Data Insight

Veritas Data Insight helps enterprises proactively assess and mitigate unstructured and sensitive data security risks. With Data Insight, you can classify sensitive data in a hybrid cloud environment and arm your operations team with the key knowledge needed to identify security threats and prepare compliance audits more efficiently. Combining data visibility, context and analytics across your whole infrastructure allows IT to gain relevant knowledge to improve data governance and resolve security, compliance, insider and cyber threats quickly and conclusively.

The Veritas Integrated Classification Engine

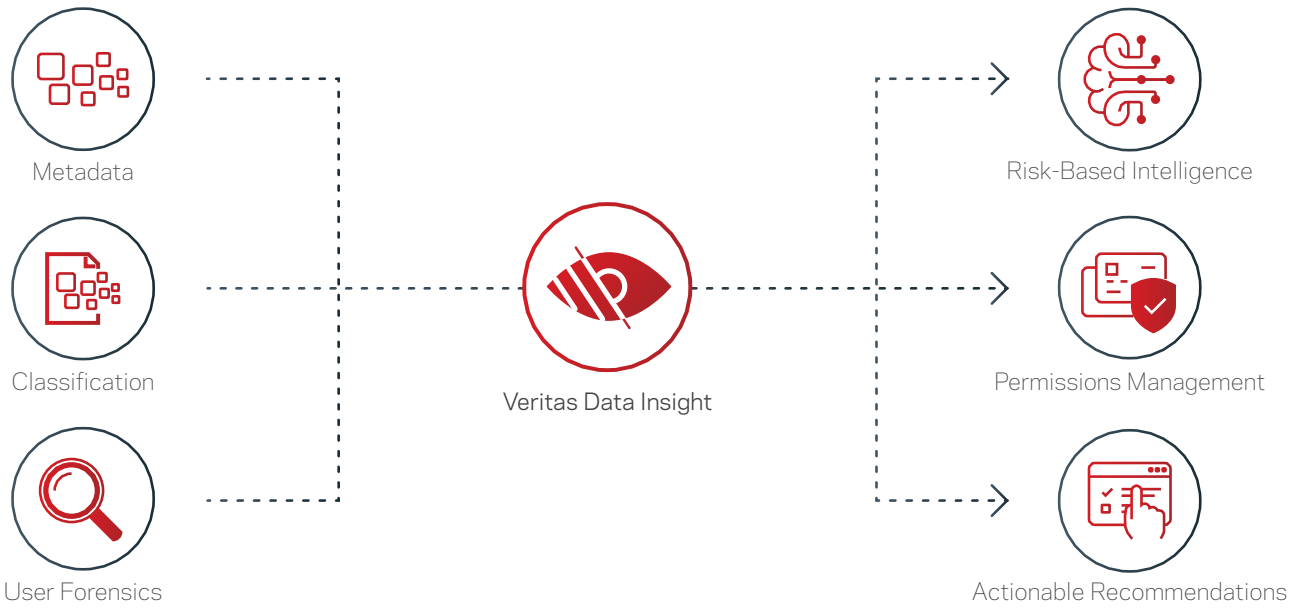
Powered by the Veritas Integrated Classification Engine, Data Insight can unearth the hidden risk in dark data and identify personal data. The Integrated Classification Engine gives users the ability to create custom policies to tag information based on the content of these files.

The Veritas Integrated Classification Engine comes pre-loaded with patterns to detect around 1,200 sensitive data patterns such as date of birth, social security numbers, credit card numbers and medical records. It includes 275+ pre-configured policies for GDPR, HIPAA, Sarbanes-Oxley and other regulations for different industries, and personal data policies relevant to 60+ different countries.

Optical character recognition (OCR) enables extracting text from images and scanned documents to detect sensitive data. Exact Data Match capability identifies any sensitive information in the environment using exact matches rather than a pattern.

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 with 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 process 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. (See Figure 2.) This information also feeds into understanding the value of data. The value 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 Data Loss Prevention (DLP) integration:** Data Insight integrates tightly with Symantec DLP for data at rest. This is a two-way integration where Data Insight leverages content 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 the CSV import mechanism.

The Risk-Based Approach to Every File, Folder and 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 the number of alerts generated for a user, anomalies, access to shares and user attributes. (See Figure 1.)

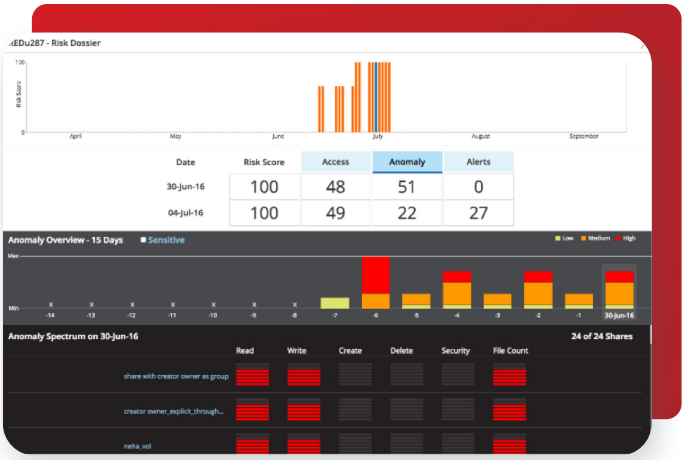


Figure 1. Data Insight's risk dossier provides deeper context around risk scores.

- **Near-real-time access alerting for sensitive data and risky users:** Data Insight offers quick access alerting capability for sensitive files—as identified through DLP or Veritas Integrated Classification Engine—to stop leakage of sensitive data. The quick access alerting capability also allows monitoring and detecting of any potential malicious activity by users.
- **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 information 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 secure collaboration processes. (See Figure 3.) Using Data Insight, administrators 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 that can be integrated with business intelligence tools like Microsoft PowerBI.
- **Ransomware detection templates:** Data Insight comes with pre-built ransomware detection templates that can detect ransomware through read and write count variables. Veritas regularly updates Data Insight's ransomware identification policies.

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 deletion capability:** Data Insight provides built-in data deletion capability for file systems that helps get rid of ROT (Redundant, Obsolete and Trivial) data. Privileged users can delete files directly from Data Insight with a single click and can automate this data remediation action via user-defined policy.
- **Native file system archiving capability:** With tight integration with Veritas 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 created in Enterprise Vault.
- **Microsoft Purview Information Protection labels:** Set MIP labels for data from Data Insight. Provide insight to build policies around data protection and compliance. Label unlabeled files requiring protection, rectify mislabeled files to ensure compliance and security, and automate MIP label creation based on content context to save time on existing and newly created documents.

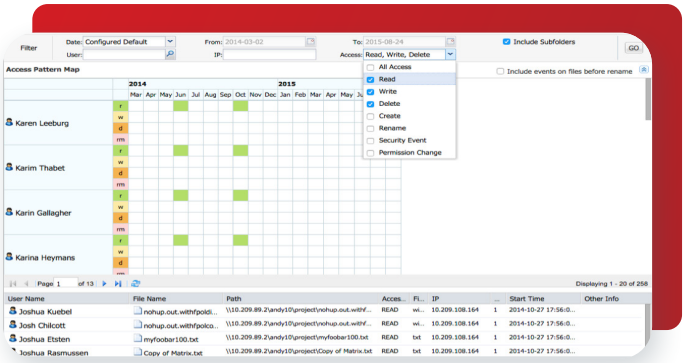


Figure 2. User forensics provides a granular view of access.

- **Chargeback/Consumption reporting:** Data Insight can show storage consumed by the owner or department based on ownership and storage reporting capabilities. This information promotes accountability and efficient storage consumption practices in the organization.
- **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 (ACL).
- **Monitor Compliance:** 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:** The access certification workflow helps users involve business owners or data custodians in looking at the permissions for the data they own and making decisions to revoke access of unwanted or inactive users and provide accountability for data they own. (See Figure 2.)
- **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.
- **Permissions search reporting:** Data Insight provides permission search capability to slice and dice ACLs, Access Control Entries and group permissions and pinpoint permission hygiene issues in the environment. It ships with various built-in templates to easily identify control points where permissions are inaccurately provisioned or provide 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 information helps identify if revocation policies are appropriate before they are implemented.

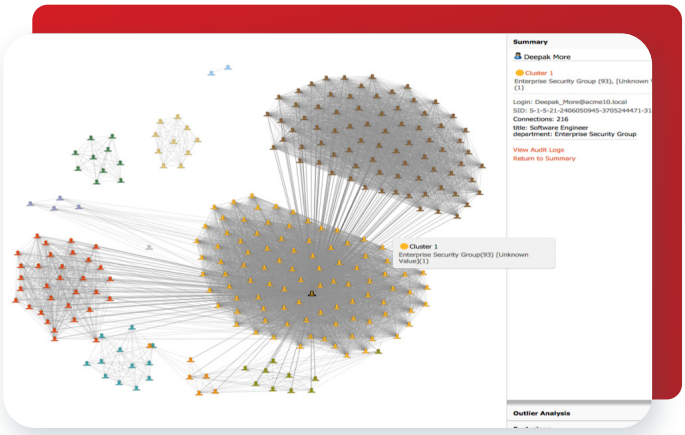


Figure 3. Social Network Maps help visualize user permissions.

- **Custom actions for remediation (third-party integration):** Data Insight presents a custom action framework customers can use to tie in any actions with Data Insight analytics and take action right from the interface on demand or automate.
- **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 and archiving on a repeatable basis.
- **Records classification workflow:** Data insight helps use content classification and tie into pre-defined content-retention policy mapping to archive to Enterprise Vault and automate the process according to retention requirements.

Data Insight is Scalable as Your Requirements Change and Your Organization Grows

Data Insight is based on a distributed architecture purpose-built to scale to multi-PB environments. 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 approach leads to more efficiency and faster turnaround.

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

- Amazon S3
- Box
- EMC® Celerra/VNX
- EMC® Isilon® / PowerScale
- EMC® Unity
- Generic CIFS/NFS
- Hitachi NAS
- Microsoft Windows® File Server
- Microsoft® OneDrive for Business
- Microsoft® SharePoint
- Microsoft® SharePoint Online
- NetApp® (7 mode)
- NetApp® Cluster Mode
- Veritas File System

About Veritas

Veritas Technologies is a leader in multi-cloud data management. Over 80,000 customers—including 95 percent of the Fortune 100—rely on Veritas to help ensure the protection, recoverability, and compliance of their data. Veritas has a reputation for reliability at scale, which delivers the resilience its customers need against the disruptions threatened by cyberattacks, like ransomware. No other vendor is able to match the ability of Veritas to execute, with support for 800+ data sources, 100+ operating systems, 1,400+ storage targets, and 60+ clouds through a single, unified approach. Powered by Cloud Scale Technology, Veritas is delivering today on its strategy for Autonomous Data Management that reduces operational overhead while delivering greater value.

VERITAS

V0130 06/23