VARONIS SECURITY SOLUTIONS

PROTECT YOUR DATA FROM:

- Insider threats
- Outsider threats
- Malware activity
- Privilege Escalations
- Exploitation
- Privilege Account Abuse
- Lateral Movement
- Data Exfiltration
- Potential data breaches
- Compromised assets

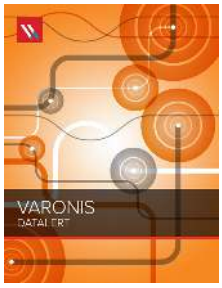
Detect cyberattacks and identify insider threats

ANALYZE DATA, ACCOUNT ACTIVITY, AND USER BEHAVIOR

Varonis captures more metadata about unstructured data and file systems than any other solution: **DatAdvantage** non-intrusively monitors activity across a wide array of platforms—Windows, NAS, SharePoint, Exchange, Active Directory, UNIX/Linux, and Office365.

DatAdvantage tracks and analyzes user data access on unstructured data. 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. Identify privilege escalations, GPO changes, and other critical events before it leads to a data breach.

MONITOR SUSPICIOUS BEHAVIOR AND UNUSUAL ACTIVITY



DatAlert performs user behavior analytics to automatically profile the entities that use data – employees, executives, administrators, and service accounts – and alert on suspicious activity. Varonis UBA Threat Models utilize thresholds, statistical analysis and machine learning to trigger alerts on what looks unusual and uncover potential security issues. Send alerts to your SIEM, syslog, or via email, and even automate a response to disable a user account or revoke access.

Prevent disaster by locking down sensitive and stale data, reducing broad access, and simplifying permissions.

Quickly lock down sensitive and stale data:

The **Data Classification Framework** incrementally scans and classifies sensitive information, shows you who has been accessing it, and highlights sensitive data that is most at risk while providing a clear methodology to safely and automatically remediate that risk. DCF can also ingest existing classification data to make it actionable. **DatAdvantage** fixes global access groups and identifies data that hasn't been touched in months or years so you can get it safely out of harm's way. **Data Transport Engine** automates quarantining, migrations and disposition.

Simplify permissions, groups and Active Directory

DatAdvantage helps structure shared data so that permissions are applied near the top of the hierarchy with single-purpose groups (groups that aren't used anywhere else) with subfolders and files inheriting all permissions.

Get to a least privilege model:

DatAdvantage identifies data owners using a combination of access activity, permissions, and Active Directory metadata. Entitlement reviews can be carried out by the data owners rather than IT. Using a patented recommendations algorithm, DatAdvantage highlights users that likely no longer need access.

Sustain a secure state by automating authorizations, migrations, and disposition.

Continually monitor and handle critical data:

DatAlert and **DatAdvantage** alert and report on deviations from policy, and when possible, correct those deviations automatically. Sensitive files in the wrong places are automatically quarantined, and stale data is automatically archived or deleted with the **Data Transport Engine**.

Automate authorization:

Data Privilege automates and tracks access requests, reviews, and approvals – so that employees quickly get access to only the information they need. Users make requests, data owners approve them through email, a help-desk system or web application, and the changes are implemented automatically – no IT involvement required. Entitlement reviews, access grants and revocations are tracked and inspected for adherence to business policy.