DataGravity®

SOLUTION BRIEF

Proactively Protect and Easily Recover from Ransomware

DataGravity for Virtualization

Responding to the Growing Threat

Ransomware, the likes of Teslacrypt, Cryptowall, Locky and many variants, is fast becoming the number one security threat that IT managers face. The rise of Bitcoin has emboldened cybercriminals' use of ransomware to anonymously extort large sums of money from infected users and organizations. This year alone has seen many high profile cases forcing hospitals, schools and government agencies to pay hundreds of thousands of dollars to recover their mission-critical data.

An infected endpoint device can be catastrophic to an individual user, but new levels of sophistication seek out all the files a user has access to, including centralized shares and file servers. An attacker's successful acquisition of an administrator's privileged access credentials widens this impact even further. As some recent attacks have illustrated, even paying the ransom does not guarantee that criminals honor their promise to decrypt your data. Whether or not the ransom is paid, the inaccessibility of critical systems can cause severe business disruptions, resulting in losses of revenue and reputation as well as the outage of key customer, client and patient services.

Preempt and Respond Effectively to Cyber Extortion

Preempt Loss with Behavior-Based Backups

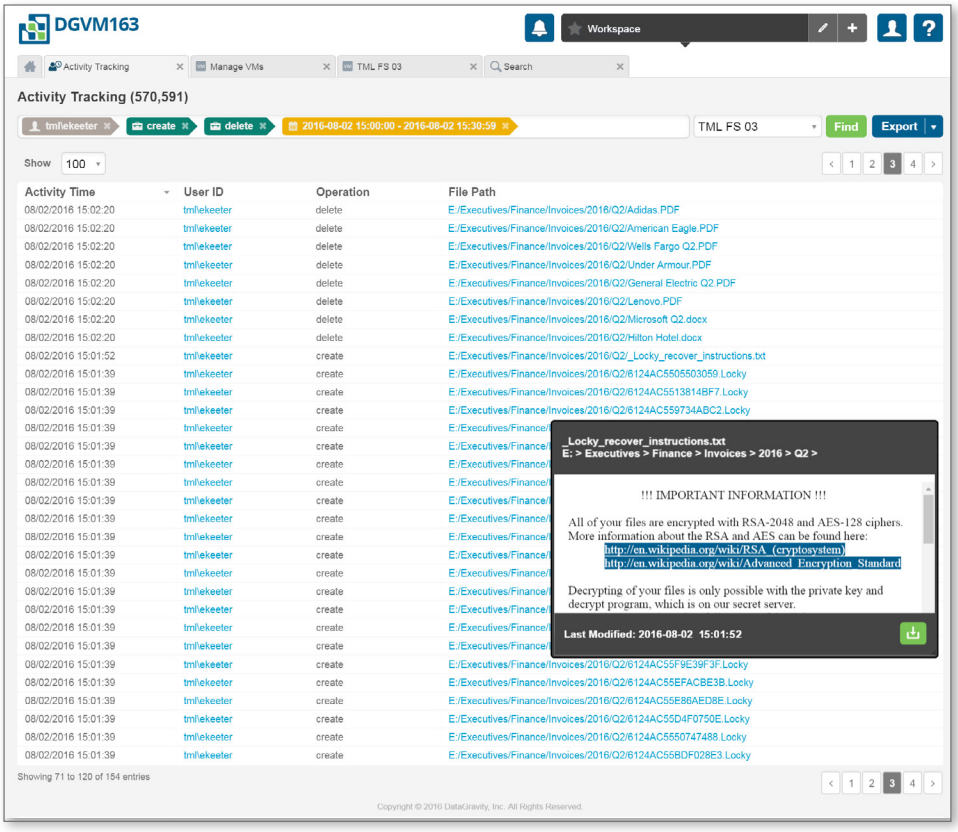
- Be alerted of suspicious file activity levels indicative of attack
- Automatically protect VMs exhibiting high rates of change

Rapidly Assess Scope of Attack

- Forensically analyze time of attack and patient zero
- Identify exactly what VMs, shares, directories, and files have been impacted

Quickly Recover from Business Disruption

- Quickly assess the impact of VM rollback recovery vs. selective file restores
- Simply recover files with the click of a button



RAPIDLY ASSESS IMPACT AND RESPOND

Using DataGravity for Virtualization, you can quickly identify and assess a ransomware attack, understand what files are affected, and develop an action plan to respond and recover.

You should do everything possible to prevent infection – through user education, up-to-date anti-virus software, as well as maintaining regular backups. But moreover, being fully prepared to quickly detect, protect, assess, and recover operations after an infection is vital to limit disruption and to avoid the embarrassment of paying an exorbitant ransom.

You are best prepared to protect your sensitive data by knowing where it is located and who is accessing it. DataGravity for Virtualization proactively monitors and protects your data, accelerating your ability to diffuse the impact of a ransomware infiltration.

Secure and Protect Your Virtualized 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 for Virtualization 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 virtualized 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 organization against ransomware, malicious users, careless exposure, data loss and regulatory non-compliance.

Take action to protect your organization and your data from ransomware attacks.

Reduce Your Overall Risk Profile

Knowing where your mission-critical data is located and limiting access to it reduces the impact of a ransomware attack. Yet, most organizations lack the tools necessary to gather this fundamental knowledge. Loose permissions management and haphazard data governance increase the attack surface.

By analyzing content from over 600 file types, DataGravity for Virtualization automatically indexes all your files for fast query and analysis. Files are tagged according to parameters you define to identify sensitive, confidential and mission-critical information. File access is tracked and recorded, providing visibility into user access patterns across all stored files. Armed with this knowledge, you can assess your exposure risk, limit user access permissions, and take quick action to remove or relocate improperly stored files.

Proactively Monitor for Suspicious Activities and Threats

A ransomware attack generates uncharacteristic spikes in activity as it traverses accessible file systems and file shares, writes ransom notes, and encrypts files for which it has access privileges. DataGravity for Virtualization monitors activity levels for each user and alerts you when defined thresholds are exceeded, so you can investigate and take action. Content alerts are also available to automatically notify you when suspicious files are created or modified. For example, by setting up alerts based on published ransomware fingerprints and ransom notes, you can quickly surface and respond to these concerns.

By directly integrating with your underlying storage and hypervisor, DataGravity for Virtualization creates storage-based snapshots of each virtual machine according to defined schedules. If a virtual machine exhibits a high rate of data change, symptomatic of a potential attack, DataGravity for Virtualization automatically creates a snapshot. Snapshots are analyzed to create DataGravity DiscoveryPoint backup catalogs of all changed and deleted files, the basis for easy ransomware impact analysis and data recovery.

Accelerate Response and Recovery

Upon discovery of a ransomware attack, DataGravity for Virtualization acts as a rich forensic analysis and recovery tool. By understanding file content changes, user behaviors, and data access over time, you can quickly identify the root cause, the exploited user account (patient zero), the timeframe of the attack, and all the VMs, shares, directories, and files that have been impacted. Audit trails, filtered by user, by file, and by VM, file system, or file path, provide targeted exploration of data access events that led up to and occurred during the ransomware attack. From your analysis, a detailed and prioritized recovery plan can be developed. Recovery strategies include file-level recovery of affected files and directories from DiscoveryPoint catalogs and rollback of entire virtual disks followed by file recovery of targeted files.

Be Secure. Be Data Aware.

By exploiting security holes and user errors, cybercriminals recognize ransomware as an easy vehicle to monetize data breaches. DataGravity for Virtualization is a key element of a multi-layered security plan to prevent access, immediately identify threats, and quickly respond. By proactively analyzing, monitoring and protecting your data where it lives, DataGravity for Virtualization reduces your overall risk profile and accelerates your ability to respond and recover from the ill effects of ransomware.

OVERCOME THE RANSOMWARE THREAT

DataGravity helps you defend against ransomware attacks by reducing your risk profile, proactively protecting your data, and aiding in the response and recovery of impacted files.

DataGravity

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

DATAGRAVITY @DATAGRAVITYINC DATAGRAVITY