

# Securely Manage Data in a Virtualized Environment

## DataGravity for Virtualization

### Proactive resource management with data awareness and security

Here's a story some IT pros know all too well: by the process of elimination, you often serve as your company's de facto security, compliance and governance expert. Perhaps your organization's smaller size prohibits the existence of a dedicated team for such functions. Or, after your company went through a phase of rapid growth, the team tends to approach security initiatives from a rear-view perspective. In any case, you're in charge of analyzing and protecting the organization's core data and infrastructure, which happens to be fully virtualized. With the introduction of virtualization, data becomes push-button mobile. It's now free to roam the company.

Luckily, IT pros tend to step up to challenges by nature. To build an actionable plan for data security, governance and compliance, it's critical to start with the data itself. DataGravity enables IT teams to uncover exactly what they're storing, where sensitive data is located within their environments and who has access to that information. Some organizations uncover misplaced records containing credit card numbers, while others notice employees have been filling the company's storage space with video files. Mapping this information creates a 360-degree view of virtualized data assets, which you can use to improve operations and curb security risks.

### Protect sensitive data, meet compliance objectives and curb VM sprawl

Content-aware auditing delivers file, user and system insights

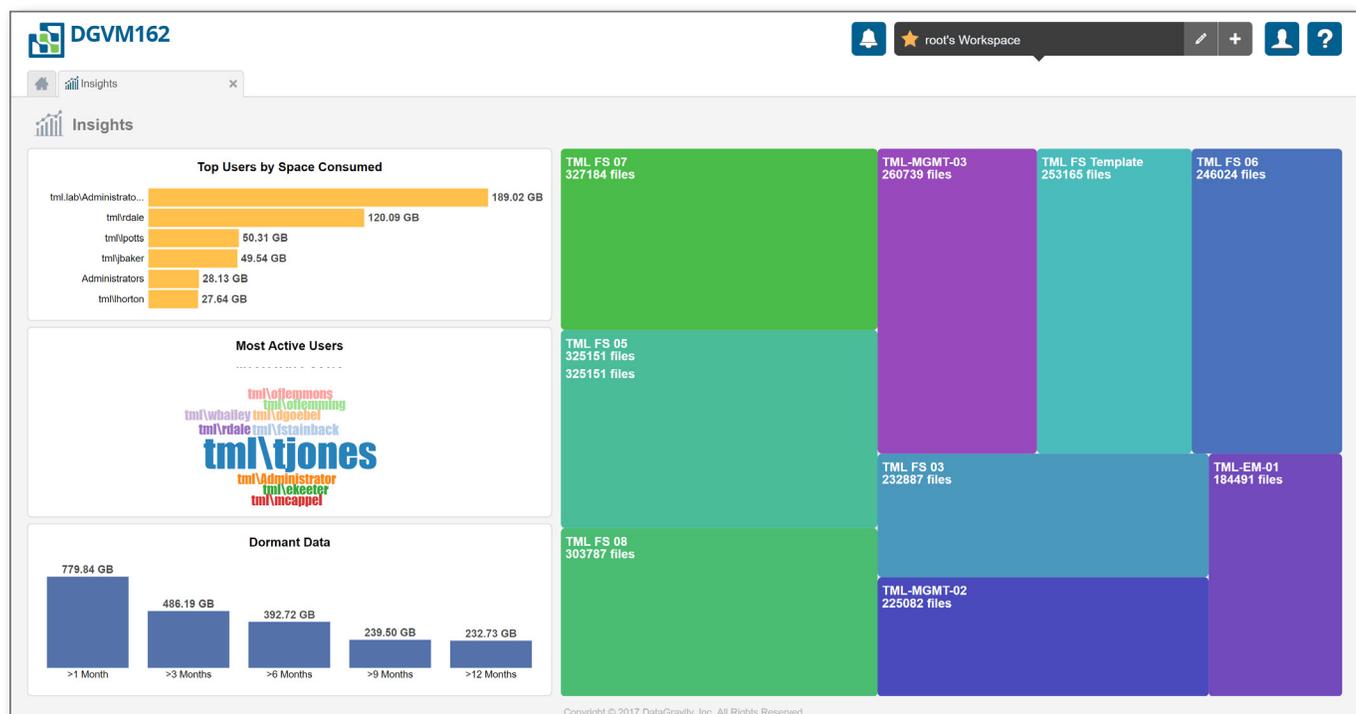
- Map audit trails across users and files
- Enhance storage and IT management by removing dangerous or unnecessary data

### Meet compliance goals in every industry

- Identify when files breach compliance guidelines before they wreak havoc
- Create data-driven processes for ongoing compliance and remediation

### Stop sensitive data loss

- Receive alerts about data exposure and loss
- Proactively take action to increase sensitive data security and protection



### OVERCOME YOUR DATA SPRAWL

Know how your data is being used and by whom for better data security, regulatory compliance and resource usage.

## Discover, define, detect and defend sensitive data

Virtualization helps consolidate server workloads, improve system performance and cut data center costs. However, it can spur data growth and virtual machine (VM) sprawl, adding complexity and complications to data management and backup procedures. Virtualized environments also tend to house sensitive information and mission-critical operations – and according to Kaspersky Lab, a security attack on virtualized infrastructure can cost twice as much as one targeted only at physical servers and endpoints.

To protect critical data, organizations need to understand how it's being used. By analyzing content from more than 600 file types, DataGravity for Virtualization uncovers sensitive elements within your virtualized data. Advanced monitoring, analytics and alerting give users the ability to define policies for recognizing valuable information, detecting anomalous user access behaviors and defending data against risks. With these insights, organizations can make informed decisions to combat risks like data loss, malicious users, ransomware and compliance issues.

## Meet compliance objectives

Depending on the industry, organizations likely need to adhere to certain data compliance regulations and protocols. DataGravity for Virtualization maintains audit logs for files and individual users, shining light on how virtualized data assets are being used (and by which users). Users can identify and attend to data containing noncompliant information before a third-party audit incurs fines and penalties on the organization.

To meet specific industry compliance needs, DataGravity users can customize search functions and target regulations such as PCI-DSS, HIPAA, FERPA and more. While auditing data to ensure compliance, DataGravity simultaneously identifies security risks and protects data that is left unencrypted or stored in locations that are not adequately password and permission-protected.

## Quickly recover critical data

Sooner or later, most organizations will experience a disruption in IT processes. Whether a security attack, hardware failure, natural event or other issue causes the interruption, the IT team will likely be tasked with restoring operations and data.

DataGravity users can avoid the complexity of restoring an entire VM just to recover individual files. As DataGravity DiscoveryPoints catalog file changes within storage-based snapshots, you can simply find and recover files that were lost, damaged or deleted. After previewing file versions, finding and restoring the right one is as simple as a single click.

## Be secure. Be data aware.

Often, a security or IT incident begins with a single user. Analyzing abnormal user access patterns and conducting regular data audits can indicate the presence of malware, rogue users and bigger security threats on the horizon. DataGravity monitors your virtual environment, recognizes suspicious behaviors and works with your storage and IT system to protect virtualized data. If an incident does occur, DataGravity helps your team identify patient zero, assess damage and facilitate recovery. In short, DataGravity delivers the insight and tools your organization needs to shut down security and compliance issues, curb VM sprawl and improve IT management on a wide scale.

## Get a free data security assessment from DataGravity today.

[Learn more](#)

### DEFEND AGAINST THE RISKS TO YOUR DATA

Secure and protect sensitive data, detect malicious data access, and quickly respond and recovery from ransomware attacks.



100 Innovative Way, Suite 3410 Nashua, NH 03062 603.943.8500 datagravity.com

