

# Data Insight 6.1

## Overview Data Sheet

Veritas™ Data Insight provides enterprise-class risk analytics to help organizations illuminate the darkest corners of their file environment. By triangulating content classification, metadata attributes and user behavior forensics, Data Insight gives users actionable intelligence that permeates—no matter how large or complicated the data landscape is.

### THE VERITAS INTEGRATED CLASSIFICATION ENGINE

Powered by the Veritas Integrated Classification Engine, Data Insight can unearth the hidden risk in dark data and identify personal data. The Integrated Classification Engine gives users the capability to create custom policies to tag information based on content of these files.

The Veritas Integrated Classification Engine comes pre-loaded with patterns to detect over 100 sensitive data types such as date of birth, social security numbers, credit card numbers and medical records. It includes more than 60 pre-configured policies for GDPR, HIPAA, Sarbanes-Oxley and other regulations relevant to different countries and industries.

The machine learning algorithm uses contextual information within Data Insight to prioritize how to crawl through dark data. Rather than spend months on classification, Data Insight can classify on a targeted basis to comply to GDPR requirements in as little as 72 hours.

Data Insight uses metadata across multiple content sources. It tracks security descriptors and uses user metadata—not just file metadata—to deliver intelligence. User metadata can include attributes like job function, department and geo location. This allows users to dynamically query the environment and understand the information-leveraging context of the file.



Data Insight's user behavior forensics help to build a baseline of activity metrics which can then be used to identify anomalies and trigger responses against policy. This also feeds into understanding the value of data. This is determined by assessing how many unique users interacted with a file and the level of transactions. It is then easier to differentiate between WORN (written once read never) data versus data that is mission critical.

- **Symantec DLP integration:** Data Insight integrates tightly with Symantec DLP for data at rest. This is a 2-way integration where Data insight utilizes content and policies from DLP and DLP utilizes ownership, permission and activity analytics for remediation and risk scoring capability.
- **Third party DLP tag ingestion:** Other DLP vendors and classification engines can tie-in with Data Insight using CSV import mechanism.

### THE RISK BASED APPROACH TO EVERY FILE, FOLDER AND EVERY USER USES AN ADVANCED, RISK-CENTRIC ALGORITHM THAT EVALUATES THE SENSITIVITY OF YOUR DATA. HIGHLIGHTS INCLUDE:

- **Risk Score:** User risk analysis aggregates anomalous activity, access patterns and sensitive content interaction into a single metric—the risk score. Customizable policies within Data Insight identify which data is at risk of exposure.
- **Risk dossier:** Risk dossier provides an interactive way to further analyze the risk score through a deep dive into factors like as number of alerts generated for a user, anomalies, access to shares, and user attributes.
- **Near real time access alerting for sensitive data:** Data Insight has access alerting capability for sensitive files (as identified through the Classification Engine or DLP) in order to stop leakage of risky data.

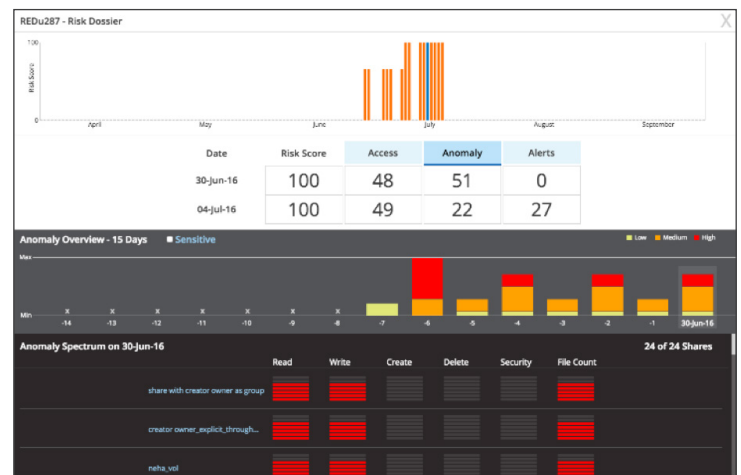


Figure 1: Risk dossier provides deeper context into risk score

- **Insider threat analysis:** Data Insight can protect against insider threats in the organization through the multi-dimensional analysis of permissions, deviations and alerts that are against access policies. This feeds into the user risk scoring that provides information around where to focus for further in-depth analysis.
- **Data use policy alerts:** Data use policy alerts in Data Insight help identify anomalous user activity or irregular activity on sensitive data.
- **Social network maps:** Social network maps that visualize how file shares are being accessed by different users enable detection of permission inconsistencies and improve on secure collaboration processes. Using Data Insight, admins can determine users who are under or over-connected to find people who are outside the normal patterns of collaboration or access. Collaboration points can be analyzed using Data Insight to understand if permissions structures are in order.
- **Flexible query interface:** A flexible query interface enables custom risk analysis and filtering based on data attributes, identity context, access exposure and activity.
- **Ransomware detection templates:** Data Insight comes with pre-built ransomware detection templates that can detect ransomware through read and write count variables.

## THE ACTIONABLE INSIGHT TRANSLATES RISK SCORES INTO INFORMED, CONFIDENT DATA MANAGEMENT ACTIONS.

- **Flexible actions framework:** The flexible actions framework simplifies remediation efforts by automating monitoring, migration and protection of data. Administrators are armed with single-click access to classify, interrogate and archive data all from Data Insight's easy-to-use workbench.
- **Native file system archiving capability:** With tight integration with Enterprise Vault File System Archiving, Data Insight provides data archiving and retention capability. Users can archive files directly from Data Insight with a single click and implement actions and retention policies as created in Enterprise Vault.
- **Chargeback/Consumption reporting:** Data Insight can show storage consumed by owner or department based on ownership and storage reporting capabilities. This enables action around accountability in end-user behavior towards storage usage.
- **Permissions recommendations:** By using permission visibility and analytics around activity, Data Insight is able to recommend users or groups that should be de-provisioned from a File System's Access Control List.

- **Compliance reports/templates:** Data Insight comes with various custom report templates (DQL templates) and permission search templates that can help users with their compliance efforts across data and access.

- **Access certification/Entitlement reviews workflow:** The access certification workflow helps users to involve business owners or data custodians to look at the permissions for the data they own and make decisions to revoke access of unwanted or inactive users and provide accountability for data they own.

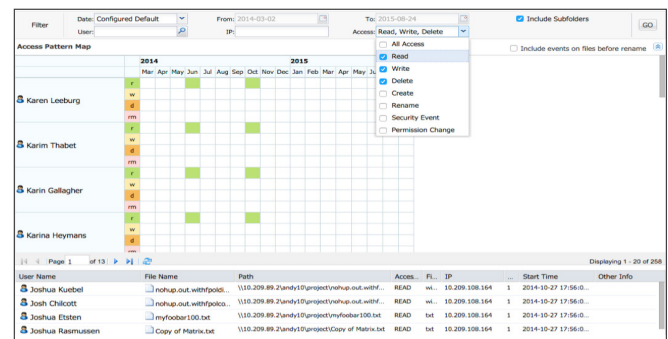


Figure 2: User forensics for granular view into access

- **Permission de-provisioning orchestration:** Data Insight provides in- context action capability for de-provisioning of access in directory services like AD and from File System ACLs. User can remove user or group from or remove from group from a parent group.
- **Permissions search reporting:** Data Insight provides permission search capability to slice and dice Access Control Lists, Access Control Entries and group permissions and pinpoint permission hygiene issues in the environment. It ships various in-built templates to easily identify control points where permissions are inaccurately provisioned or providing unwanted access to users.
- **Permission what-if/Group change impact analysis:** Data Insight provides information for the critical business impact that can lead to any remediation action. This helps identify if revocation policies are appropriate before they are implemented.

- **Custom actions for remediation (third party integration):** Data Insight presents a custom action framework using which customers can tie in any actions with Data Insight analytics and take action right from the interface on-demand or automate using report scheduling and post-processing invocation of custom actions.

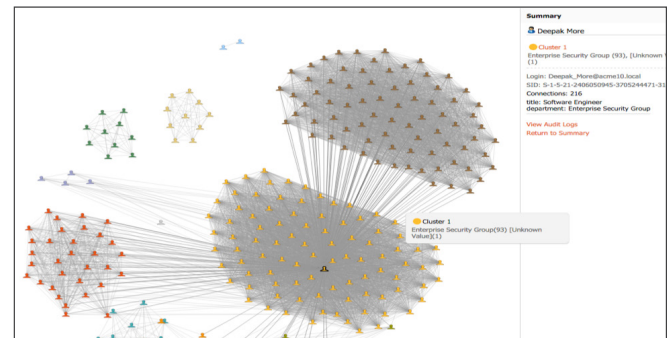


Figure 3: Social Network Map visualizes permissions

- **Policy (Automated Rule) based data management:** Data Insight has a flexible query/custom reporting engine that is tied to the scheduler and actions framework. Utilizing the post-processing remediation from rules created within reports, users can automate data movement, migration, tiering, archiving etc. on a repeatable basis.
- **Records classification workflow:** Data insight helps to utilize content classification and tie into pre-defined content-retention policy mapping to archive and automate the process according to retention requirements.

## DATA INSIGHT IS SCALABLE AS YOUR REQUIREMENTS CHANGE AND YOUR ORGANIZATION GROWS.

Data Insight grows and adapts with your architecture and infrastructure, using machine learning to drive efficient scanning. The engine learns about the specific attributes of the data without going into the file, and then uses that information to decide the most likely areas of importance. This leads to more efficiency and faster turnaround.

Data Insight captures data from multiple data sources. Currently Data Insight supports the following:

- Microsoft Windows® File Server
- EMC® Unity
- MSFT® OneDrive for Business
- Netapp® (7 mode)
- Hitachi NAS
- MSFT® Sharepoint Online
- Netapp® Cluster Mode
- MSFT® Sharepoint
- OpenText Documentum
- EMC® Celerra/VNX
- Box
- Generic CIFS/NFS
- EMC® Isilon®
- Veritas™ File System

For more information, visit <https://www.veritas.com/datainsight>

## ABOUT VERITAS TECHNOLOGIES LLC

Veritas Technologies empowers businesses of all sizes to discover the truth in information—their most important digital asset. Using the Veritas platform, customers can accelerate their digital transformation and solve pressing IT and business challenges including multi-cloud data management, data protection, storage optimization, compliance readiness and workload portability—with no cloud vendor lock-in. Eighty-six percent of Fortune 500 companies rely on Veritas today to reveal data insights that drive competitive advantage. Learn more at [www.veritas.com](http://www.veritas.com) or follow us on Twitter at [@veritastechllc](https://twitter.com/veritastechllc).

Veritas Technologies LLC  
500 East Middlefield Road  
Mountain View, CA 94043 USA  
+1 (866) 837 4827  
[veritas.com](http://veritas.com)

For specific country offices and contact numbers, please visit our website.  
[www.veritas.com/about/contact](http://www.veritas.com/about/contact)

**VERITAS™**

The truth in information.

V0130 04/18