TECHNICAL WHITE PAPER

The Role of Cloud Backup and Recovery in Protecting Against Ransomware Attacks

TABLE OF CONTENTS

INTRODUCTION

Ransomware is creating a data-security crisis. The 2019 Internet Security Threat Report from Symantec explains that enterprise ransomware infections were up 12 in 2018. In addition, Symantec cites databases as a weak point for organizations. MongoDB saw a surge of ransomware attacks in 2017 — and there's no sign that they're slowing down.

In ransomware attacks, malware encrypts data, making it unreadable. A message then instructs the victim to pay a modest "fee" to anonymous hackers in exchange for decrypting the data. Without the key, the data is inaccessible. The malware might even delete the data after a few days for good measure.

Ransomware has targeted small and large organizations alike, and it is increasingly going after next-generation applications that run on databases such as Cassandra and MongoDB or even data lakes that run on Big Data filesystems such as Hadoop. These can be high-value targets for attackers, and the security processes and tools aren't in place to defend them.

This white paper explores four topics:

1. How ransomware has become a significant problem for next-generation applications
2. The crucial role cloud backup and recovery plays in providing a layer of defense
3. The challenge of backup and recovery for next-generation applications
4. How Rubrik Mosaic's application-centric cloud data-management solution addresses these challenges

HOW RANSOMWARE HAS BECOME A PROBLEM FOR NEXT-GENERATION APPLICATIONS

Next-generation cloud applications are an attractive target for criminals. These applications are often used by the organization to store and process sensitive, high-volume sets of data, and years' worth of records. Security vendors, corporations, and governments run event analytics and real-time risk-assessment programs. Financial institutions store years' of account or trade records and create unified views of the customer. Retailers have created critical e-commerce capabilities, run loyalty programs and generate customized offers.

Although hackers demand payment in return for decrypting the files, the cost of data loss and downtime are much higher. In an annual survey, 98% of enterprises said downtime cost them at least $100,000 per hour, and 33% reported that it cost an estimated $1 to $5 million per hour. Downtime, data loss, and security breaches can cost companies their reputations and the loss of even their most loyal customers.

Attackers clearly see the potential for big payouts. Recent reports and incidents are likely just the beginning of an uptick in activity:

- More than 10,500 MongoDB clusters were compromised in a single week, with attackers demanding $150 to $500 in ransom to restore data. At least 34,000 MongoDB instances were eventually compromised.
- At least 443 CouchDB servers were compromised in a single attack.

Clearly, the applications both make for tempting targets and are especially vulnerable to attack. The underlying database is often exposed to the internet, sometimes by necessity. The databases might connect directly with other data sources over the internet or support a web-native application.

The distributed cluster architecture that many modern applications use also compounds the problem. Distributed databases like MongoDB and Cassandra replicate data across nodes quickly by design, so if ransomware infects a single node, it will quickly bring the database to a halt — possibly shutting down customer-facing or other critical applications with it. The distributed architecture protects against failed nodes, but can't "roll back" or "undo" data corruption or malware.

THE CRUCIAL ROLE OF BACKUP AND RECOVERY IN PROTECTING AGAINST RANSOMWARE

Given the rapidly evolving threat of ransomware, it's likely that even organizations with strong security technology and policies will be affected. Reliable backup and recovery has quickly become a crucial line of defense against ransomware. It allows companies to roll back in time and recover files or databases to just prior to the infection with ransomware.

Gartner recommends using backup as a defense for desktops, laptops, and file shares that are particularly vulnerable to ransomware. The same approach is a must for databases, especially as attackers have begun to target them.

Backup and recovery has become a critical part of the security infrastructure. A good database backup and recovery solution makes it possible to go back to a specific point in time and restore part or all of the database from that point. Even if ransomware was dormant on the system, point-in-time recovery makes it easier to identify, quarantine, and recover from infections without losing data.

Infrastructure and application teams also should secure open ports whenever possible, change default settings that can leave databases vulnerable to attack, and make certain that authentication and access controls are managed in line with corporate policies.

THE CHALLENGE OF BACKUP AND RECOVERY FOR NEXT-GENERATION APPS

Traditional data protection leaves enterprises exposed because it lacks the ability to effectively protect nonrelational databases such as Apache Cassandra, DataStax Enterprise, and MongoDB.

Modern applications built on non-relational databases stretch across systems and clouds, so it isn't sufficient to back up a single system or recover a full instance. You need to be able to extract specific versioned data. Existing solutions aren't designed to backup and recover these loosely coupled applications and non-relational databases that are becoming business critical today. Instead, existing solutions were designed to support single-node, scale-up databases using disk-based snapshots. In an eventually-consistent, write-anywhere non-relational database architecture, it's almost impossible to capture a consistent state using traditional backup. Successful data recovery is even less likely!

In response to this challenge, many organizations have scrapped their traditional backup and recovery solutions and instead write scripts to handle the task using native database tools. The result, unfortunately, is that although these solutions might offer rudimentary data protection, they are incredibly inefficient and typically require:

- Three to four times more backup storage due to in-cluster replication. Scale-out application databases typically have a three-times replication factor, making traditional backups 75% to 80% inefficient.
- Thirty to fifty percent more infrastructure to maintain a replica of the cluster topology. Effective restores usually require identical topology on the recovery cluster.
- Very long recovery times. It can take days or even weeks to repair and restore a database.

The bottom line is that neither traditional backup and recovery solutions nor any native non relational database tools deliver the necessary backup and recovery capabilities required to protect an organization's next-generation applications against ransomware attacks.

HOW RUBRIK MOSAIC PROTECTS NEXT-GENERATION APPLICATIONS AGAINST RANSOMWARE

Rubrik Mosaic is designed to work specifically with non-relational databases and applications and fills a key gap in the fight against ransomware. Unlike traditional backup and recovery or scripted solutions, Rubrik Mosaic provides the following:

APPLICATION-CENTRIC BACKUP

Unlike traditional backup and recovery solutions that rely on virtual machine or logical unit (LUN) constructors, Rubrik Mosaic is application-centric and delivers application-consistent backup copies to any point in time.

ANY POINT-IN-TIME RECOVERY

Rubrik Mosaic enables organizations to restore application data to any point in time prior to infection, encryption, or malicious deletion.

RAPID RECOVERY

Databases can be recovered in minutes, and application traffic can be redirected to the restored database. By comparison, traditional recovery approaches require lengthy repair processes.

PARTIAL RECOVERY

Rubrik Mosaic supports granular recovery of specific data from any point in time so that specific changes can be restored or rolled back.

STORAGE-EFFICIENT BACKUP

Rubrik Mosaic uses *semantic de-duplication*, which reduces backup storage requirements up to 70%.

Rubrik customers such as Maxwell Health and Ayla Networks are better prepared to fend off ransomware attacks. With timely, complete, and consistent backups of their next-generation databases, Rubrik Mosaic customers can immediately restore a compromised database. This can save hours or days of time and, more important, protect customer data and revenue against ransomware attacks.

SUMMARY

Following security best practices is a crucial first line of defense in the fight against ransomware, but it is almost a statistical certainty that your organization will eventually be attacked with ransomware — it's not if, but when. There are too many exposed points for enterprises to completely secure without compromising functionality. Organizations need to be prepared.

Backup and recovery is a key component of any organization's overall ransomware defense strategy and is a critical last line of defense against ransomware when it penetrates other security countermeasures. Organizations need the right tools to protect files, applications, and databases against ransomware — including fast point-in-time restore. If next-generation applications are in your current or future plans, you need to ensure that those applications are protected against ransomware attacks.

To find out more about how to protect your next-generation applications and databases against ransomware, visit us at www.rubrik.com or contact your local sales representative to schedule a demonstration.

ABOUT RUBRIK MOSAIC

Rubrik Mosaic is the application-centric NoSQL data-management solution from Rubrik designed for the multicloud world. Mosaic delivers a radically novel approach to NoSQL data management to help organizations embrace the cloud with confidence.

rubrik

Global HQ
1001 Page Mill Rd., Building 2
Palo Alto, CA 94304
United States

1-844-4RUBRIK
inquiries@rubrik.com
www.rubrik.com

Rubrik delivers a single platform to manage and protect data in the cloud, at the edge, and on-premises. Enterprises choose Rubrik's Cloud Data Management software to simplify backup and recovery, accelerate cloud adoption, and enable automation at scale. As organizations of all sizes adopt cloud-first policies, they rely on Rubrik's Polaris SaaS platform to unify data for security, governance, and compliance. For more information, visit www.rubrik.com and follow @rubrikInc on Twitter.

20190627_v1