rubrik

EBOOK

How to Develop a Ransomware Remediation Plan for Cyber Resiliency

Table of Contents

Introduction

As enterprises adopt data-driven business models to increase agility, data has become more lucrative for cyberattacks. Even with defense mechanisms in place, ransomware attacks continue to rise and successfully encrypt organizations' data. In the first quarter of 2019 alone, ransomware attacks grew by 118% with new ransomware families detected.[1]

Backups are one of the most, if not the most, important defenses against ransomware. But if subject to corruption, attackers will use it against you. **Advanced ransomware is now targeting backups, modifying them or completely wiping them out, compromising the last line of defense and maximizing chances of ransom payout.** Despite advising against paying ransoms, the FBI estimates extortionists will earn over $1 billion.[2]

If paying ransom is an unreliable recovery option, why do organizations continue to pay? That's because recovery can be painful and time-consuming—if you even have backups to recover from. Furthermore, businesses lack visibility into the scope of damage, forcing them to perform mass restores of their entire environment instead of just recovering impacted data, which ultimately leads to higher data loss.

Organizations should not be forced to trade off paying a ransom with costly downtime. Instead, they should be able to rely on their backups to recover quickly with as little data loss and financial impact as possible. Developing and testing a strong remediation plan prior to an attack should be a top priority for IT organizations.

This eBook will walk through what to look for in a backup and recovery solution and how to build an effective ransomware remediation plan to ensure you can quickly respond to a cyberattack without paying any ransom.

118% **Increase in ransomware attacks (Q1 2019)***

Advanced ransomware now targeting backup files

FBI estimates cybercriminals will earn over $1 billion in ransom**

Delivery via a range of mechanisms, such as phishing emails and exploit kits

* McAfee Labs Threats Report, August 2019
** Fall 2019 OCR Cybersecurity Newsletter - The U.S. Department of Health and Human Services

Selecting the Right Backup and Recovery Solution for Cyber Resiliency

Restoring files from a backup should be your safest and most reliable solution for recovering from ransomware. How do you determine what data protection vendor best prepares you for a ransomware attack? While there is no one-size-fits-all approach, there are critical features of a ransomware remediation plan that all organizations should consider:

Instant Recovery

The biggest pain for most ransomware victims is recovery. Often, organizations rely on complex, multi-step restores that are error-prone and inefficient, ultimately leading to more downtime. The longer a recovery takes, the more impact the attack has on revenue, employee productivity, and customer loyalty. This is true for any security incident—whether it's ransomware, an insider breach, or rogue employee.

A strong backup and recovery solution should be designed for fast, reliable disaster recovery. Even in the event of a security breach, it should be easy to identify and restore to the most recent clean version of your data, whether you need to do a full or partial system restore, and avoid business closure or critical system failures. Backup data should be instantly available and enable you to instantly recover without any rehydration required. Additionally, leveraging automation via APIs allows greater flexibility when restoring and can speed up search and recovery at a large scale.

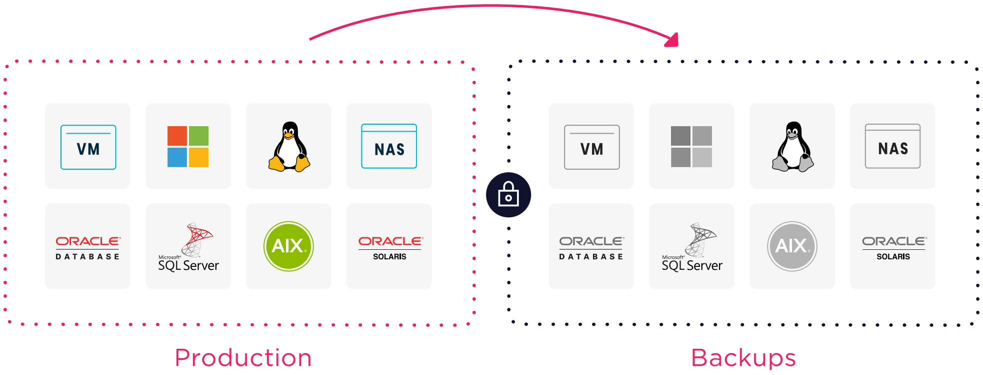
Key Questions to Ask Vendors

Can you deliver near-zero recovery time objectives (RTOs) for VMs, file shares, and databases?

Can you execute instant file recovery without rehydration of data?

Native Immutable Filesystem

One of the reasons enterprises are unable to recover from a ransomware attack is that backups become compromised, forcing IT teams to either pay the ransom or restore from offsite backups. Be cautious of data protection vendors that advise offsite backups as the primary recovery option. This can take weeks to months to restore and is often subject to data integrity challenges, leading to longer RTOs. Additionally, some backup vendors advise implementing an isolated recovery to address ransomware. While this is a viable option, it comes with a large cost burden and management complexity to implement—think of it as equivalent to the operational and financial overhead as a DR infrastructure.



Immutable filesystems prevent attacks from accessing or encrypting data.

How can you ensure your online backups are not compromised by ransomware? The best and easiest way is to select a backup and recovery vendor that stores all applications and data in an immutable format, meaning that no external client can read, modify, or delete data once it's been ingested. Backup data should never be available in read/write mode to an external client at any time, as this easily opens up that data to being corrupted or deleted by an attacker.

Key Questions to Ask Vendors

How can you guarantee your backups are not susceptible to ransomware?

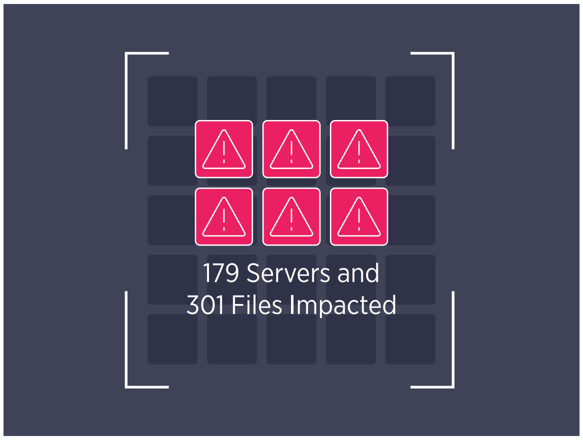
Do you store your backups in native formats open for attack?

Do you require an open read/write SMB or NFS share for backup archives?

Do you encrypt and digitally fingerprint every backup to ensure integrity?

Granular Impact Diagnosis

Performing the restore is only one part of the recovery. Knowing *what applications and files to restore and where they're located* is usually more difficult. Minimizing data loss from a ransomware attack requires IT teams to be able to quickly identify its impact. The manual process of assessing the affected surface area typically involves sifting through millions of files to pinpoint the breadth of the attack. This can take days to weeks, and most businesses resort to mass restores of the entire environment, including uncompromised data, to avoid further delays.



Technologies that help automate the assessment of an attack's impact and provide a clear view into what applications and files were encrypted, and where those reside, enable IT teams to quickly restore at a more granular level. This minimizes the risk of data loss associated with mass restores.

Key Questions to Ask Vendors

Do you alert on the presence of abnormal file access and encrypted files?

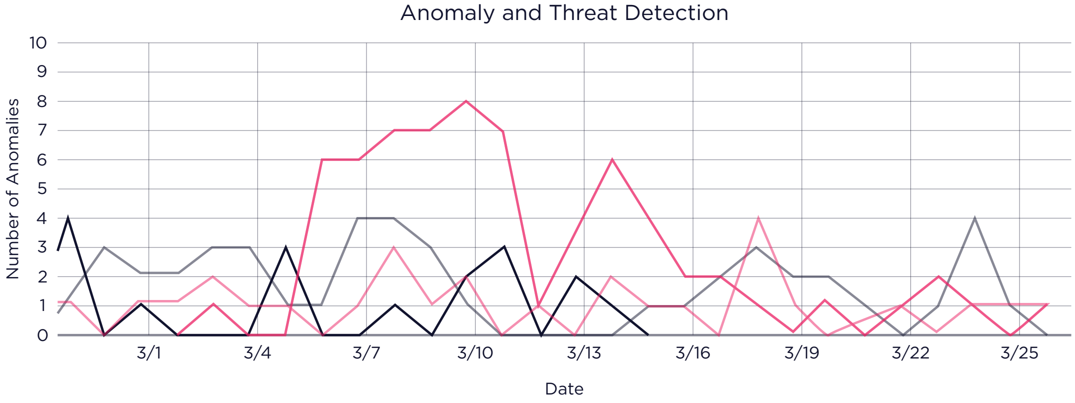
Are you able to show which files are impacted from a ransomware attack?

Do you allow for surgical file-level recovery of only impacted files and data?

Multi-Layered Defense with Added Detection

Ransomware continues to get more and more sophisticated, meaning that even the best prevention efforts can leave you vulnerable to an attack. According to the 2019 Verizon Data Breach Investigations Report (DBIR), 56% of analyzed breaches took months or longer to discover.[3] Delayed detection can directly impact the integrity of backup and recovery data.

Modern technologies that leverage machine learning models can help detect security threats through deep analysis of filesystems and content behavior. Backups contain rich metadata that can be securely analyzed to detect and generate alerts on anomalous activity with ML-based technologies as your last line of defense to complement your real-time detection and prevention tools. When unusual behavior such as ransomware is detected, IT teams should be alerted immediately to investigate and accelerate recovery if needed.



Some vendors use signature-based detection that compare patterns and sequences to a system of known malware variants. However, this is not always an effective approach since ransomware easily mutates. In addition, signature-based detection is only valid if you are not the first victim. Most ransomware attacks use a morphing and code obfuscation approach with a zero-day signature, so signature-based detection will only be valid after the first victim. A better approach is to select a vendor that employs behavioral-based detection, which will still catch zero-day ransomware attacks.

Key Questions to Ask Vendors

What method do you use to detect ransomware attacks?

Does your platform leverage ML-based technologies?

Additional Technical Requirements of a Secure Architecture

To ensure proper protection against ransomware, best-in-breed backup and recovery vendors implement strong security controls by design. Here are a few technical requirements when evaluating the underlying architecture:

- Access to the filesystem to perform read/write operations is available to only the vendor at all times and never to an external client.
- Vendor does not expose any standard storage protocols, such as NFS or SMB, for interacting with the filesystem.
- Vendor does not allow read access of data in its native format to external clients.
- Vendor performs backup validation checks to ensure backup data is never changed. This ensures that you only restore exactly what was in the original copy.
- Immutability is native to the filesystem with no user configuration or management needed.

Key Learnings from Real-Life Ransomware Attacks

The following stories are real-life examples of how various organizations responded to ransomware attacks with insights into what makes an effective strategy.

Kern Medical Center Quickly Recovers 100% of Protected Systems

Kern Medical Center, a leading Central Valley healthcare organization, was attacked by ransomware in June 2019 that infiltrated their environment and began encrypting production data, rendering it unusable. The attack was discovered after an hour when users reported they couldn't access their systems. With Rubrik, they were able to recover 100% of the impacted systems within minutes, including recovering their business-critical electronic medical record system. Post-attack, Kern Medical Center moved more of their legacy systems to Rubrik to protect against potential future attacks, citing immutable backups as a major driver in this decision.

ASL Airlines France Builds a Multi-Leveled Ransomware Defense Strategy

ASL Airlines France, a cargo and passenger airline based in Tremblay-en-France at Bâtiment Le Séquoia, operates in an industry that's highly targeted by ransomware. Due to this high risk, it's incredibly difficult for ASL and other airlines to obtain cyber insurance. They leverage Rubrik's multi-leveled defense to accelerate discovery of cyberattacks, gain detailed impact assessment, and simplify ransomware recovery. With this solution in place, ASL Airlines is approved for cyber insurance to proactively protect the business against cyberattacks.

The City of Durham Rapidly Recovers from Natively-Immutable Backups

The City of Durham detected a ransomware attack on Friday, March 6, and their leaders credited their quick response to Rubrik's backup solution. With Rubrik's built-in immutability, they were able to quickly restore critical city services, including access to 911. In addition, Kerry Goode, Durham CIO, emphasized that core business systems, including ones that manage payroll, were back online by the start of the business week.

> “The city can be assured that our backups are very good because they're immutable. [This means that] they could not be consumed by ransomware.”
>
> **Kerry Goode**
> CIO at The City of Durham

Ransomware Remediation Checklist

The ability to quickly identify the impact of and recover from a cyberattack is the goal of any ransomware remediation plan. To ensure fast recovery and that business goals are still met after an attack, IT teams must map out and rigorously test their response strategy.

Here are suggested steps to take in the event that you've been hit by ransomware:

□ **Isolate the infected device from the network.**

The success of a ransomware attack is dependent on how quickly it can spread across your network. A fast response can greatly reduce the impact to your organization and prevent the infection from spreading. To isolate the infection, immediately shut down and disconnect all compromised devices from the network and any shared storage. Power-off all devices that have not been infected as well to contain the damage.

□ **Ensure backups have not been compromised.**

Ransomware is getting increasingly advanced, putting the integrity of backups at greater risk. To protect your backups, backup data must be immutable. This means that once data has been written, it's never available in read/write mode to external clients, and cannot be read, modified, or deleted by an attacker on your network. This is the only way to ensure recovery when production systems are compromised.

In addition, pause all backups until you understand where the infection originated and completed all security forensics, and ultimately have identified the most recent clean snapshots.

□ **Identify the infection.**

It's critical to understand how far-spread the infection is in order to seal it. One starting place is to assess what was accessed by the first infected machine. Another option is to check the ransomware registry, which lists all the encrypted files so that the software knows which files to decrypt once the ransom is paid. Consult your security team or specialists to help conduct the forensics.

□ **Check retention time.**

It may be advantageous to extend retention times of your backups during impact analysis and remediation. Short retention times increase the risk of backups expiring prior to the completion of remediation efforts. Extending retention times will help ensure recovery to the most recent clean state prior to the infection.

□ **Activate your response plan.**

Finally, it's time to engage your incident response team, notify the key stakeholders, and evaluate your options so that you can retrieve your data and get back online. These are the courses of action to choose from:

Option 1: Restore your files from backup. The most reliable way to recover from a ransomware attack without paying the ransom is to restore the affected machines to the most recent clean state. That's why having a comprehensive backup plan that is regularly tested is critical to any effective ransomware response plan.

Note that not all data protection solutions will safeguard your backups in the event of an attack, and backups can become compromised. That's why it's highly recommended to choose a solution that prevents ransomware from ever modifying your backup data while also providing fast restores and greater visibility.

Option 2: Attempt to locate a decryptor. Once you've determined the exact strain of ransomware, it may be possible to find a decryptor through third-party sites. However, newer versions of ransomware are more sophisticated and mutate quickly, making it less likely that a decryptor is available.[4] In addition, when relying on a third-party decryptor, you risk downloading additional malware, so it's not a reliable or advisable solution.

Option 3: Do nothing and accept the data loss. Organizations that lack a strong backup strategy prior to the attack or are unable to locate a decryptor may choose to not recover their files. Of course, a strong ransomware remediation plan should then be developed, tested, and put in place to ensure a rapid recovery in the event of a future attack.

Option 4: Negotiate and pay the ransom. For those who have tried all other options and are unable to recover their files, paying the ransom may seem like the only viable solution. The FBI and most security experts strongly warn against paying any ransom because it does not guarantee that you'll get all or any of your data back. A 2019 report by CyberEdge Group shows that 17% of organizations that opted to pay the ransom never obtained access to their encrypted data or infected systems.[5] Paying the ransom also incentives future attacks—potentially at a higher ransom—opening up your business to even more risk and perpetuates the cycle of attacks by rewarding the bad actors.

- □ **Diagnose the scope of infection.**
  Minimizing data loss from a ransomware attack requires IT teams to be able to quickly identify the impacted applications and files—a process that can take days to weeks with legacy technology. However, it is critical to first determine which applications and files were impacted and where to roll back at a granular level. This will minimize the risk of data loss associated with mass restores that include uncompromised data.

- □ **Alert the authorities.**
  Following an attack, inform law enforcement, customers, and any other necessary authorities. Certain organizations may be legally required to notify authorities and users; this is highly dependent on your business, industry, and location.

Disclaimer

This document is intended to supplement, not replace, existing ransomware response, remediation, and disaster recovery plans.

This template is made available “as-is”, without warranty, and is free from liability for damages resulting in the use of information provided in this template—and has not been endorsed by any official body or organization.

Customization of this template, and testing of the plan, is a requirement for success.

Sources

1 *McAfee Labs Threats Report, August 2019.* McAfee, www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-aug-2019.pdf.

2 *Fall 2019 OCR Cybersecurity Newsletter: What Happened to My Data?: Update on Preventing, Mitigating and Responding to Ransomware.* The U.S. Department of Health and Human Services, https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-fall-2019/index.html

3 *2019 Data Breach Investigations Report.* Verizon, https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

4 Alessandrini, Adam. *RANSOMWARE: Hostage Rescue Manual.* KnowBe4, 2016, www.wired.com/wp-content/uploads/2016/03/RansomwareManual-1.pdf.

5 *2019 Cyberthreat Defense Report,* CyberEdge Group, LLC. https://cyber-edge.com/wp-content/uploads/2019/03/CyberEdge-2019-CDR-Report.pdf

rubrik

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

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