GORILLA GUIDE®
FOUNDATION EDITION

# 5 Keys to Mitigating Data Risk

Joey D'Antoni

## Inside the Guide

- Know data risks and be prepared with remediation plans
- Ensure your backups are immutable
- Fast and effective recovery

ActualTech Media | rubrik

# 5 Keys to Mitigating Data Risk

By Joey D'Antoni

## TABLE OF CONTENTS





**ActualTech Media**

6650 Rivers Ave Ste 105 #22489 | North Charleston, SC 29406-4829

www.actualtechmedia.com

# Publisher's Acknowledgements

**EDITORIAL DIRECTOR**
Keith Ward

**DIRECTOR OF CONTENT DELIVERY**
Wendy Hernandez

**CREATIVE DIRECTOR**
Olivia Thomson

**SENIOR DIRECTOR OF CONTENT**
Katie Mohr

**PARTNER AND VP OF CONTENT**
James Green

**WITH SPECIAL CONTRIBUTIONS FROM RUBRIK**
Arushi Jain, Principal Product Marketing Manager

---

**ABOUT THE AUTHOR**

**Joey D'Antoni** is an Senior Architect and Data Platform MVP with over a decade of experience working in both Fortune 500 and smaller firms. He is currently Principal Consultant for Denny Cherry and Associates. He is frequent speaker at major tech events, and blogger about all topics technology.

# Introduction

Welcome to the Gorilla Guide® (Foundation Editon) to 5 Keys to Mitigating Data Risk! This short, easy-to-digest book is all about staying safe in the new cloud IT era.

If you have responsibilities for data security, whether you're an IT architect, CISO, database administrator, or admin, this Guide will show you five crucial things you need to know to protect what's yours.

Your data is one of your business's most valuable assets. But, those assets are increasingly at risk from a variety of attackers, from ill-meaning nation-states to disgruntled employees to a rogue hacker. They are all trying to infiltrate your business.

Beyond just monitoring for attacks, you need to ensure that your data is protected from system failure, data breaches, data exfiltration, and ransomware attacks. Having a robust backup solution across your environment provides fast recovery from various failures and security threats.

If the worst happens, having detailed knowledge of the data landscape can help you establish recovery order in the event of an attack and subsequent failure. The keys to surviving security attacks, including ransomware, include:

- Quickly indentifying the impact of an attack
- Having indestructible or immutable backups
- Being able to quickly restore your critical data

- Identyfing sensitive data exposure

So grab a water bottle and some mosquito netting, and let the Gorilla be your guide.

# Overview of Data Risks

According to the Emsisoft Malware Lab, ransomware attacks in 2020 *"impacted at least 2354 government agencies, educational establishments and healthcare providers"*, at a potential cost of untold billions of dollars. While cyber security teams have invested in a myriad of protection tools such as anti-virus, logging tools, and endpoint protections, extortionists continually find new mechanisms to encrypt organizations' data. It is the IT organization's responsibility to have data protection and recovery plans against these attacks.

### RANSOMWARE ATTACKS

Ransomware attacks typically install themselves in your network. This is done by targeting users convincing them to click on a malicious link or email file. Once the initial attack vector takes place, the software will move laterally in the network. It will attempt to gain access to admin credentials, and then attempt to encrypt servers, files, and backups. Often, they will leave a text file asking for payment for decryption key.

On top of that, new types of ransomware are now being combined with a data exfiltration attack. Essentially, this is an attacker threatening to publicly expose your critical data to increase pressure of ransom payment. Data breaches can also be an internal risk—privileged bad actors within your organization could also attempt to export data from your environment.

**Ransomware attacks in 2020 "impacted at least 2354 government agencies, educational establishments and healthcare providers", at a potential cost of untold billions of dollars.**

Protecting against ransomware attacks requires a defense in depth strategy that includes best practices around ensuring only the right people have access to your data, especially for your most sensitive data, along with strong user authentication and communication protocols, immutable backups that cannot be deleted from ransomware, and fast recoveries.

# Remediation Plans Are Nonnegotiable

The best laid plans are written down and well-rehearsed. Before disaster strikes, document when it's time to engage your incident response team, notify key stakeholders, and evaluate your options so that you can retrieve your data and get back online. It is critical to engage your business leadership regarding disaster recovery planning, and the IT department needs to be included business continuity planning meetings.

### RANSOMWARE REMEDIATION TIMELINE

1. Isolate the infected machines from the network
2. Ensure that your backups have not been compromised
3. Identity the type of infection that you are facing
4. Determine your options for recovery. This might include:
    a. Paying the ransom
    b. Attempt to remove the malware from your network
    c. Recover from backups (often, the recommended recovery option if available)
5. Engage your incident response team
6. Diagnose the scope of the infection in terms of what applications and files were infected and where they are located
7. Alert the authorities

**Figure 1:** This outlines the important steps to take for ransomware remediation

Beyond just restoring your backups, this plan can include cyber insurance, reviewing your backup strategy, and having a data recovery consultancy on retainer. Many organizations perform testing exercises to test a complete environment restoration. Note, with cloud infrastructure this can be a cost-effective option adding confidence that you can restore when needed.

An example of a ransomware remediation timeline and steps is shown in **Figure 1**.

### IMMUTABILITY

Immutable means something is not vulnerable to ransomware compromise. In computer systems terms, this is a file that is written once and then cannot be accessed, modified, or deleted by clients on your network. This is critical for your backup provider to be have an architecture that stores all backup data natively in an immutable format to ensure you have backups to recover from in the event of an attack.

# Ensure Your Backups Are Immutable

Backups are a major target of malware attacks. Having reliable backups is the single best protection against a malware attack, especially when combined with endpoint monitoring that helps you quickly identify when you are being attacked. Once the attack has been identified, you can quickly move to restore machines back to a last good state. Since backups are critical, they are also often a target for attackers.

Traditional backup solutions, such as file shares, or even some more advanced backup solutions allow for backups to be overwritten, or updated by end user accounts. This makes the backup files vulnerable to both ransomware attacks or attacks from privileged bad actors.

To protect your backups, ensure that backups are natively **immutable**.

This can be visualized as shown in **Figure 2**.

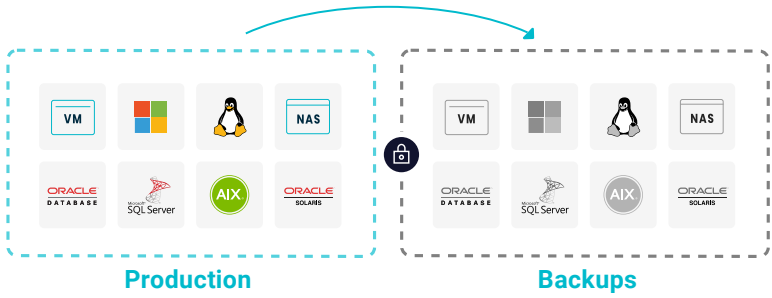



**Figure 2:** This illustrates an immutable backup

## SECURE BACKUP ARCHITECTURE

On top of having immutable backups, your backup architecture needs to be designed so that no security exposure can tamper with the backups. This means secure communication protocols that do not write backups to network accessible file shares, like SMB or NFS, which have weak security protocols that can potentially be bypassed. Additionally, when it comes to restores of files, it's important your backup provider does fingerprinting at ingest time to validate your backup data is never changed, thus ensuring data integrity.

In addition, your backup architecture should be implemented with a zero-trust cluster design. In traditional clustering models, which rely on a full-trust model, all members of a cluster are able to communicate with each other. In some cases, this means a member node or service can obtain

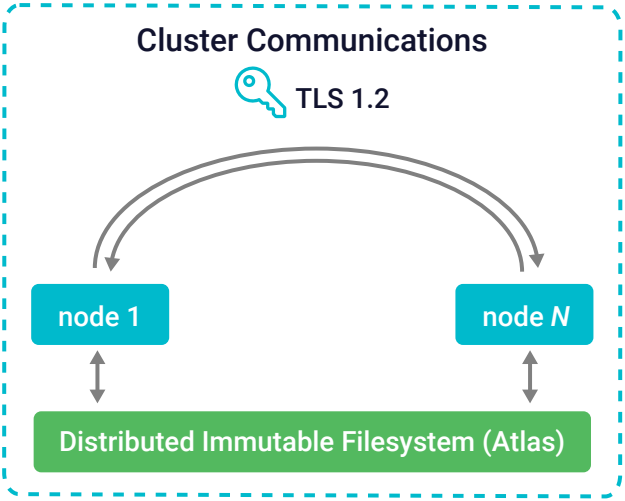



**Figure 3:** Overview of secured cluster communications

root-level authority without mutual authentication checks. If that happens, the node or service gains the ability to read and write data to the filesystem which could overwrite backups or other sensitive data. This type of architecture leads to a larger attack surface area, which puts your data at risk .

A zero-trust model ensures that intra-cluster communications are encrypted with certificate-based authentication protocols for secure communications. Limiting network traffic by reducing exposed ports protects against potential side channel attacks. Forcing authentication to all APIs and other system interfaces protects against lower credentialed users gaining access. **Figure 3** shows an example of secured cluster communication environment, featuring encryption of cluster network traffic.

**Traditional backup solutions such as file shares, or even more advanced backup solutions, allow for backups to be overwritten or updated by end-user accounts. This makes the backup files vulnerable to both ransomware attacks and to attacks from privileged bad actors. To protect your backups, ensure that they are natively immutable.**

# Understand Attack Impact to Minimize Data Loss

Small organizations may have the ability to restore all their infrastructure in the event of an attack, but for a larger or distributed organization data restoration can challenging. There are two components of this:

- Added layer of intelligence on backup data that analyzes and detects abnormal system behaviors, such as ransomware, as an added layer of intelligence on backup data

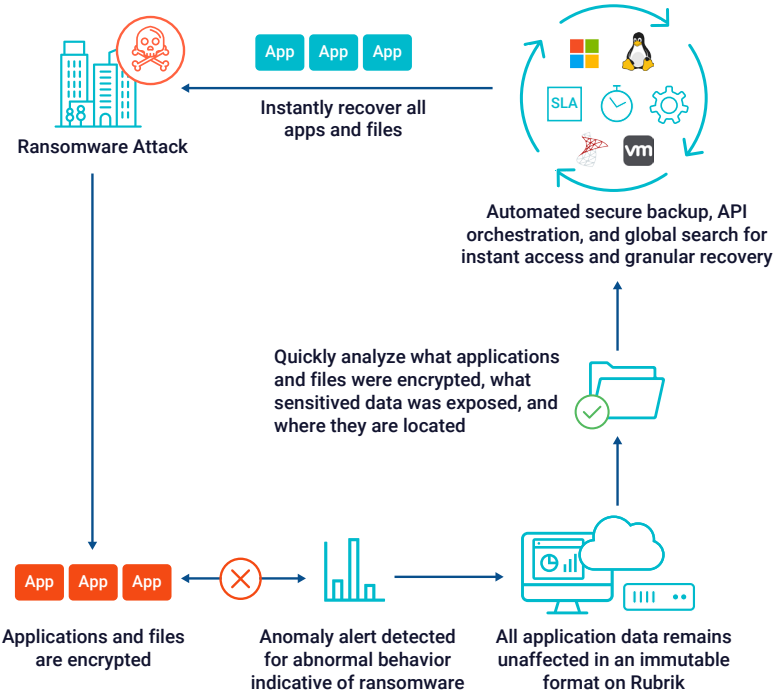



**Figure 4:** Ransomware recovery process

- Automatically identify what applications and files have changed via file system analysis
- Then, execute a fast and easy restore process

This is visualized in **Figure 4**.

Analysis techniques include machine learning to detect and alert on anomalous behavior based on the number of files added, modified, and deleted. It compares this to a unique normal baseline for each environment. By using machine learning, it will continuously refine its anomaly detection model over time and stay ahead of the most advanced threats and strengthen your detection and response strategy.

Aditionally, the restore process largely consists of identifying which backup files contain pre-infection content and restoring files to that point in time. Its often hard to manually determine the scope of attack impact. Modern data protection solutions can automatically visualize the breadth of damage in an easy-to-use UI, allowing users to browse and drill-down to investigate what was changed at the file-level. This helps minimize the time spent discovering what happened and the data loss with granular visibility into the latest unaffected files.

**It is important that you know what business data is sensitive, where it is located, and who has access to what sensitive files to ensure it is stored in authorized locations with strong access controls.**

Traditional analysis and restores can take hours, and even days, which means to recover quickly you need a backup solution that can reduce restore time using modern snapshot technology and deep system intelligence.

## Know What Sensitive Data Is Exposed and Where It Is

Another component of modern ransomware attacks is data exfiltration, which combines ransomware with a data breach. This can also lead to big financial penalties under data privacy laws, such as EU's General Data Protection Regulation (GDPR) or industry-specific regulations as Health Insurance Portability and Accountability Act (HIPAA) and Payment Card Industry Data Security Standard (PCI DSS).

**Modern data protection solutions can automatically visualize the breadth of damage in an easy-to-use UI, allowing users to browse and drill-down to investigate what was changed at the file-level.**

It is important that you know what business data is sensitive, where it is located, and who has access to what sensitive files to ensure it is stored in authorized locations


**Figure 5:** The data classification process

with strong access controls. A sample workflow for data classification is shown in **Figure 5**.

Classifying your data can be a challenge. Most enterprises rely on manual approaches, which consists of siloed teams and spreadsheets. Having a solution which can automatically identify sensitive data and apply policies by looking for sensitive information patterns can help you know what types and where your sensitive data resides.

Beyond just being able to do an initial scan, a solution that incrementally scans and can classify newly identified data is

another important information security step. Once you have this information, you can search on-demand for where the data is stored and apply policies that alert you to policy violations, such as when sensitive data is potentially in the wrong locations or has excessive access.

You can then audit to see who has access to that senstitive data and ensure that access is required for business purposes. Having this information also allows you to proactively apply higher levels of protection to ensure you have visibility into what sensitive data is where and who has access, mitigate at-risk data, and monitor if protection levels have changed. With data exfiltration ransomware attacks on the rise, this can help proactively ensure data controls if implemented prior to an attack or help you quickly scan and identify potential exposure levels after an attack occurs.

# Accelerate the Recovery Process

While protecting and isolating data and backups are part of an extensive defense, in-depth strategy, being able to quickly recover in the event of failure or attack is the most critical part of any backup solution.

A strong backup and recovery solution should be designed for fast, reliable disaster recovery. If restoring a database takes days, this means your critical business systems are not functional. The restore process needs to be seamless and easy

to execute. Your backup solution must also automatically discover new resources and ensure they are backed up in line with your backup policies to ensure that you have complete coverage of your environment.

Backup data should be instantly available and enable you to recover without any rehydration. Many backup solutions struggle with restoring multiple systems at one time because of the CPU overhead involved in rehydrating many files at once. This can greatly increase latency and add many hours to your restore process.

Also, many systems may require you to fully restore a backup to identify the state of the data. Live mount backup technology allows you to examine your files and quickly identify your last known good state.

## DON'T PUT IT OFF

You've reached the end of the jungle, and come out safe on the other side. It was a short journey, but one we hope you feel was worthwhile.

As you've seen, being able to restore your data is one of the most important functions your IT organization provides. The tools you choose should allow you to quickly detect abnormal behavior, diagnose attack impact, and quickly restore your data easily from ransomware-proof, immutable backups built on a secure architecture.

When you're researching backup solutions, consider what Rubrik offers across its Cloud Data Management and Polaris platform. It helps securely protect your data for instant

recovery and offers added intelligence on attack impact and sensitive data exposure. If you'd like to learn more, reach out to Rubrik and request a demo, to see these tools in action.

Whatever you do, don't put off efforts to protect your data from ransomware, data exfiltration, and other security threats. Get started now. Tomorrow might be too late.

# About Rubrik


Rubrik helps enterprises achieve data control to drive business resiliency, cloud mobility, and regulatory compliance. Rubrik bridges the gap between owned, on-premises infrastructure and the cloud by decoupling data from the data center through a software-defined fabric and offering a single management plane for all data, whether on-prem or in the cloud. Comprehensive data management is delivered through instant access, automated orchestration, and enterprise-class data protection and resiliency.

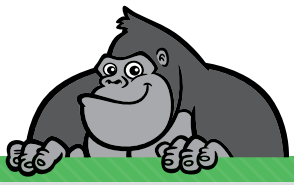
# About ActualTech Media

ActualTech Media

ActualTech Media is a B2B tech marketing company that connects enterprise IT vendors with IT buyers through innovative lead generation programs and compelling custom content services.

ActualTech Media's team speaks to the enterprise IT audience because we've been the enterprise IT audience.

Our leadership team is stacked with former CIOs, IT managers, architects, subject matter experts and marketing professionals that help our clients spend less time explaining what their technology does and more time creating strategies that drive results.



**If you're an IT marketer and you'd like your own custom Gorilla Guide® title for your company, please visit https://www.gorilla.guide/custom-solutions/**