VARONIS SECURITY SOLUTIONS

Despite the enormous growth and increasing value of content stored across file shares, intranets, SharePoint, and the cloud, many organizations still lack the security intelligence required to protect unstructured data. Without a scalable way to identify sensitive content, monitor access, and alert on abnormal user behavior, organizations become vulnerable to data breaches and struggle to remain compliant.

> *"Organizations should use file analysis to gain a true understanding of their unstructured data, where it resides and who has access to it."*[i]
>
> –Gartner

Varonis helps security teams ensure that only the right people have access to data at all times, monitor all use, and alert on abuse.

COMMON SECURITY USE CASES:

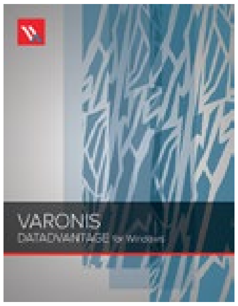
1. Alert on permissions changes to critical folders
2. Alert on privilege escalations and GPO changes in Active Directory
3. Prevent malware infections like CryptoLocker
4. Alert on abnormal user behavior (e.g., insider threats)
5. Lock down overexposed sensitive data

Security Challenge:

Can’t identify insider threats or risky user behavior.

Varonis Solution:

DatAdvantage tracks and analyzes user data access on unstructured data—behavioral analytics. By establishing a baseline of normal activity for each user, our framework can detect and alert when anomalous or undesirable activity—like a malware infiltration or a trusted insider gone bad—occurs.



Security Challenge:

Can’t identify privilege escalations and other critical events in Active Directory.

Varonis Solution:

DatAdvantage for Directory Services gives you a granular audit trail for Active Directory, showing you who escalated privileges for whom, when, and what the user did with their administrative access.

DatAlert can notify you of privilege escalations in real-time by sending an alert to your SIEM, syslog, or via email.

Security Challenge:

No audit trail or monitoring for file, email, or SharePoint access.

Varonis Solution:

DatAdvantage non-intrusively monitors activity across a wide array of platforms—Windows, NAS, SharePoint, Exchange, Active Directory, UNIX/Linux—and stores activity in a normalized database that is sortable and searchable.

A complete audit trail is critical for forensics investigations, detecting risky activity, and monitoring key assets. Varonis can feed your SIEM with the unstructured data activity that it’s been missing.

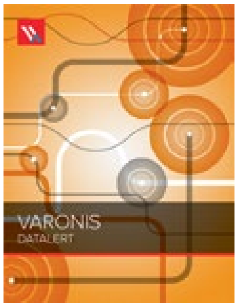
Security Challenge:

Can’t detect and recover from malware like CryptoLocker.

Varonis Solution:

DatAlert allows you to configure real-time alerts based on activity thresholds (e.g., modifying more than 500 files in 5 minutes), which is critical to detecting malware like CryptoLocker. Send alerts your SIEM, syslog, via email, and even automate a response to disable a user account or revoke access.

If malware such as CryptoLocker does hit your servers, **DatAdvantage** can help pinpoint exactly which files and folders were impacted, making recovery much easier.

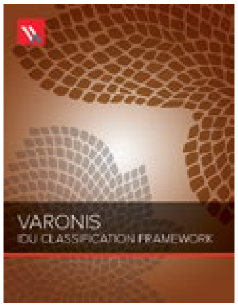


Security Challenge:

Can’t identify where sensitive information resides or who can access it.

Varonis Solution:

The **Data Classification Framework** incrementally scans and classifies sensitive information, shows you who *can* access it, who *has been* accessing it, and highlights the highest concentrations of sensitive data that are most at risk and provides a clear methodology to safely remediate that risk without manual effort. Already classifying? Great! DCF can ingest classification data to make it actionable.



Security Challenge:

Trouble identifying and remediating global access groups, such as “Everyone” or “Authenticated Users”.

Varonis Solution:

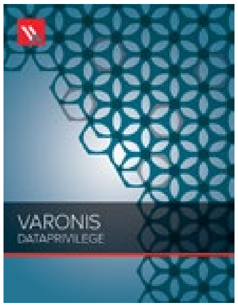
DatAdvantage will show you where global access groups are applied across multiple platforms and who has been using them. You can run simulations to see the potential impact if you were to revoke global access, based on who has been accessing data through these groups in the past. Once you’ve determined that your permissions changes won’t do any harm you can commit (and rollback) changes directly from the DatAdvantage interface.

Security Challenge:

Users have access to more data than they need to do their job (i.e., permissions creep).

Varonis Solution:

DatAdvantage’s highly accurate recommendation engine uses machine learning to predict which permissions users really need and tells you which permissions can be locked down without disrupting productivity.
With **DataPrivilege**, you can deliver access control recommendations directly to designated decision–makers in the business who can revoke access without IT’s assistance.



IS YOUR UNSTRUCTURED DATA PROTECTED?

In two easy steps, we'll help you find risk areas, audit access, and take control of your data.

Yes, I'd like a free risk assessment

http://bit.ly/expressrisk

Our Express Assessment Report will summarize key findings, rank identified weaknesses in order of risk, and provide a recommendation for remediation. The report includes detail on areas such as:

- Overly accessible folders containing important or regulated content
- Overly accessible hierarchies and data structures
- Folders with stale information
- Users with too much access
- Unused, enabled user accounts

WHAT PEOPLE ARE SAYING

"Varonis is on an extremely short list of companies that supply products I wouldn't be without in any major executive role in any public company, three-letter agency, government office, or IT firm."

–Rob Enderle
President and Principal Analyst, The Enderle Group

[1] *Market Guide for File Analysis Software. Alan Dayley, Garth Landers, Debra Logan, Earl Perkins. 23 September 2014.*