Define, Detect, & Defend Sensitive & Confidential Data
DataGravity for Virtualization

Security at the Point of Storage

Whether it is confidential information about clients, patients, and employees or critical intellectual property and trade secrets, your most valued data is increasingly at risk. Potential risks go beyond fines, lawsuits, and lost revenue. Failing to manage this data effectively can have damaging repercussions to your business' reputation and may even impact its long term financial viability.

With more than 75% of all data breaches being caused by employee carelessness or malicious behavior, access authentication at the perimeter is no longer sufficient. With two thirds of end users reporting that they have access to data they shouldn't be seeing, it's no wonder that over 90% of organizations feel vulnerable to insider threats. Moving forward, organizations need to adopt a zero-trust security model - protecting data and data access at every layer – from the perimeter through the network and down to the storage system.

Enhance your data's security by simply identifying sensitive data and tracking users' access
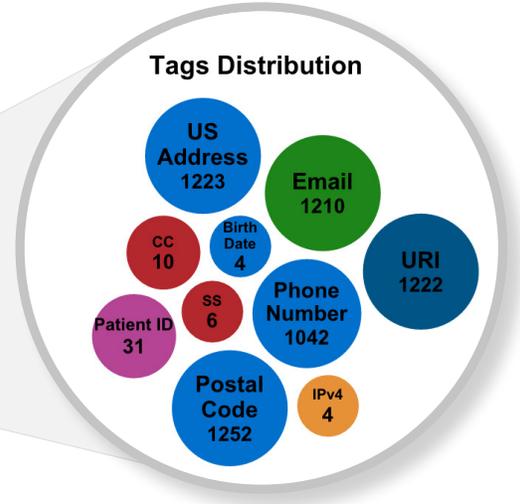
Preempt Sensitive Data Loss

- Simply identify files containing sensitive data
- Be alerted when data is exposed

Simplify Auditing and Reporting

- Know what files users are accessing and when
- Export detailed reports for compliance and remediation

Respond to Breaches More Quickly

- Assess exposure risks and impacts
- Quickly restore data lost to breaches, malware and malicious users

EASILY FIND AND PROTECT SENSITIVE DATA

DataGravity for Virtualization advanced analytics make it simple to find sensitive data within your data sets, assess risk exposure, and take action.

Preempt Data Loss by Managing Risks to Your Data

DataGravity for Virtualization is the only data security solution designed to protect your data in the place where it lives, embedded within your virtualized environment. Seamlessly deployed as a virtual appliance, DataGravity provides timely intelligence and actionable insights to secure and protect your entire virtualized data infrastructure.

Advanced monitoring, analytics, and alerting provide you with a 360 degree view of all your data. With DataGravity for Virtualization, you define policies to automatically discover the data that is valuable to you, detect anomalous user access behaviors, and defend your data against careless exposure, data loss, malicious users, ransomware and regulatory non-compliance.

Easily assess your risks by understanding where your sensitive data lives, if it has been exposed, and how broadly it has been accessed.

Find and Protect Sensitive Data

By analyzing content from over 600 file types, DataGravity for Virtualization automatically identifies sensitive data within the data that it stores. Files within the system are indexed for fast query and analysis, and tagged for sensitive content, including pre-defined tags such as credit card numbers, date of birth, addresses, social security numbers and e-mail addresses. Custom tags can also be created specific to your environment to identify files containing account numbers, patient or student IDs, or internal classification codes.

Insight Profiles are used to group tags and assign them to virtual machines, providing granular control over what sensitive data types to look for. Profiles can be tailored for specific departments and workflows, and to comply with specific internal or regulatory mandates, for example, HIPAA and PCI-DSS. The system actively scans files according to schedules you define, identifying and surfacing sensitive data files for evaluation and remediation.

Results are reported in "click and drill" dashboards so that additional details can be easily retrieved. Users can also create and save advanced queries to search for specific tags, keywords, users and time frames. For the most rapid notification of security concerns, users may subscribe to these saved searches for immediate email notification. In all cases, detailed reports are exportable for further review, remediation, and compliance reporting.

Track and Audit Data Usage

DataGravity for Virtualization tracks and audits data access, providing in-depth visibility and understanding of usage patterns across all stored data files. You can identify what data is being accessed, who has accessed it, what operations have been performed, and when these actions occurred. Armed with this knowledge, system administrators, compliance officers and security analysts can understand and assess exposure risk, respond to inappropriate access, and take action to remove or relocate improperly stored files.

Audit logs are maintained not only for files, but also for each user, including privileged users. They are searchable and filtered by user, activities, and timeframes to provide insights and forensic analysis of security incidents. As a result, any user's activities can be audited and analyzed for irregular access patterns and data usage that may be indicative of malicious intent, improper usage, or malware infiltration. Audit logs are easily exported for additional analysis, review, and compliance reporting.

Be Secure. Be Data Aware.

Knowing what data you have, where it is located, and who has access to it are necessary for managing and protecting your most sensitive information. Yet, most organizations lack the tools to gather this most fundamental knowledge. Preventing data loss requires you to become data aware.

In contrast to solutions that require additional servers, databases and costly professional services, DataGravity for Virtualization deploys as a single virtual appliance that is easy to configure and manage. By gathering data intelligence as it happens and correlating people, content and time, you have a comprehensive solution that defines, detects and defends your sensitive data and its usage.

ENHANCE YOUR DATA'S SECURITY WITH DATAGRAVITY

DataGravity for Virtualization helps you ensure your data is securely managed, its confidentiality preserved, and its access limited.

DataGravity®