineering		34.9 GB	
Legal	F M R W X L	235 GB	Visa (35), US SSN (20)
Marketing		235 GB	Visa (118), SOX (50)
Medical	R W X L	15 GB	Visa (10), HIPA
Memcached		2 GB	
Mergers	R W X L	52 MB	
PRS		22 KB	

Look for: Search

- Domain Admins
- IT_System
- Group_Finance
- Kevin Malone (CORP)
- Michael Scott (CORP)**
- Pam Beesly (CORP)
- Dwight Schrute (CORP)
- Oscar Martinez (CORP)
- Stanley Hudson (CORP)

Varonis DatAlert analyzes all this activity, permissions and content information, identifies executives, service accounts, and administrators, and profiles normal use. When DatAlert detects a meaningful deviation from normal behavior, it signals that an attack may be underway and can even automate responses.

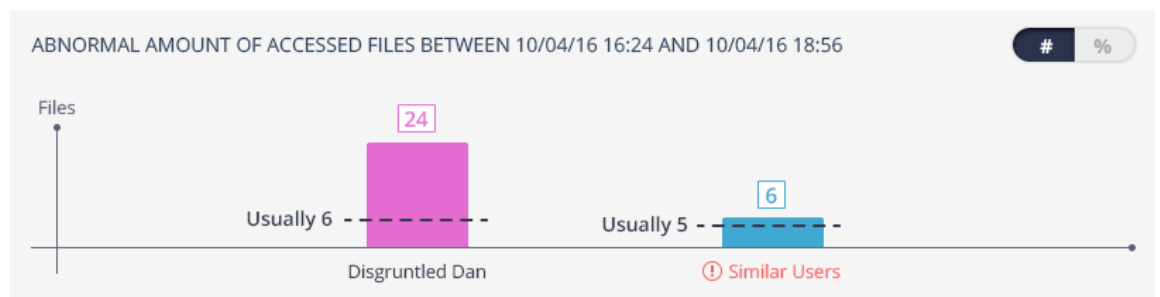
For example, if a user normally accesses a handful of sensitive files each day, and then one day accesses many more, he will trigger an alert. If they normally don't access much stale data, and start to access a lot more over a week or so, they will trigger an alert. If an administrator normally doesn't read an executive's email, and then starts reading and marking their messages and unread, DatAlert will catch it. DatAlert has over 100 built-in threat models that look for unusual patterns of access using User Behavior Analytics.

▲ CRITICAL | **🕒 RECONNAISSANCE**

Abnormal behavior: Unusual amount of access to sensitive files


Disgruntled Dan accessed 24 system files, exceeding normal behavior (6 files) by 300%

[Threat model info](#) ▾



With some threat models, like those that detect ransomware that moves past an endpoint and starts encrypting files on accessible file systems, some customers use DatAlert to notify IT and then shut down the compromised accounts automatically – before they do serious damage.

With the detailed audit log captured by DatAdvantage, it's possible to assess damage quickly. Instead of searching through logs or workstations, you can run a query for all the access activity by any user over any time period to identify all the files or emails they accessed, changes they made, and whether any files were sensitive.

Activity Log				
Look for:		Drag a column header here to group by that column		
<input type="text" value="Allen"/> <input type="button" value="Search"/>				
 Allen Carey (CORP)	1:51:00 PM	Windows	C:\Share\Finance\Billing.xlsx	File Opened
	2:11:00 PM	NetApp	C:\Share\Finance\Staffing.docx	File Deleted
	2:22:00 PM	Exchange	Mailbox Store\Amy Bolton	Attachment Deleted
	2:25:00 PM	Exchange	Mailbox Store\Amy Bolton	Mark All as Unread
	3:01:00 PM	EMC Isilon	C:\Share\Legal\S-1.pdf	Permissions Changed
	3:03:00 PM	Active Directory	Dwight Schrute (Domain Admins)	Group Membership Added
	5:55:00 PM	SharePoint	drop-database	File Modified
	5:59:00 PM	Active Directory	corp.local/users/Andy Bernard	User Locked Out
	6:05:00 PM	Active Directory	corp.local/users/Andy Bernard	Password Reset

2

Data Lockdown

One of the biggest soft spots for insider threats is shared folders, which typically hold 10 to 1,000 times more data than on a laptop or a workstation. In the 2017 Varonis Data Risk Report, we found that 20% of all shared folders were open to every employee. One rogue user could potentially steal any part of 20% of your data without requiring any more sophistication than mapping a drive.

Varonis DatAdvantage analyzes file system permissions, user and group relationships, and activity to find overly broad access granted through global groups (like everyone, authenticated users, and domain users), permissions malfunctions, and excessive group memberships. DatAdvantage also provides the ability to model or sandbox changes to reduce access, and then execute them, safely. The Varonis Data Classification Framework can help you prioritize remediation efforts by identifying sensitive and regulated content, and the Varonis Automation Engine can safely remove global access groups over entire shares or servers – automatically. By reducing broad access, an insider can do far less damage.

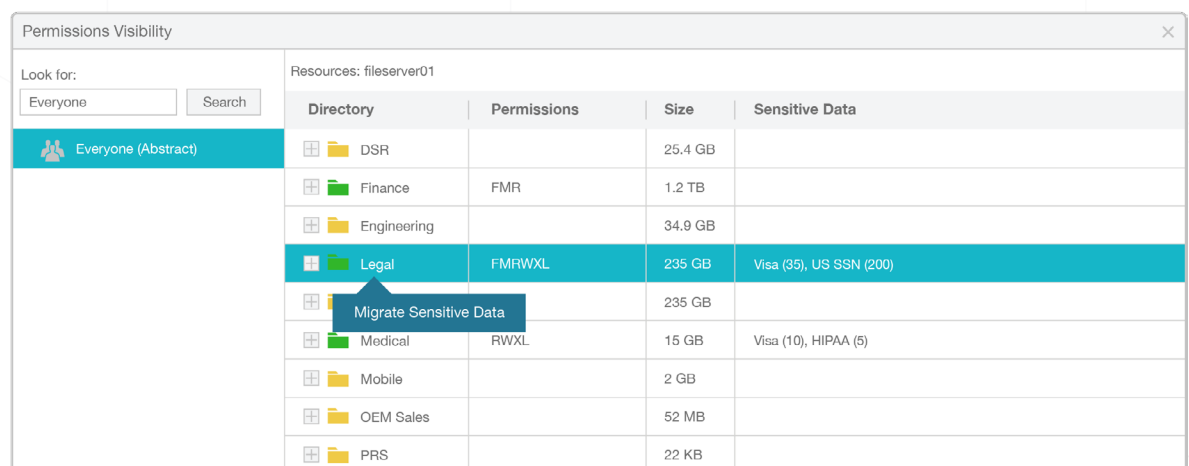
Recommendations			Look for:	
Resources: DirectoryServices			<input type="text"/>	<input type="button" value="Search"/>
Directory	Permissions	Size		
DSR	F M R W X L	25.4 GB	Domain Admins	
Finance	R W L	1.2 TB	IT_System	
Engineering		34.9 GB	Group_Finance	
Legal	F M R W X L	235 GB	Kevin Malone (CORP)	
Marketing		235 GB	Michael Scott (CORP)	
Medical	R W X L	15 GB	Pam Beesly (CORP)	
Memcached		2 GB	Dwight Schrute (CORP)	
Mergers	R W X L	52 MB	Oscar Martinez (CORP)	
PRS		22 KB	Stanley Hudson (CORP)	

3

Data Cleanup

Varonis automates data disposition and clean-up projects. Sensitive data that's exposed to all insiders can be locked down or quarantined. Non-business data can be deleted. Data that hasn't been accessed for a long time can be moved to cheaper storage and restricted. The Varonis Data Transport Engine allows you to define rules to identify data that meets criteria for sensitivity and relevance, move or delete it, even translating permissions across data stores and domains.

By reducing the amount of accessible stale and sensitive data, you can reduce the scope of damage an insider can do.



The screenshot shows the 'Permissions Visibility' window in the Varonis interface. It displays a table of resources for 'fileserver01'. The table has columns for Directory, Permissions, Size, and Sensitive Data. The 'Legal' directory is highlighted in blue, and a tooltip 'Migrate Sensitive Data' is shown over it. The 'Sensitive Data' column for 'Legal' lists 'Visa (35), US SSN (200)'. Other directories include DSR, Finance, Engineering, Medical, Mobile, OEM Sales, and PRS.

Directory	Permissions	Size	Sensitive Data
DSR		25.4 GB	
Finance	FMR	1.2 TB	
Engineering		34.9 GB	
Legal	FMRWXL	235 GB	Visa (35), US SSN (200)
Medical	RWXL	15 GB	Visa (10), HIPAA (5)
Mobile		2 GB	
OEM Sales		52 MB	
PRS		22 KB	

Summary

By combining sophisticated analytics with content analysis and permissions management, Varonis protects you from insider threats with rapid detection, optimized access controls, and data-driven policy enforcement. In addition to insider threats, Varonis also protects organizations from malware, APT's and hijacked accounts with a data-centric approach, focusing on some of the most valuable, voluminous and vulnerable concentrations of data -- file and email systems stored on premises and in the cloud. The Varonis Data Security Platform helps you make sure you answer the most important security question: Is my data safe?



“ Varonis is a
Fantastic Solution ”



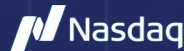
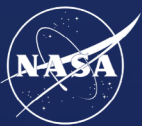
DatAlert is the most-reviewed UEBA production
Gartner Peer Insights.

[Read about customer results →](#)

ABOUT VARONIS

Varonis is a pioneer in data security and analytics, specializing in software for data security, governance, compliance, classification, and analytics. Varonis detects insider threats and cyberattacks by analyzing file activity and user behavior; prevents disaster by locking down sensitive data; and efficiently sustains a secure state with automation.

We help thousands of customers prevent data breaches.



Get a Personalized Risk Assessment



Data Risk Assessment

Get your risk profile, discover where you're vulnerable, and fix real security issues.

info.varonis.com/start



Live Demo

Set up Varonis in your own environment and see how to stop ransomware and protect your data.

info.varonis.com/demo

