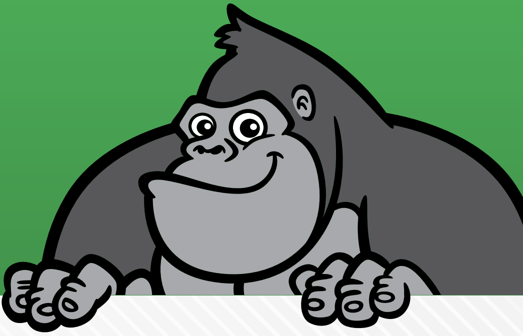
ActualTech Media

rubrik

The Gorilla Guide to...®

Express Edition



Buyer's Guide to Ransomware Recovery

Ed Tittel

Inside the Guide

- What Happens When Ransomware Strikes
- Key Features for Defeating Ransomware
- Making Backup and Recovery Ransomware-Ready

THE GORILLA GUIDE TO...

Buyer’s Guide to Ransomware Recovery

Express Edition

By Ed Tittel

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

Ed Tittel is a 30-plus-year veteran of the IT industry who writes regularly about cloud computing, networking, security and Windows topics. Perhaps best-known as the creator of the *Exam Cram* series of certification prep books in the late 1990s, Ed writes and blogs regularly for GoCertify.com, Win10.Guru, ComputerWorld, and other sites. For more information about Ed, including a resume and list of publications, please visit EdTittel.com.

ENTERING THE JUNGLE

CALLOUTS USED IN THIS BOOK

The Gorilla is the professorial sort that enjoys helping people learn. In the School House callout, you'll gain insight into topics that may be outside the main subject but are still important.

This is a special place where you can learn a bit more about ancillary topics presented in the book.

When we have a great thought, we express them through a series of grunts in the Bright Idea section.

Takes you into the deep, dark depths of a particular topic.

Discusses items of strategic interest to business leaders.

ICONS USED IN THIS BOOK

DEFINITION

Defines a word, phrase, or concept.

KNOWLEDGE CHECK

Tests your knowledge of what you've read.

PAY ATTENTION

We want to make sure you see this!

GPS

We'll help you navigate your knowledge to the right place.

WATCH OUT!

Make sure you read this so you don't make a critical error!

TIP

A helpful piece of advice based on what you've read.

INTRODUCTION

Welcome to the Buyer's Guide to Ransomware Recovery! If you need to protect yourself from the latest security scourge, you've come to the right place!

Only readers who've been off planet for a while will be unaware that ransomware poses a huge risk to businesses of all kinds and scales. But the scope and impact of ransomware keeps creeping up, as does the damage it leaves in its wake. In fact, Cybercrime Magazine predicts a ransomware attack will occur every 11 seconds by the end of 2021—nearly 8,000 attacks daily. That could translate into global damages of $20 billion according to the same source, which goes on to calculate that this level is 57 times greater than in 2015. It's no surprise to learn further that this "makes ransomware the fastest growing type of cybercrime."

When ransomware strikes, business pulls to a screeching halt as that malware encrypts drive contents and locks users out of systems, software, and data. The company is informed that the data will remain inaccessible until they pay a ransom, usually in BitCoin or some other anonymous digital currency—after which they'll obtain a decryption key to make the data accessible again. If that sounds too good to be true, it often is. In fact, the FBI recommends against paying ransoms. Reports from ransomware victims indicate that less than half of those who pay regain access to their systems, yet SecurityBoulevard reported in April 2020 that an increasing number of companies are caving in anyway. They indicate that 39% of victims paid ransoms in 2018, 45% in 2019, and 58% are expected to have done so by the end of 2020.

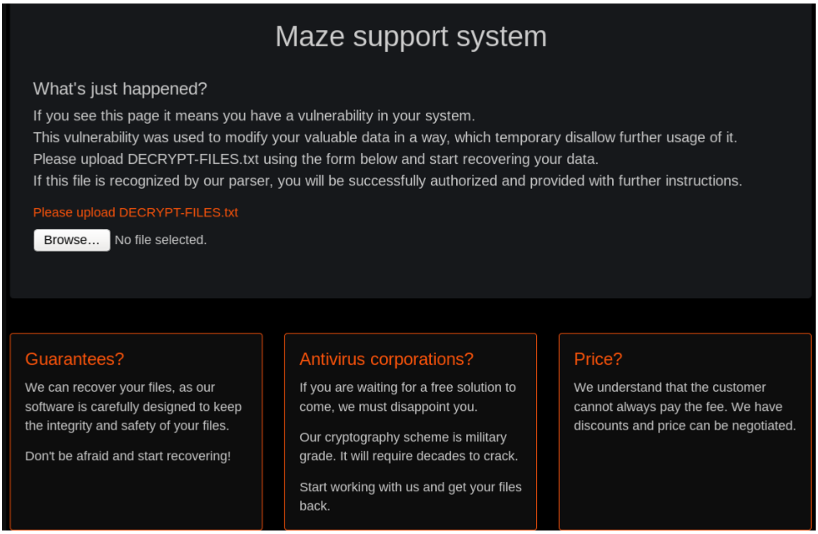
Given the odds, why do organizations pay ransoms? Many do so because they find themselves unable to recover. Some pay because recovery through other means could mean lengthy downtime and loss of vital services. (In 2016, for example, a California hospital found itself compelled to pay ransom to get its emergency room scheduling and patient records and billing systems back online.) It's far better to heed the FBI's advice and to counter ransomware with the tools and methods they recommend—in particular, backing up your data regularly and securing those backups.

This Guide is written for anyone with responsibility for an organization's IT security, from CISOs to CTOs to the frontline admins charged with keeping data safe. So let's enter the jungle, ready to do battle with the bad guys. We start with a discussion of how ransomware works.

CHAPTER 1

What Happens When Ransomware Strikes?

The mechanics of ransomware are glaringly obvious. Through a variety of illicit means, the malware takes up residence on end-user computers and servers. Once it starts running, ransomware systematically encrypts all the drives and volumes it can access. As soon as it blocks access to those assets, it pops up a message informing the reader it has encrypted all files, making them inaccessible. Another type of ransomware exfiltrates the files it finds before locking them up, so that victims may be further extorted through threats of public disclosure or sale of files and data to third parties.



Maze support system

What's just happened?

If you see this page it means you have a vulnerability in your system.
This vulnerability was used to modify your valuable data in a way, which temporary disallow further usage of it.
Please upload DECRYPT-FILES.txt using the form below and start recovering your data.
If this file is recognized by our parser, you will be successfully authorized and provided with further instructions.

Please upload DECRYPT-FILES.txt

Guarantees?

We can recover your files, as our software is carefully designed to keep the integrity and safety of your files.

Don't be afraid and start recovering!

Antivirus corporations?

If you are waiting for a free solution to come, we must disappoint you.

Our cryptography scheme is military grade. It will require decades to crack.

Start working with us and get your files back.

Price?

We understand that the customer cannot always pay the fee. We have discounts and price can be negotiated.

Figure 1: What a typical ransomware demand looks like (Maze, 2019, still current) Source: CYBERSECasia

A typical ransom demand (from the still-active Maze, 2019) looks like what's shown in **Figure 1**.

Ransomware can be spread in a variety of ways. It often arrives through phishing email with malicious attachments. It may arrive via drive-by download (a download triggered automatically when visiting a malicious or compromised website). Social media has been implicated in some ransomware attacks via attachments to instant messaging facilities. Once ransomware appears on a network, it will attempt to encrypt networked drives, shares, and other network storage resources. This can lead to rapid proliferation across multiple systems.

Mechanics aside, ransomware is a kind of denial-of-access attack. This can have profound repercussions on businesses and other organizations that depend on computer access to function. First and foremost, ransomware imposes productivity and opportunity costs. Opportunity costs come into play because those same people can't accept new business, clients, or transactions. If a company remains sidelined long enough, it will not only lose money, it may start losing customers. And, if word gets out that a company is sidelined owing to ransomware, this can damage the company's brand(s) and reputation. In short, it's a nasty, expensive, and bothersome mess.

The Right Way to Recover from Ransomware

Assume for an uncomfortable moment, please, that your company or organization has fallen victim to ransomware. You already know that paying the ransom may or may not get you out of jeopardy and back to work. What, then, is the right way to recover, given advance access to proper tools, preparation, planning, and execution? Good question. Before we dig into some good answers, to elaborate on the importance of backups and supporting technology, let's revisit the potential damage that ransomware can cause.

Recent Ransomware Attacks and Their Costs

In August 2020, Nationwide Insurance published a study, "The Cost of Ransomware Attacks," based on its analysis of security incidents through Q1 2020. This study's highlights read (quoted verbatim):

- The average enterprise ransom payment is $111,605.
- 205,280 organizations were affected by ransomware attacks in 2019
- The average cost for victims of ransomware attacks to recover more than doubled in the final quarter of 2019. According to a new report from Coveware, a typical total now stands at $84,116. That's a little over double the previous figure of $41,198.

In particular, the Nationwide study cites the increasing costs of "significant business interruption" as a follow-on to dealing with ransomware itself. They go on to observe that "… once a business has been infected, they may face long-term reputational harm, have to pay a considerable sum for forensics experts to investigate their system, or invest in additional IT expenses to prevent future attacks."

Although the July 2020 Cybersecurity Insiders article, "Costliest Ransomware Attacks of 2020," covered only the first seven months of the year, it still found devastating business outcomes. Here's what it found:

- ISS World announced in March that ransomware impacted its email servers. Recovering from that attack cost $74M, and left hundreds of employees without access to systems and email for weeks.
- Cognizant fell victim to a ransomware attack in April, which is said to have cost the company between $50 and $73M for

recovery, including legal, consulting, and data recovery costs, in addition to outright financial losses reflected in its Q2 2020 earnings report.

- The United Kingdom's Redcar & Cleveland Borough Council experienced a ransomware attack that disrupted its network, tablets, computers, and mobile devices for three weeks. In March, the council informed the press that it would take months to recover, with associated costs of $14M to $21M.
- On New Year's Eve, foreign exchange giant Travelex reported that malware shut down internal networks, its website, and several of its client apps for a week. *The Wall Street Journal* ran a story that Travelex paid $2.3M (285 BitCoin) to free up locked data.
- Phishing is named as the source for a ransomware attack on California company Communications & Power Industries, which took its storage servers offline. Authorities reported that the company paid $500K for a decryption key to unlock those servers.

In the period from Jan. 1 to Jan. 26, 2021, the value of BitCoin has fluctuated from a low of $29K or so (1/1) to a high of $40.5K (1/8). Right now (on Feb. 1, 2021), it's trading at $34,013. One year ago, BitCoin traded at around $10K. This digital currency is increasingly volatile and expensive. It's also a preferred form of payment for digital ransoms. Alas, this suggests yet one more reason to avoid paying ransoms, especially those demanded in BitCoin (or fractions thereof): It can be incredibly expensive. Moreover, the FBI observes that paying a ransom to criminals can have serious legal implications, which organizations must explore with legal counsel before acting.

- Other firms' and organizations' ransom payments include UCSF ($1.14M), La Salle County, Texas (>$500K), Grubman, Shire Meisalas & Sacks ($365K paid, additional $42M demanded), Tillamook County, Ore. ($300K), the city of Florence, Ala. ($291K), and San Miguel County, Colo. ($250K).

Note that all of these amounts are well in excess of the typical average values of $111K in ransom payment and $85K in recovery costs cited in the previous Nationwide study.

Ultimately, companies and organizations that can identify and restore the correct backed-up files and systems are those who can avoid paying any ransom. The best way to make this work is to use a system that provides "intelligent recovery"—capabilities that depend on fast and easy restores to the most recent clean snapshots, ML-driven file system monitoring for malicious or unscheduled changes, and immutable backups that ensure they're safe from encryption.

CHAPTER 2

What Kind of Backup/ Recovery Can Handle Ransomware?

Using a safe, secure backup to replace files illicitly encrypted by ransomware is the best recovery option available when it comes to foiling such attacks. Given access to current, safe replacements, and the right tools to find and restore encrypted files to production or end-user systems, there's no need to pay any ransom. This raises a key question when it comes to evaluating backup/restore systems already in place or when considering possible alternatives—namely, what are the key features in a backup/recovery system that enable it to deal quickly and effectively with ransomware attacks?

Backup/recovery systems represent the last line of defense in providing ransomware protection. They're not intended to replace or substitute preventive and protective measures, such as firewalls, application gateways, or anti-malware screens, scans, and filters. Rather, an intelligent recovery represents the organization's final layer of defense against ransomware, one that will be invoked only if and when a ransomware attack succeeds. In fact, recent statistics mentioned earlier favor "when" not "if" when it comes to experiencing attack. When that happens, intelligent recovery will put things back the way they were before the attack occurred.

Key Features for Defeating Ransomware

For any given file locked away by ransomware encryption, two key items of information are absolutely essential to restore a usable replacement:

- When did the affected file become inaccessible?
- Which backup of that file is time-stamped as close as possible before that change?

As long as it can be irrefutably proven that the backup itself is free of malware, it’s precisely that version that should be restored to undo the ransomware encryption with minimal impact.

This requirement establishes an essential feature for a backup/restore system capable of dealing with ransomware: It must track file system changes so it can identify when individual files have been altered or rewritten. It should be able to identify, locate, and retrieve the most recent and clean backup version of that same file, and restore it quickly and easily with minimal manual oversight and involvement from administrators and operators. Since the time factor in recovery is always important (“time is money” applies even more forcefully when systems are down and business is interrupted), these tools leverage automation in driving such recovery speeds and reduce additional costs related to human time and effort.

It’s also important to make sure that backup policies are clear and reliable. Above all, the most recent snapshots must honor RPOs and RTOs to maximize uptime and minimize data loss. Organizations must test their backup and restore operations, not just to make sure they work, but also to make sure the underlying security and backup policies are in keeping with RTO, RPO, and compliance and governance requirements.

Understanding RTO and RPO and Their Business Impact

Recovery Time Objectives (RTOs) represent the maximum amount of time a computer, system, network, or application can remain out of service following a failure or disaster event. This interval captures two important concepts. First, RTO is the longest time an organization can tolerate the absence of an IT infrastructure component without suffering significant damage. Second, it should capture how long it takes for the component to go from being offline to going through recovery and returning to service. The higher the value of (or the greater the cost of doing without) an IT infrastructure component, the more an organization is usually willing to spend to shorten RTO as much as possible. Thus, RTO succinctly captures the notion of "How long should it take for certain applications, services, and capabilities to return to normal after an interruption or disaster?"

Recovery Point Objectives (RPOs) represent the maximum amount of data loss a company or organization can withstand before significant harm is likely. Thus, RPO is also a time interval, but it measures how far back in time the most recent backup must be with respect to a failure or disaster event. Setting an RPO requires deciding how much data you can stand to lose and making backups at corresponding frequencies. Typical intervals are 24, 12, 8, or 4 hours. Anything 4 hours or less demands scheduled snapshot replication; 8 hours or longer typically works within the scope of typical backup systems (though most modern backup systems use snapshot replication anyway, to capture snapshots of active systems without forcing them to pause or imposing performance penalties).

Both RTO and RPO have business impacts. For either interval, certain levels of loss and disruption may be involved. When either or both intervals are short, additional expense must be incurred to make it (or both) possible.

Do RTO and RPO Really Matter?

Indeed, both RTO and RPO do matter because they determine how much a company or organization is willing to spend on backup and recovery tools and technologies. Ultimately, both intervals determine how much loss an organization is willing to withstand. RTO sets a time limit on how long interruptions can last; RPO sets a limit on how much data an organization can lose, and sets a time limit for intervals between backups and/or replication snapshots. Among other things, these values also tie into an organization's disaster recovery (DR) and business continuity (BC) plans, as described in the next section.

Potential Roles for DR and BC

Disaster recovery defines how an organization can recover from an incident that renders its normal business operations impossible or untenable. Disasters may be natural (hurricane, flood, earthquake, and so forth) or manmade (acts of war or terrorism, industrial accidents or mishaps, and so on). Either way, they result in catastrophic interruptions of service. Planning and preparation are key to DR, because declaring a disaster and implementing a DR plan involves moving business (including IT) operations to a different location, bringing up (or switching over to) new equipment, and restoring backups (or snapshots) to resume operations. Business continuity covers how the organization keeps going in the interval between when the disaster occurs and when recovery is complete and operations resume. BC, likewise, requires planning and preparation, and includes obtaining and securing backups as a key element on its to-do list. Thus, backup/recovery systems and the backups and/or snapshots they create and manage are essential for both BC and DR, especially when ransomware strikes.

In particular, companies and organizations evaluating backup/recovery systems for their ability to respond quickly and well to ransomware attacks should examine the following discussions closely and carefully.

Data Availability

For a restore to succeed—for one file or all files—it must remain available even in the face of downtime or disaster, as must the recovery facility that performs such restores. Thus, it's important to make sure that backups are stored in a location that remains accessible even if one or more sites are offline. Likewise, it's essential that backups are secured from tampering and all other forms of unwanted and unauthorized access. When ransomware strikes, it will try to encrypt backups just as readily as any other file it encounters. For backups to be truly available, this can't be allowed to happen.

Ease of Access, Investigation, and Restore

If the backup/restore environment is tracking file system activity, it will be able to quickly report all changed files within some arbitrary time interval ("in the past hour," for example, or "since 1:15 p.m."). The resulting list of files should be amenable to analysis to determine which such changes are routine and which are potentially anomalous. Ideally, ML-driven anomaly detection can quickly flag all irregular items. The resulting list might be reviewed and pruned to drive actual restores, or the entire list might be handed over to a restore facility immediately for restoration in the event of a wholesale ransomware attack.

Avoiding Complexity and Configuration Issues

When interruptions of service or business capability occur, time is of the essence in meeting RPOs and RTOs. This also limits the potential for financial losses and damage to an organization's brand(s) and reputation. Thus, it's essential that backup/restore systems be well-understood, and ready to undertake a return to "business as usual" as quickly as possible in the event of an incident. Where ransomware is involved, this means the ability to detect whether anomalies are present, to pinpoint them swiftly, to identify the corresponding elements and files in the most recent backup or snapshot available, and to commence targeted restore operations as swiftly as possible. Thus, a backup/restore system should be preconfigured and ready to respond to ransomware attacks on demand. Administrators shouldn't have to dig into a manual or a help file to figure out the sequence of commands and inputs needed to get a targeted restore underway. They should already be restoring encrypted files and undoing ransomware's damage.

Automated Ransomware Response

Indeed, automation is widely recognized as a vital improvement for IT operations of all kinds. Two primary factors influence its benefits. First, automation can respond in computer time (usually measured in microseconds to milliseconds) when events occur. Humans, on the other hand, do well to respond to events in seconds to minutes, if they can even react immediately as events occur. This is an eternity when ransomware is already encrypting files—easily thousands of files per second, except for the largest files. Second, automation must be thoroughly tested before it's deployed into production environments, so its bugs and errors are worked out in advance. Humans working with a mouse and keyboard do make mistakes, especially under pressure. Thus, automation is inherently more accurate and reliable, which is why automated ransomware response is absolutely essential to speedy, accurate, and reliable recovery from such attacks. Anything less can't help but take longer. When time is money, automation makes a big difference.

In fact, automation is especially well-suited to speeding ransomware responses. It's particularly adept at compiling a list of changed files, and flagging files that have been unexpectedly (and unwantedly) encrypted. Likewise, automation is ideal for identifying clean replacements for such encrypted files—and for orchestrating writing over encrypted files with clean counterparts. Not only does automation relieve the tedium involved, it's also faster and more accurate.

CHAPTER 3

Making Backup and Recovery Ransomware-Ready

Immutability = Once-Written, Never Changing

An essential part of making backups (and recovery systems) effective against ransomware is to make backups immutable. This means they must be read-only files whose contents can't be changed. Once written, such files can't be created, accessed, or altered by clients on your network. This must be combined with strong user permissions management and authentication controls to minimize potential intrusion points. For example, in Microsoft Windows 10, the accounts with the highest privileges are "System" and "Trusted Installer." They can do things no other accounts can. To resist and prevent ransomware, backup and recovery must work at those levels of privilege (or their equivalents in other OSes) and their files must be inaccessible to all other parties, and incapable of being altered in any way (including encryption). What makes for immutability? Once data has been written, it can't be read, modified, or deleted by network clients.

Secure Backup Architecture

In general, ransomware-ready backup and recovery systems must implement a secure backup architecture. What does this mean? Beyond immutable backups, it also means that such systems must incorporate the following capabilities:

- **Strong user authentication:** Ideally, this incorporates multifactor authentication, so that users not only access accounts with strong passwords, but must also provide additional proofs of identity, such as security tokens, cellphone-supplied validation strings, and so forth. Because malware can impersonate accounts and passwords, additional proofs of identity make successful impersonation far less likely. All operations must be authenticated using appropriate credentials and encrypted communications.

- **Strong encryption:** Backup systems must encrypt all data to meet potential compliance and governance requirements. In addition, storing backups in unencrypted form raises the possibility they could be restored by unauthorized third parties outside the organization's purview or control. Best security practice dictates that backups be encrypted using military-standard encryption both in motion and at rest (such as FIPS 140-2 Level 2 certified self-encrypting drives). Encryption at the hardware level means that only those with access to the Trusted Platform Modules (TPMs) where keys are stored will ever be able to decrypt drive contents. Software-based encryption for data at rest (but not yet written to backup drives) should also use strong TPM-based encryption such as AES-256. Data in motion should use similar encryption techniques, as well as PKI to support secure access to and use of keys.

- **Zero-trust cluster design:** Inevitably, backup and recovery software uses API calls to interact with storage devices and various kinds of services. Because an incoming API call is ultimately just another network packet, there's no telling if that packet comes from a trusted and valid sender or an untrusted malefic actor seeking to subvert the system. In a zero-trust cluster design, only authenticated APIs can request or perform operations. This is achieved using the Transport Layer Security (TLS) 1.2 protocol, certificate-based mutual authentication, and perfect forward secrecy (PFS). This locks API-level access to all unauthorized, unauthenticated third parties, and applies to all API communications (thereby also avoiding man-in-the-middle attacks). All writes for backup should be what's called *out-of-place*, which means that new writes don't alter or overwrite data written earlier. And, finally, backup data should be fingerprinted when ingested and the fingerprints stored with that data. This enables subsequent checks to make sure that once written, data never changes.

- **Support for automation:** As explained in Chapter 2, automation is essential for rapid, accurate responses to events as they occur. Without the ability to automate responses to ransomware file changes, human backup operators would be overwhelmed and outgunned.

- **Sufficient coverage:** A backup system must be able to accommodate all the runtime components active on any of the organization's clients or servers. That means it must be able to capture backups from all the operating systems, databases, applications, service delivery systems, and so forth that the organization runs on its various computers. For many applications, this means knowing how to work with and around their runtime activity and transaction stores, and how to deal with volume shadowing services and storage at the operating system level.

- **Customizable SLAs around RPO and RTO:** A service-level agreement (SLA) usually specifies terms or objectives that providers agree to meet or exceed in the course of delivering services to their clients and customers. A good ransomware-ready backup and recovery system will let its users establish SLAs for RPO and RTO so that they become easy to monitor, track, and analyze. Such SLAs will often reside in third-party systems such as ServiceNow, or within the backup and recovery system itself. Either way, such a system should be able to track snapshot-capture frequency, retention, duration, and desired locations, as well as RTO and RPO metrics.

- **Fast restore is always a factor:** If and when a disaster is declared, backup and recovery systems provide key ingredients to bring the business or organization back to life—namely, the most recent backups or snapshots needed to turn bare metal into working systems. It's essential to make sure that the backup and recovery system can identify and deliver those backups on demand, and that they work when restored. The best backup and recovery systems support on-demand test restores. Likewise, they feed into scheduled DR test runs, which inevitably include test restores, as well.

CHAPTER 4

Intelligence for Detection and Recovery

The best backup and recovery systems make use of intelligence software to support faster and more accurate detection of and recovery from ransomware. This can include machine learning (ML) to identify patterns of behavior. It helps establish a baseline for "normal" filesystem activity against which current activity may be compared. ML can also help to customize general-purpose threat intelligence to match items of interest for a specific organization, based on its systems, software, versions, configuration settings, patch levels, and so forth.

The best backup and recovery systems generally offer some or all of the following capabilities, all of which make use of threat intelligence and/or ML capabilities, and give such systems their most important abilities to respond rapidly and accurately to ransomware:

Detect anomalies: The backup and recovery system applies ML algorithms against application metadata to establish a normal baseline for each machine. It proactively monitors the system, looking at behavioral patterns to flag activity that deviates significantly from the baseline. It also analyzes file properties that include change rates, abnormal system sizes, and entropy changes. Once an anomaly is detected, the system issues an alert via its UI or email. Using ML, such a system continuously refines its anomaly detection model over time to stay ahead of advanced threats.

The Key to ML's Ransomware Value

ML-driven behavioral detection is key to recognizing behaviors that can indicate ransomware attacks. Adding this capability on existing backup data strengthens an organization's multi-layered security as a last line of defense. ML-based tools monitor file system behavior to establish a normal baseline. They can also detect and alert to unusual or suspicious behavior. The very best ransomware-ready backup and recovery systems build in this capability, and provide 24/7 intelligence feeds to drive ransomware detection and identification.

Analyze threat impact with data intelligence: The backup and recovery system continuously scans the entire environment to offer insights on how data has changed over time. Should an attack occur, it can quickly identify impacted applications and files, along with their locations, using simple, intuitive visualizations. Its UI can browse through entire folder hierarchies and drill down to investigate file-level changes, additions, modifications, and deletions. Using this system, organizations minimize not only the time spent discovering what happened, but data losses, as well. They can also locate potential replacement files quickly and easily.

Accelerate recovery to minimize business disruption: A ransomware-ready backup and recovery system empowers users with a simple way to globally manage what should happen. After conducting a ransomware attack analysis, users can select all impacted applications and files, specify a desired location, and restore to the most recent clean versions in just a few mouse clicks. The system automates the rest of the restore process and lets users track progress through its UI. Because backups are immutable, all data is safe to restore. Ransomware can never access nor encrypt backup data.

Identify data exposure: More sophisticated forms of ransomware may do more than encrypt files. Certain forms of ransomware—including the Maze example cited in Chapter 1—can also copy data outside an organization's boundaries to a server or data store of the attacker's choosing. This is called data exfiltration, and this exposure adds to the consequences of a ransomware attack, where such data can be held hostage for further extortion, threats of unwanted exposure or disclosure, and more. If an organization experiences an exfiltration attack it's essential to be able to scan backup data to identify sensitive data that may be exposed in a data exfiltration attack to determine level of risk. In addition, by using tools that can perform such scans and maintain a map of sensitive data proactively, organizations can get quick and easy visibility of what sensitive data exists where and who has access prior to such an attack. Thus, they can make sure sensitive data is kept away from high-access, high-traffic data stores and remediate any such data found in unauthorized locations. This helps minimize chances of sensitive data exposure and potential loss or unwanted disclosure.

Key Questions for a Proper Ransomware Response

When considering a backup and restore system to help you recover from ransomware, or to evaluate your current system in that light, it would be wise to choose one that could answer the following questions affirmatively:

- Does my backup system store all data in an immutable format natively and without requiring user management and configuration?

- Does it support a secure backup architecture with strong authentication, access controls, end-to-end encryption, secure network protocols, API authentication, and absolute immutability for backup data?

- Can the system identify unusual file system behaviors?

- Can it detect anomalies to gain insight into suspicious activities?
- Can it identify data exposed in an exfiltration attack?
- Can it identify all applications and files affected?
- Can it map changes over time?
- Does it provide a granular view of change activity?
- Can it map changed files to their most recent, safe backup counterparts?
- Does it make restore simple and fast? (Does it use automation to restore selected files to the most recent clean versions?)
- Does it support policy-driven automation and encrypt all data end-to-end to cover integrity, compliance, and governance needs?
- Can the system scale easily? Grow to whatever capacity is needed? Accommodate new tools and technologies easily?

All of the key questions for a proper ransomware response are important, but the answers to some can make a huge difference in achieving positive business outcomes and avoiding loss and damage. Simplicity and ease of use; usable, accurate automation; secure APIs; protection of sensitive data through end-to-end encryption; and fastest possible time to recovery are paramount. Likewise, ML-driven anomaly detection fed by actionable intelligence that assesses attack impacts helps drive deeper insight and faster recovery times.

If you don’t like some or all of the answers your questions elicit, it may make sense to investigate Rubrik’s suite of data protection and security solutions. Visit Rubrik to learn how its data management system helps organizations identify attack impact and quickly recover from ransomware attacks.

Don’t Just Survive—Thrive

Throughout this Gorilla Guide, you’ve been exposed to a lot of information, but don’t let it overwhelm you. Ransomware is a scary threat, and one that shows no signs of slowing—in fact, it’s quite the opposite. Every organization is vulnerable, and more and more, companies are feeling like it’s more a matter of “when” rather than “if” it hits them.

But that doesn’t mean there’s nothing you can do about it. Apply the checklists and advice you’ve read about here, and be proactive in your approach, rather than reactive. Stay ahead of the bad guys, and your chances of surviving an attack go way up. Not only that, but you increase your chances of avoiding a ransomware attack altogether.

Stay safe out there!

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.

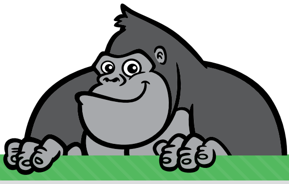
ABOUT ACTUALTECH MEDIA

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/