WHITE PAPER

DATAGRAVITY AND VEEAM

BETTER TOGETHER

DataGravity®

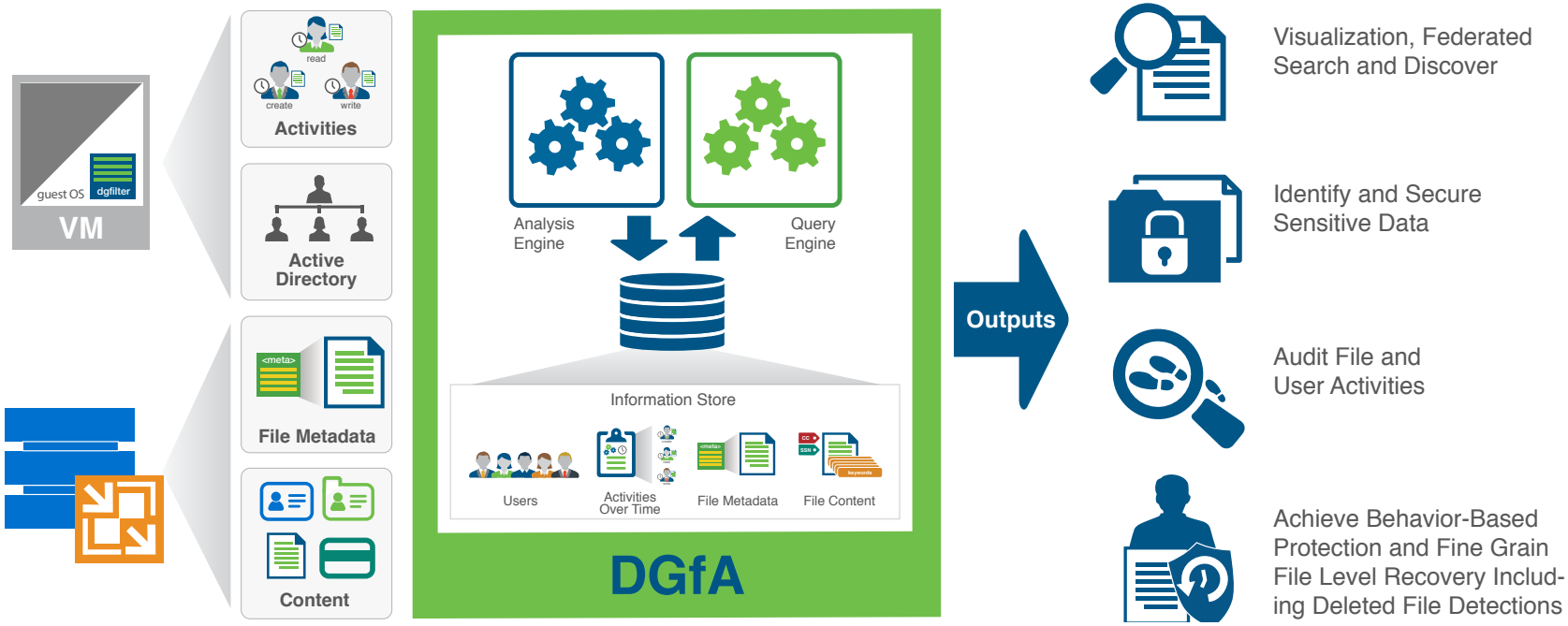
Introduction

When it comes to protecting and ensuring availability of the Always-on Enterprise, Veeam is peerless. DataGravity for Availability is the only product on the market today that both secures and protects virtual machines. Whether running in production or stored in a Veeam backup repository, the two solutions work together seamlessly for complete protection of virtual machines.

DataGravity extends the capabilities delivered by Veeam, giving administrators an enhanced feature set which includes:

- Enhanced recovery capabilities
- Sensitive data detection and management
- File and user audit information
- Data visualization
- Behavior driven data protection

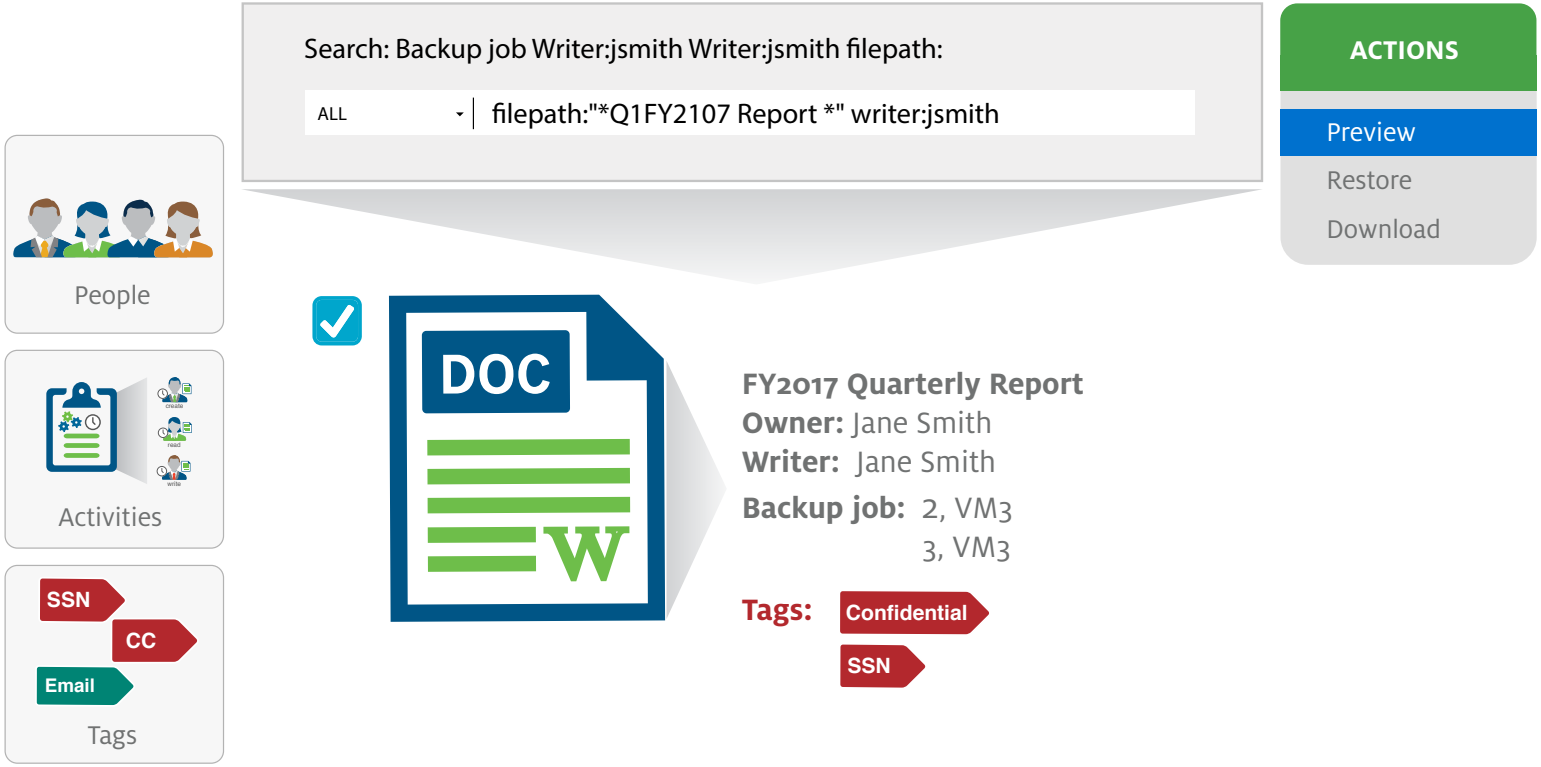
These additional smart capabilities allow administrators to carry out data recovery in a more intelligent and targeted manner, while also automatically creating a forensic trail to meet data compliance, regulatory objectives, and the insight to do quick, targeted restores.



Enhanced Recovery Capabilities

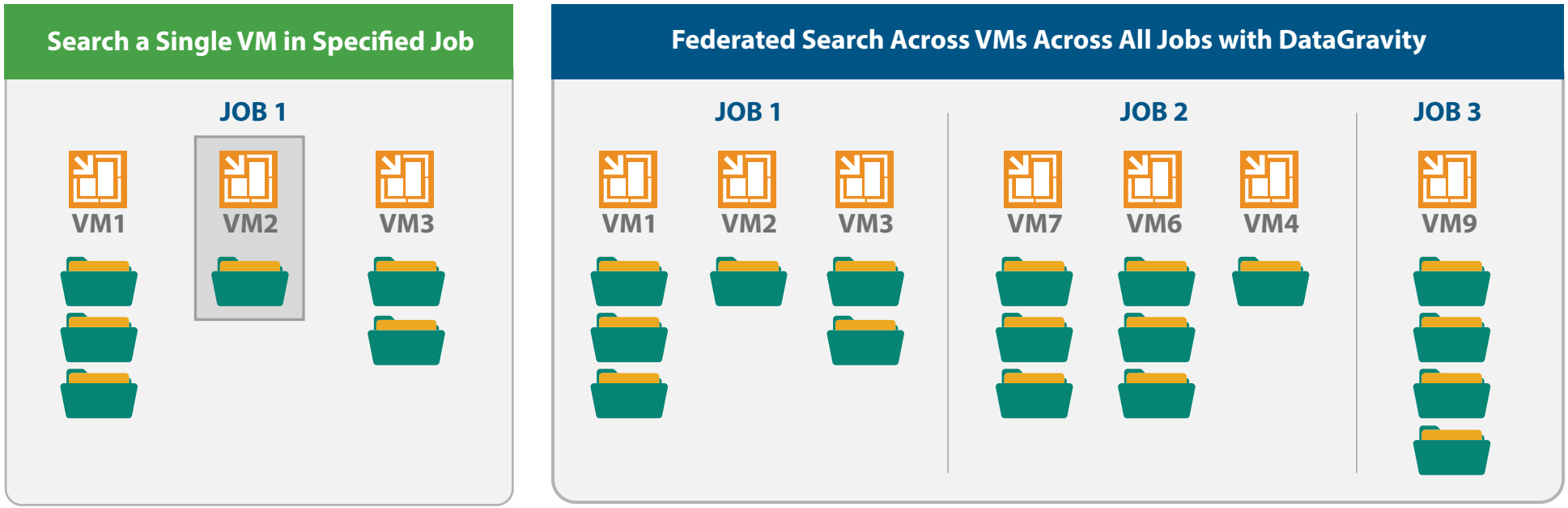
Locating files you need to restore fast is critical when restoring an entire system from backup, as is the ability to restore just the minimal set of files required. When DataGravity and Veeam are used together, the DataGravity federated content-aware search engine enables faster discovery of vital files to recover within Veeam's backup repository.

Data loss is never acceptable. During the restoration process, administrators must restore back to a previous point in time to correct an issue. This will likely result in loss of data and could result in fixing some problems while creating new ones. With DataGravity forensic search, administrators don't just know exactly what to restore; they also know the exact results the restoration will yield.



Federated Search

DataGravity extends Veeam's search capacity to consolidate all jobs in your backup repository, making it easier than ever to find the files you need. Ultimately, the guesswork has been taken out of the equation, eliminating redundant searches.



Search Beyond File Names

DataGravity enhances the search experience through multi-faceted queries with additional parameters, allowing administrators to be much more specific when searching for a file, leading to faster, more accurate results.

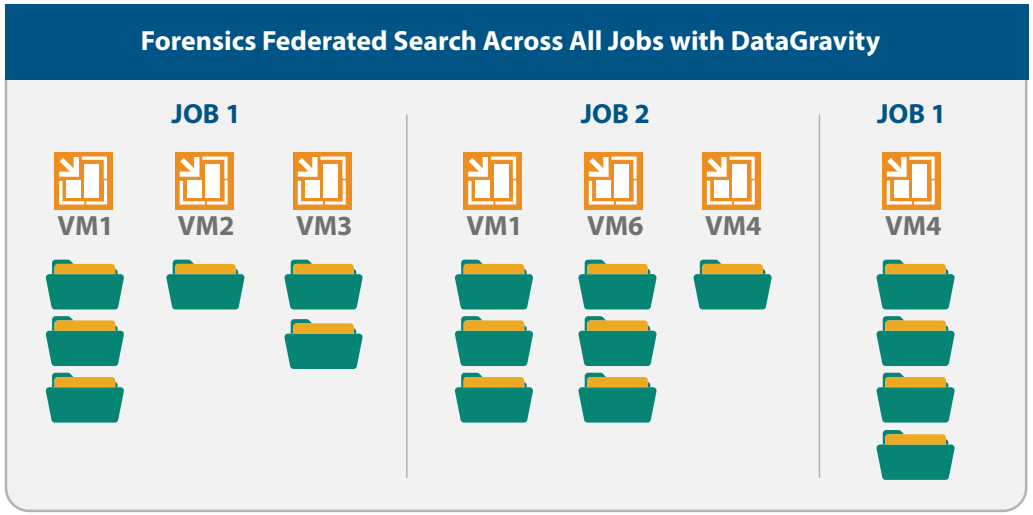
There is also an optional search capability allowing you to search based on user interaction with the file and the tasks performed on the file.

Searches can be based on:

- File Names
- File Path
- File Properties
- Content
- Tags
- Users
- Activities
- Ownership

Find all sales compensation plans with social security numbers

ALL | Tags: SSN "Sales Compensation plans" Modified: 2014-01-14

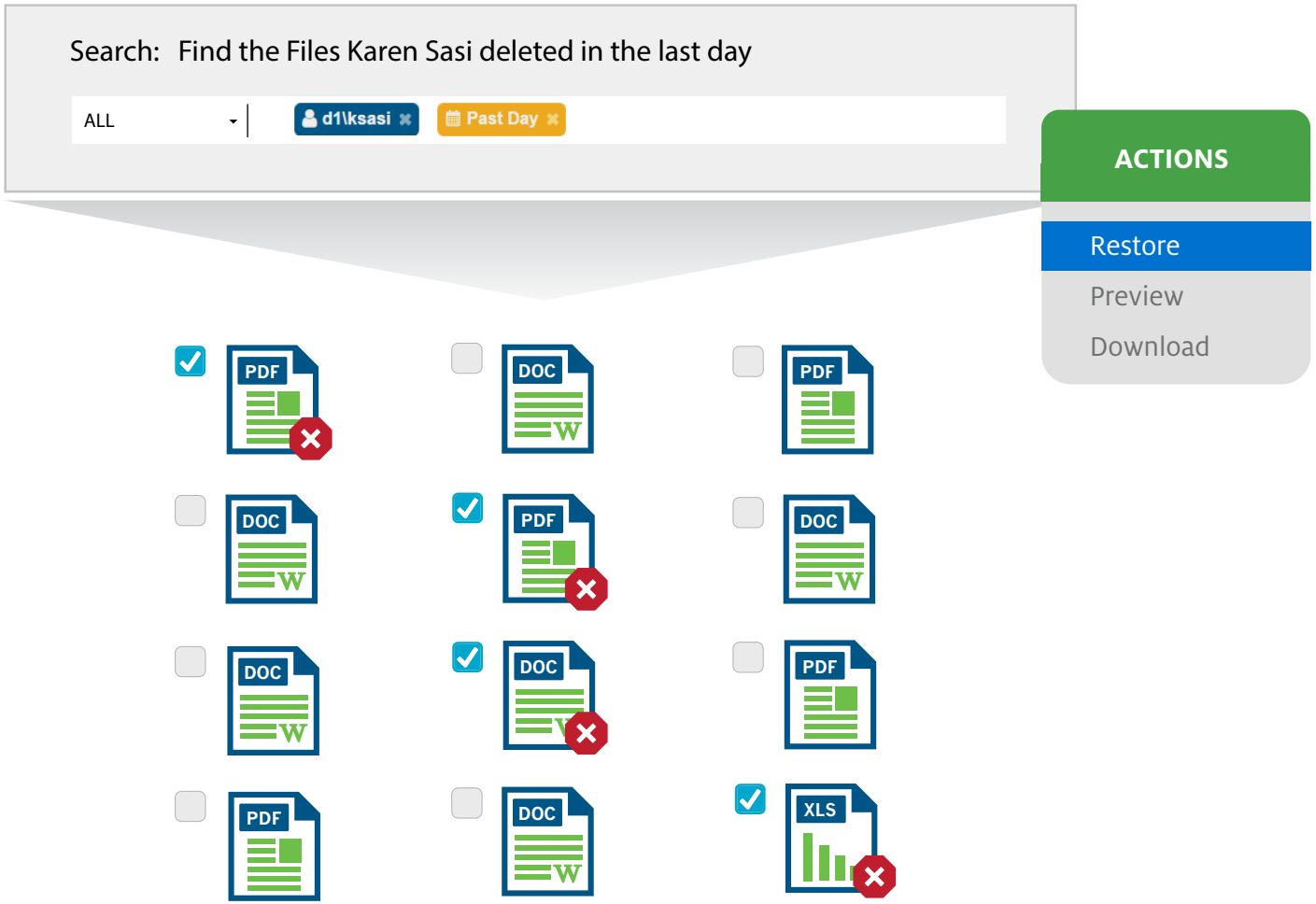


XLS w:...\Y14plan.xlsx
VM6 Owner: ksasi
Modified: 2014-01-14 10:20:00
SSN

XLS w:...\SaleCompensationPlansFY15.xlsx
VM3 Owner: cscott
Modifed 2014-01-14 10:20:00
SSN

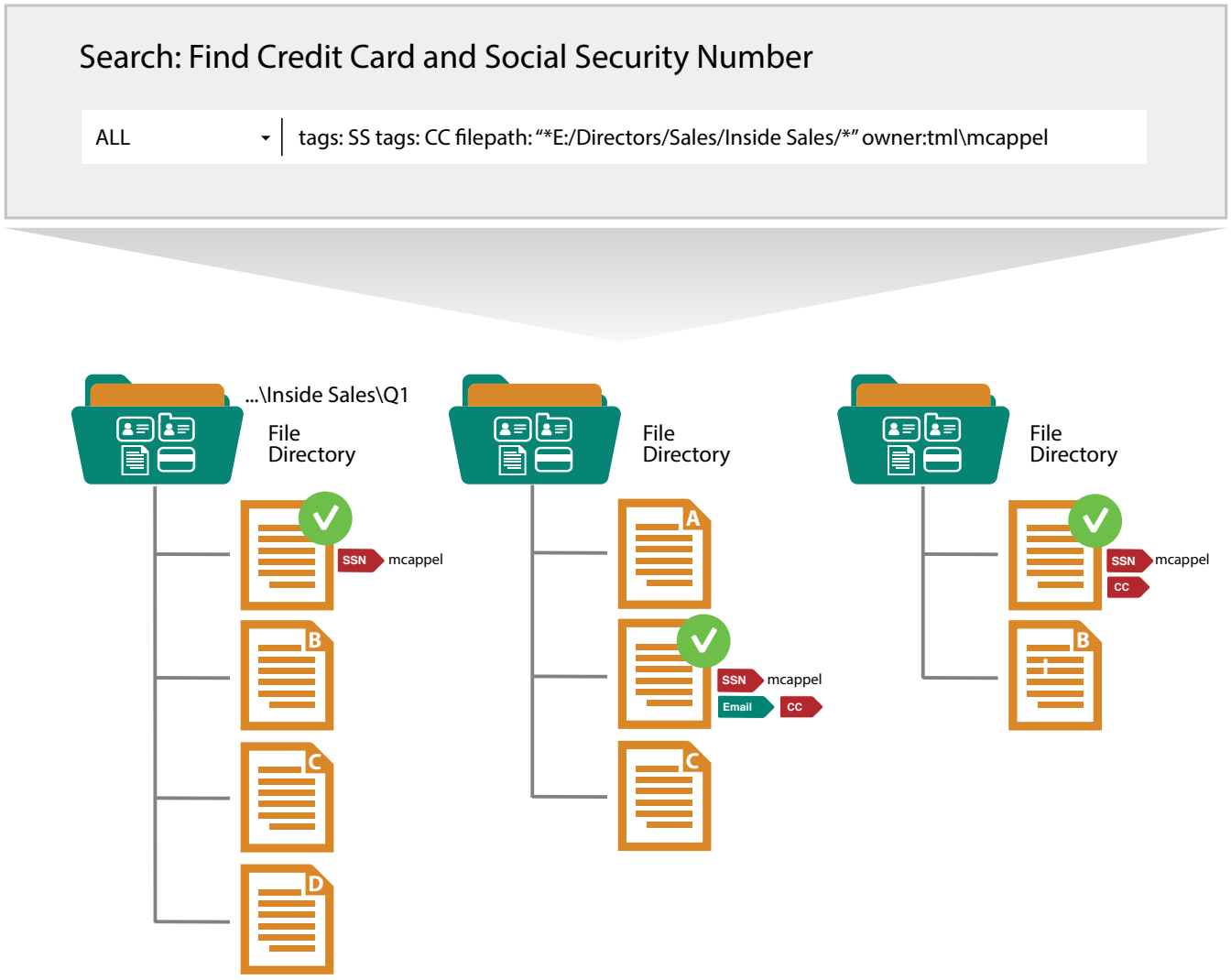
DOC w:...\CompensationPlansFY15.docx
VM6 Owner: cscott
Modifed 2014-01-14 13:20:00
SSN Confidential

Find Deleted or Missing Files



DataGravity gives you a window into the past with full visibility. Administrators can see which files were deleted between backups and which backups contain deleted files. Whether you're dealing with ransomware which can delete original files, or with user error (e.g. a cut and paste rather than a copy and paste), DataGravity enables you to easily find the affected files and quickly restore them without having to mount multiple backups and try to manually determine which files were deleted between them.

Understand What You Are Restoring



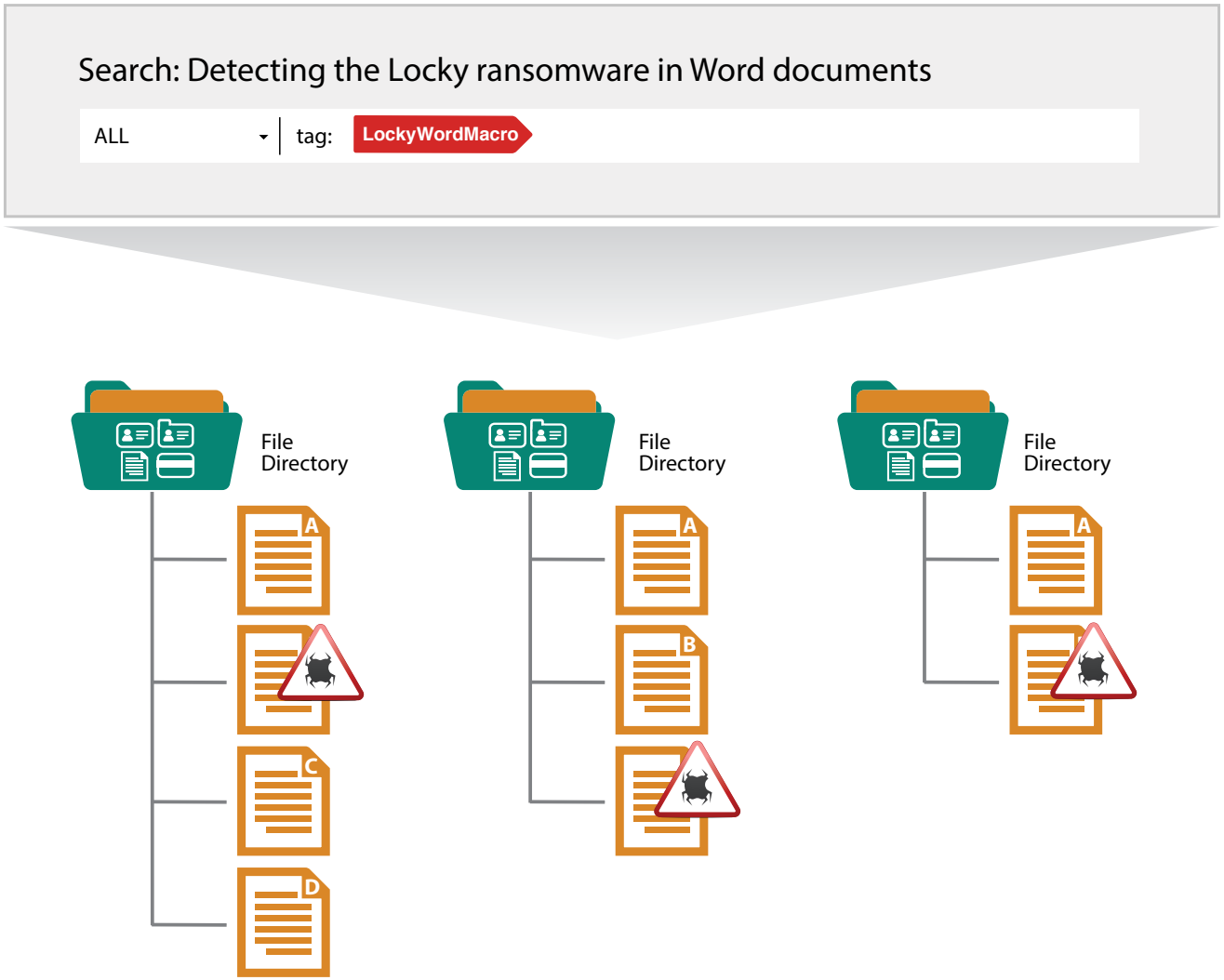
When your system is down, there is no time to waste trying to figure out exactly what needs to be restored to get operations back up and running, particularly if the backup is too extensive to conduct a surgical restore.

In this case, image backups are often the last resort, restarting your system from a moment back in time while losing your most recent data. While this can be sanctioned as a best worst-case result, administrators will not have gained insight into what was lost—or even gained—in the process.

DataGravity tracks the journey that data has taken, letting you know what has changed, how it has changed and who made the change. You will see exactly what is missing, and what has been replaced with an older version. This important information makes it easier to apply a second surgical restore to remove files which are no longer needed while picking up lost data.

Avoid Restoring Old Problems

When restoring a backup, old problems which have since been fixed can be re-introduced—be it a virus or a remnant of ransomware, these old issues can cause new issues. DataGravity lets you visualize the data in your backup, allowing you to confirm that you aren't creating new issues as you fix the issues you are working on in the data.

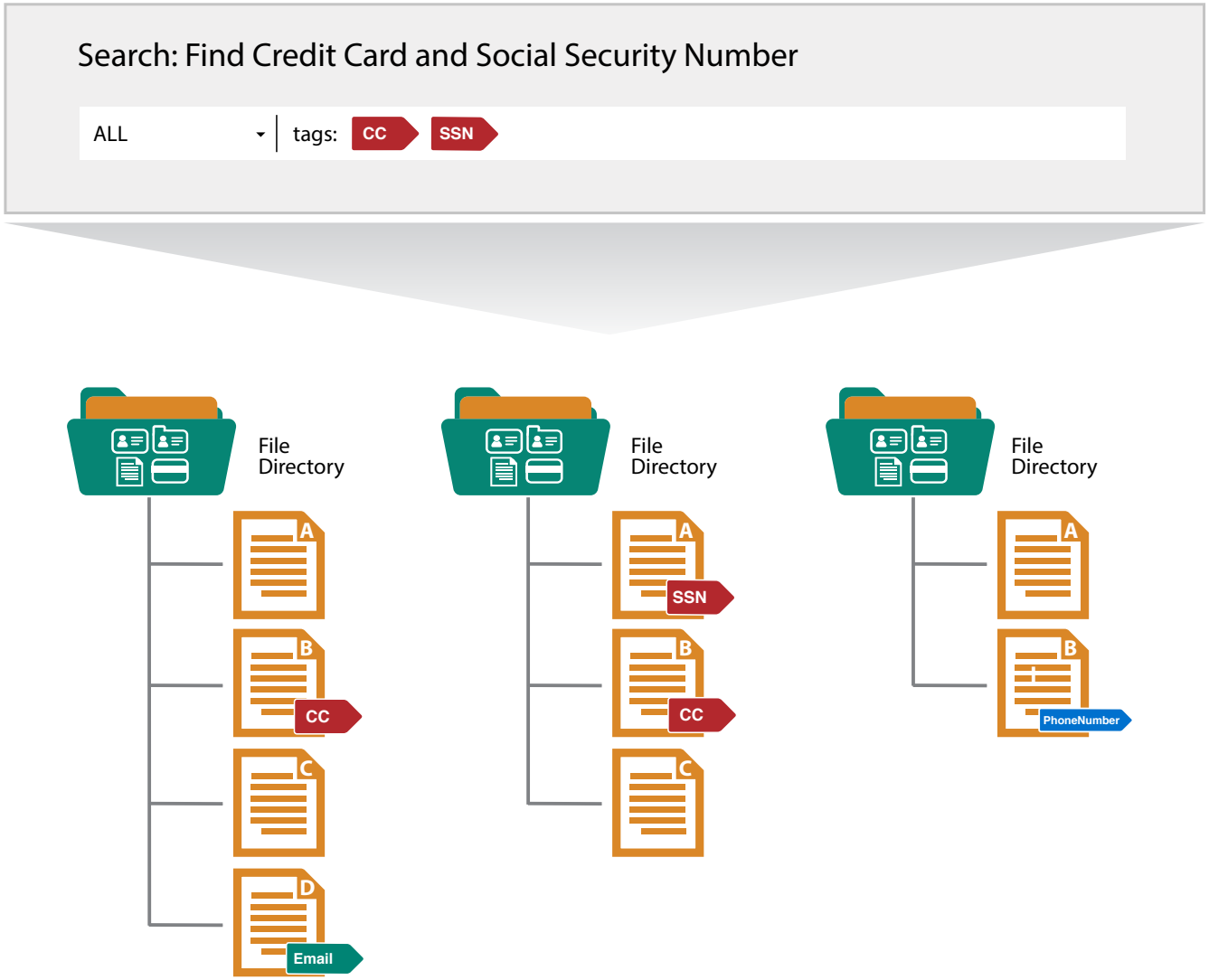


Analyze Backups for Sensitive Data Exposure

Data security is an area of sensitive importance, and finding sensitive data hiding in your backups can be a chore: credit card numbers, social security numbers, patient IDs, customer information and even confidential intellectual property could be hiding in the open.

Now you can monitor, detect and pro-actively report back data security concerns with the DataGravity built-in and customer-defined classification tags across each of your backups as they are created. Combined with user policies that highlight potential issues (e.g. exposed password files or latent ransomware issues), administrators will know whether a backup has potentially problematic issues.

Administrators storing their backups on the Cloud can also ensure that these backups adhere to company policy and regulatory objectives regarding sensitive data before they are moved to the Cloud.



Backups Includes File and User Level Audit Information

When the DataGravity dgfilter is installed on running VMs, it turns a formerly passive backup into a data-rich set. Administrators and security professionals can then conduct forensic work on file activity, including who did what to the data and how. DataGravity maintains these three key pieces of information automatically:

With this information, administrators can forensically and accurately answer many important questions, including, the 5Ws (Who, What, When, Where, and Why) about your data.

Without the DataGravity dgfilter, you would only see information about the content.

Visualize Your Backups

DataGravity offers a comprehensive 360° view of all data in every backup file, letting administrators find dormant data, as well as the data's demographics and the biggest consumers of data in your system. Put together, this enables administrators to improve their data management and curation.

Additionally, reducing the footprint of your data improves backup times, reducing your data surface (and consequent risk profile) while decreasing storage costs.

Behavior Driven Data Protection

Backups are generally made on a time-based schedule or on-demand, manually or by a script. When a VM has the DataGravity dgfilter installed, a third option is added: backups triggered by user or file activity and behavior.

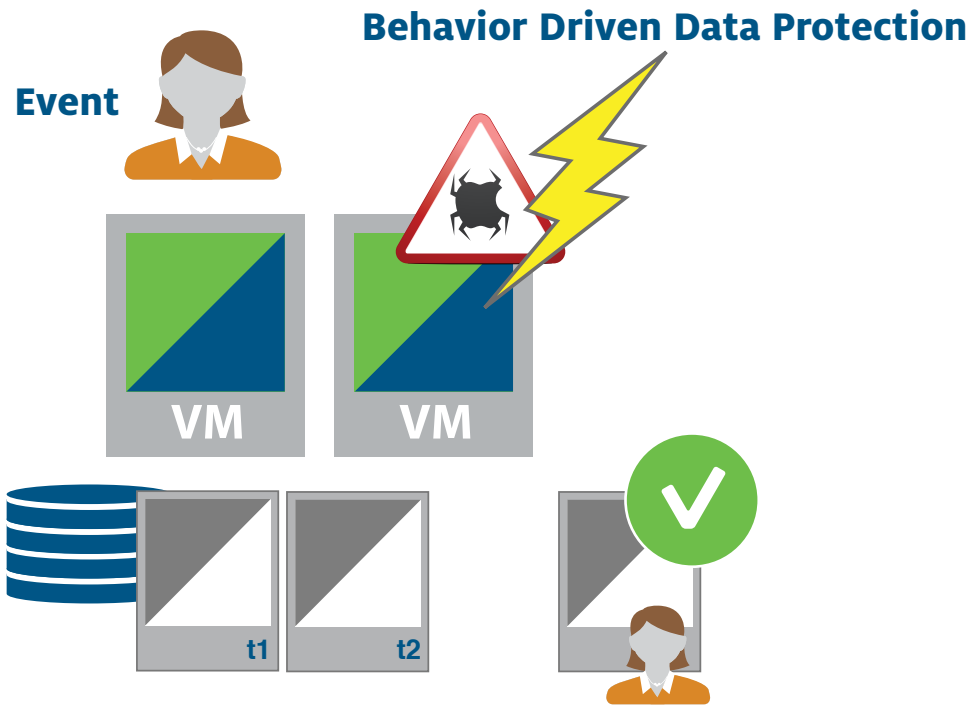
For example, if one of your Recovery Point Objectives (RPOs) is to maintain a data loss no higher than 1%, in the past you would have had to create a schedule to approximate the desired results. Backups may have been taken too frequently while missing the desired objective. With DataGravity and Veeam, administrators simply inform the system to make a backup when a specific amount of data changes.

The DataGravity built-in trigger also identifies and zones in on ransomware patterns, automatically taking a Veeam backup upon detection. This automatic backup can also be triggered by anomalous user activity such as a sudden spike in file deletions and other non-typical activity.

At the same time, administrators can also use the built-in forensics to determine what happened and intelligently perform any remediation required.

Trigger a backup and other actions based on events detected in the environment.

- Sensing anomalous behavior
- Orchestrating protection point
- Blocking user access
- Alerting the administrator



Putting it All Together– Recovering from Ransomware Example

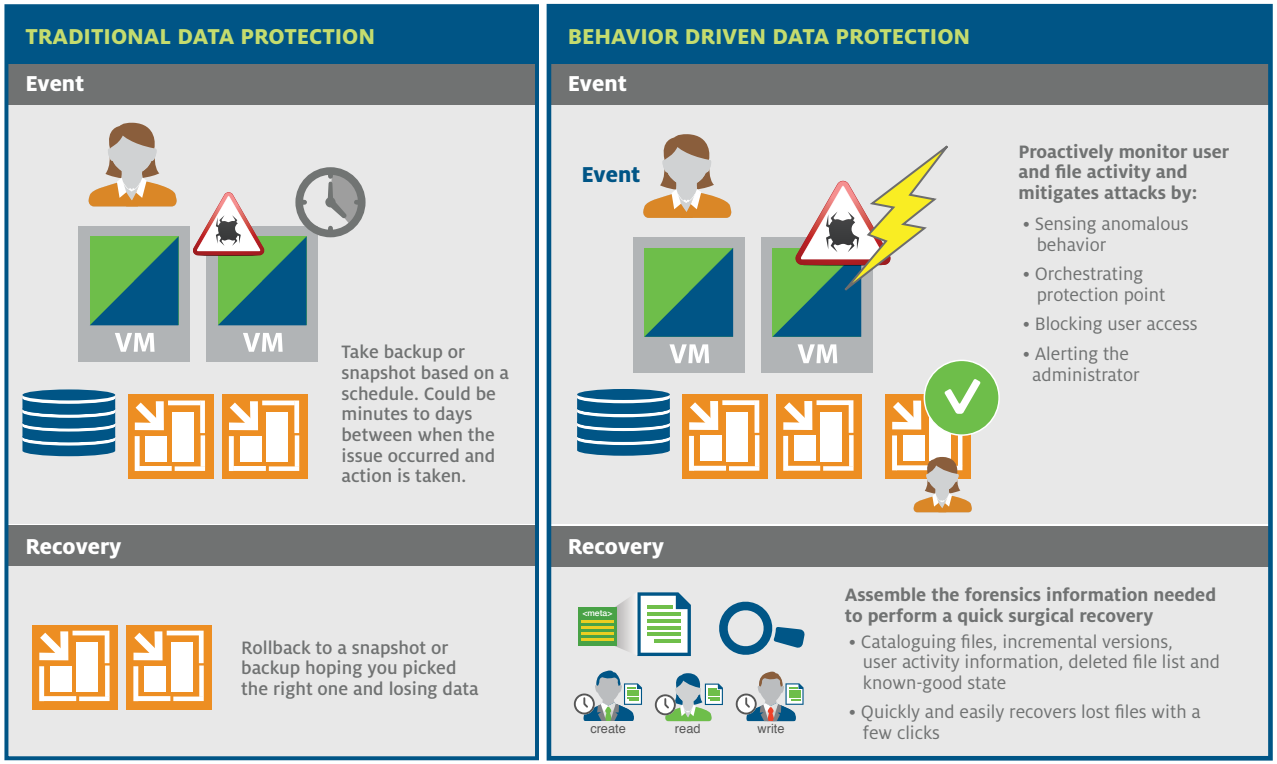
Recovering from a ransomware attack can be tricky, but when using DataGravity, you can significantly decrease the impact of such an attack.

DataGravity offers behavior driven data protection capabilities that will automatically trigger a Veeam backup as soon as suspicious, ransomware-like activity takes place. DataGravity can optionally take action against suspect users such as disabling their access, as well as sending notifications when an attack takes place. The notification will include the users and files that are affected.

DataGravity brings you out of the dark, giving you a clear view of both file and user activity: not only do you see what files were affected, but you know what data was left untouched. With this information, administrators can start to build an informed recovery plan.

For localized damage affecting just one user, it may be as simple as restoring the files to the last known good state for that user, a list that DataGravity can help you to build.

For more extensive system damage in which the ransomware deleted the original files, DataGravity makes it easy to get a list of all the deleted files and restore them. This can be files deleted by the affected user(s), or all files deleted. DataGravity also presents a list of auxiliary files created during the attack, such as ransomware notes and even *.locky files.



If an attack has left a system extensively damaged with overwritten files, the easiest course of action may be to get a list of files modified by an unaffected user, rollback to a clear backup and then reapply the unaffected files.

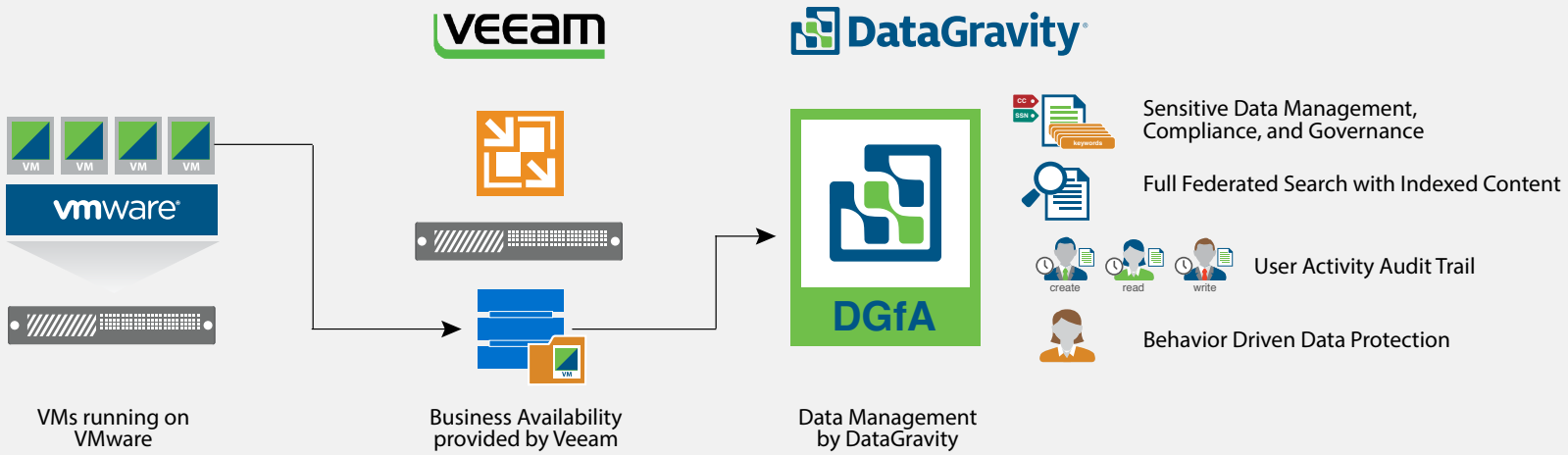
By combining Veeam and DataGravity, administrators can quickly create a data recovery plan to meet any attack. With complete information available for forensic work, there is no longer any need to incur the penalty of data loss or an incomplete restoration.

Conclusion

DataGravity capabilities add significantly to Veeam Backup and Replication, providing a clear, 360° view of exactly what is inside your data, adding invaluable forensic and diagnostic information:

- Data changes, creations and deletion by user, location and time
- Seamless detection of sensitive data
- Both user and file-level auditing for the content contained in every backup
- Behavior driven data protection, triggering automatic backups based on user behavior and data specifics

Veeam just works—and combined with DataGravity, it just works better.



Get Started NOW

Learn more

Request a LIVE DEMO

Learn more

603.943.8530

sales@datagravity.com