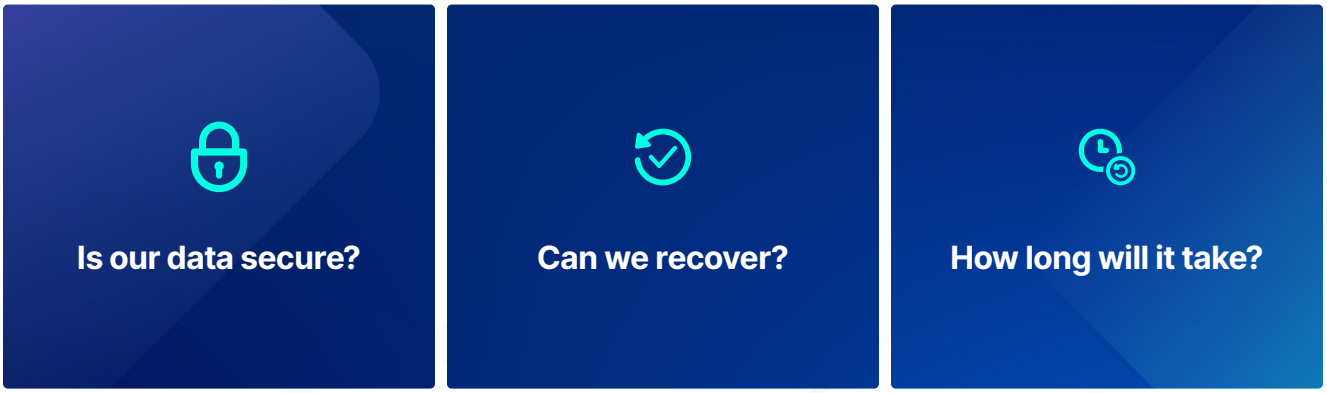
rubrik

YOUR CYBER RECOVERY BLUEPRINT

Navigating Chaos with Decisive Actions When Every Second Counts

Let's start with a little exercise in imagination. Picture this scenario: You're doing your thing, and out of nowhere, you get an alert. It's not just any alert—it's the kind that makes you nervous. It's an alert about malicious activity. You investigate, and your worst fears are confirmed: it's ransomware.

During the crucial hours, you'll be the one in the hot seat. Your stakeholders and leadership will be looking at you for answers to questions like:



If you're even a little unsure, then your job and your business are on the line.

Cyber recovery is not just an IT problem that can be solved by simply having backups; it's about the ability to recover from an attack rapidly and reliably. This requires a fundamental change in mindset, moving away from measuring and performing disaster recovery to optimizing for the fastest possible cyber recovery—to minimize the impact of cyberattacks on your team morale, customer trust, and business revenue.

Let's face it—uncertainty isn't something we handle well, and we tend to shy away from thinking about unpleasant future events.

We convince ourselves, "It won't happen to us." But it's not a matter of IF.

So, what can we do about the chaos that cyberattacks bring?

01

Hope it won't happen to us
That's not a strategy. It's wishful thinking at best.

02

Brace for impact
Less-than-adequate preparation, like showing up to a rainstorm with an umbrella, is just not enough.

03

Become cyber resilient
This is the only wise and forward-thinking decision.

Cyber resilience means preparing ahead of time, testing everything out, and executing plans flawlessly.

In this guide, we'll share what you might experience during the critical hours after a cyberattack. We'll unpack what separates a quick and reliable recovery from a drawn-out disaster. We'll take a look at why what you already have in place might not be enough, and most importantly, what it actually takes to bounce back with speed and accuracy. And to wrap up, we'll share some tools and actionable insights to help you build a business case within your organization and get the budget you need to put cyber resilience into action.

The Aftermath of a Cyberattack

In the critical hours following the discovery of a breach, teams often scramble to assess the damage, identify the time and scope, find clean data, and find ways to recover.

You can either be in PANIC MODE where:

- Chaos spreads
- Teams are fumbling
- Executives are chasing answers
- Disruption is lengthy

Or, you can be in RESILIENCE MODE where:

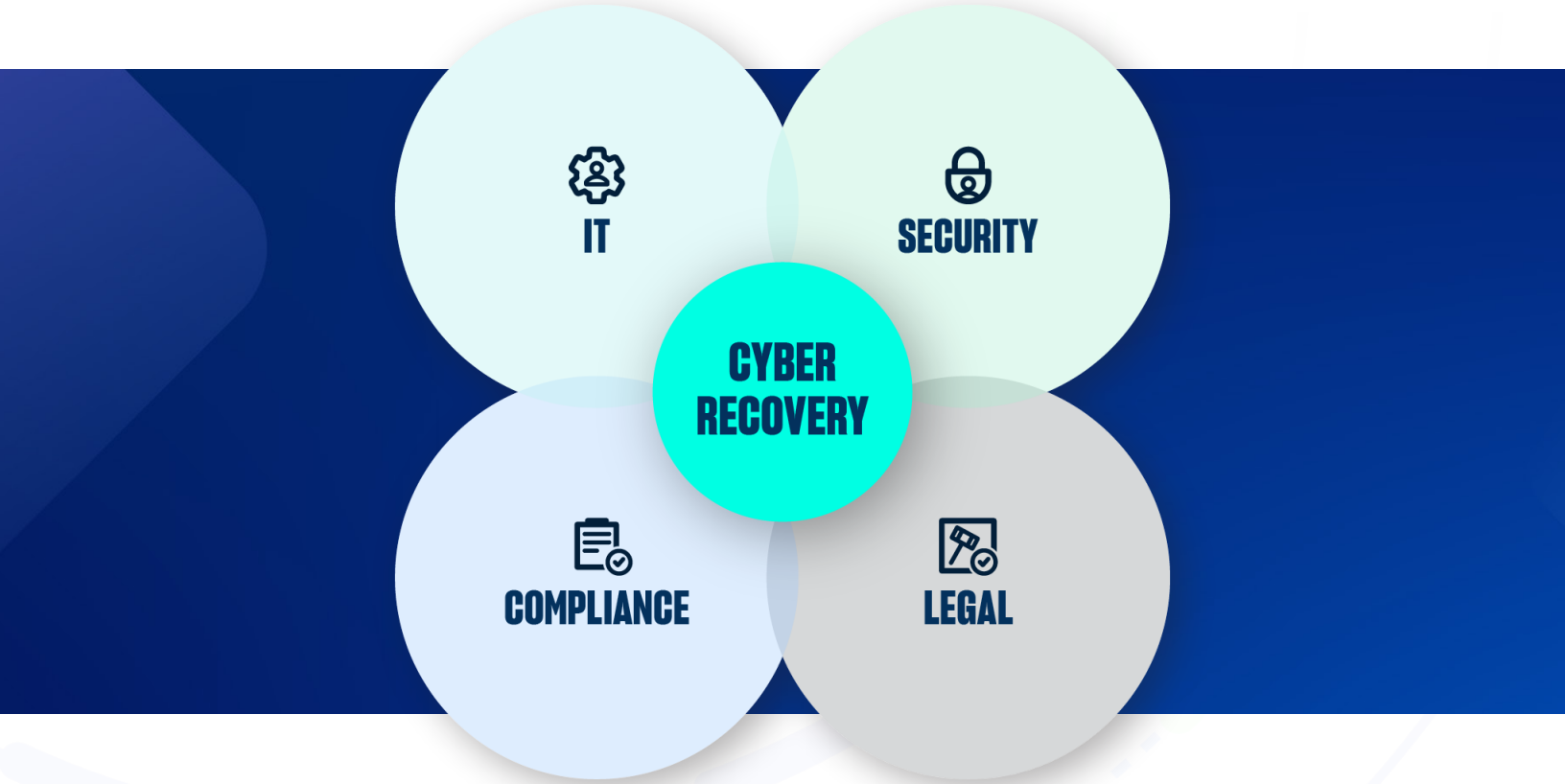
- You're calm and collected
- You're well-prepared to take decisive actions
- You bounce back
- You restore business continuity

That is the difference between disaster and resilience.

A successful cyber recovery means you can:

- Quickly pinpoint the affected systems
- Surgically restore operations and reduce reinfection risks
- Minimize downtime
- Maintain business continuity

But recovering from cyberattacks is hard because during the crisis, you'll face critical questions that sit across IT, Security, and Compliance teams.



Knowing where to find the answers quickly is essential for responding and recovering from an attack and bringing your organization back up and running. Your IT and security teams must come together to mitigate risks and minimize the impact, and your CSOs and CIOs must be armed to demonstrate cyber resilience to your board.

Measuring and Reducing the Impact of Cyberattacks

Cyber recovery demands a unique set of capabilities that go beyond traditional disaster or operational recovery methods.

While disaster recovery focuses on getting systems back online after an outage caused by a natural disaster or hardware failure, cyber recovery is about identifying attacks early and recovering from them quickly while ensuring that the attacker is not reintroduced into the environment.

Two key metrics that you can use to reduce the impact of cyberattacks are:

Clean Cyber RPO (Recovery Point Objective)

extends beyond traditional RPO that focuses solely on minimizing data loss. **This metric ensures recovery points are thoroughly validated, scanned for threats, and certified safe to restore.** This verification process is essential for achieving true cyber resilience, as it prevents the risk of reinfection that can occur when restoring from compromised backups, ultimately reducing extended downtime.

Cyber RTO (Recovery Time Objective)

defines the critical timeframe within which an organization must restore systems and data following a cyber attack. **This metric balances speed with security, focusing on maintaining data and system integrity throughout the recovery process.** Successful Cyber RTO implementation requires quick, decisive action for finding clean recovery points.

Cyber RTO is often lengthier than disaster RTO because the scene is often more chaotic and riddled with major uncertainties and questions about what just happened, who was behind it, what they did, and how to be sure they're completely out of the environment.

Here are a few challenges you might encounter that could slow down your recovery:

Impact Assessment

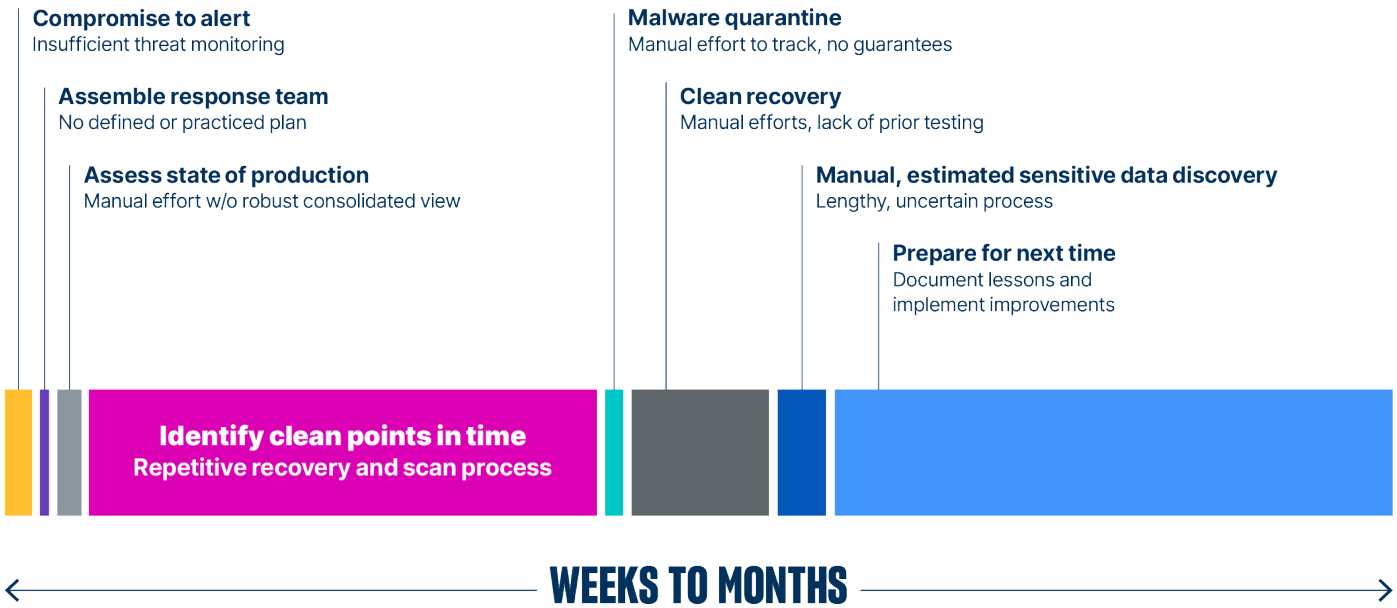
- You need to assess what's going on, where the attackers entered, whether or not they moved laterally, how long they've been in the environment, and which data was affected.

Stakeholder Collaboration

- You'll need to assemble the right team and get started on the response.

Recovery Operations

- You will have to decide if you just need to replace a couple of systems and applications or if you need to recover everything into a secondary recovery environment.
- If you don't know what was affected, you may need to restore everything to another recovery environment and wait to see if malware starts to spread again.
- If your actual recovery process isn't automated, you still may run into unknowns that can compromise your success or slow you down.



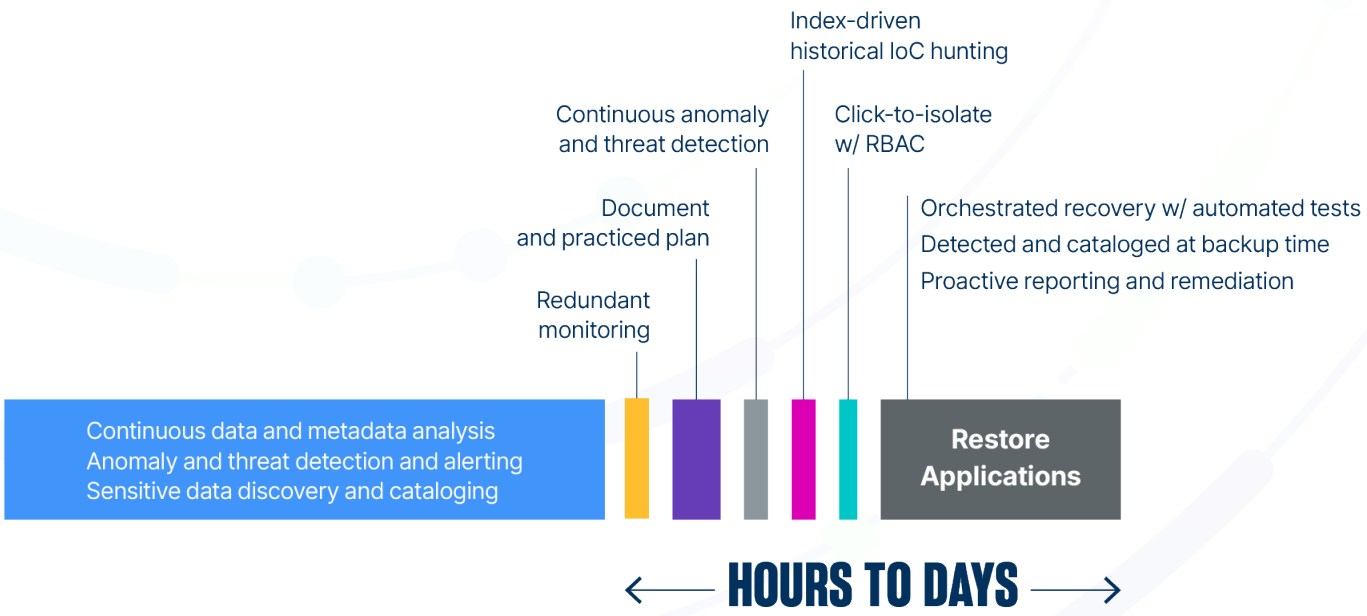
A slow, inefficient cyber recovery timeline

Building a Cyber Recovery Blueprint

Let's take a look at how you can create a blueprint that can be used in times of crisis.

Establish An Optimized Cyber Recovery Timeline

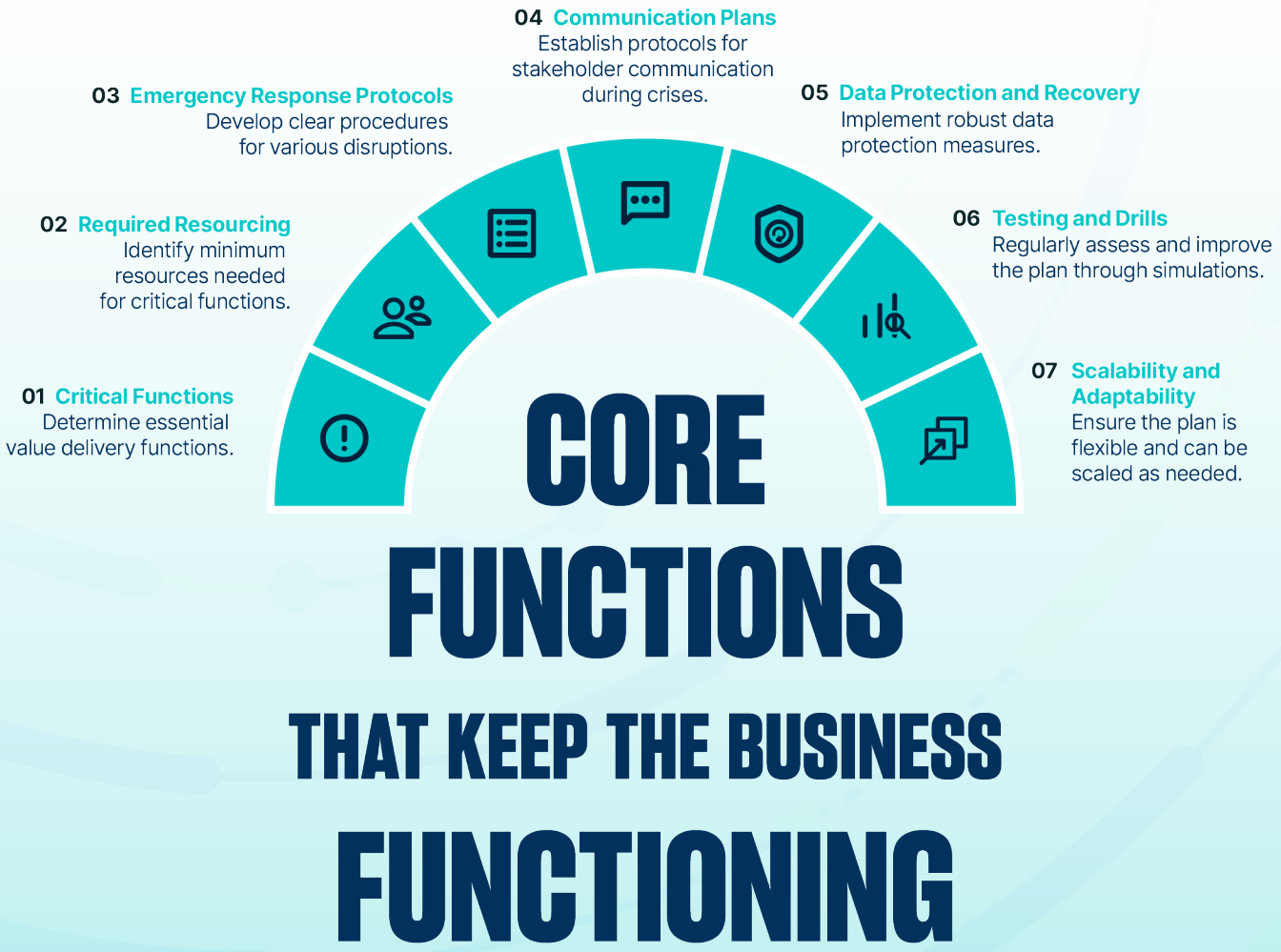
We've talked about what a confusing cyber recovery process can be like. But what if you could take your weeks- or months-long recovery down to just hours or days? To accomplish that, you'll need to define all the necessary steps required to restore systems and establish best practices with automation and collaboration.



An optimized cyber recovery timeline

Define Your Minimal Viable Business

An effective cyber recovery blueprint must prioritize the recovery of critical systems and data. This requires a clear understanding of your Minimum Viable Business (MVB)—the essential functions that must be restored first to maintain business continuity. By focusing on the MVB, you can make sure that you are directing resources towards the most important systems and data during the recovery process.

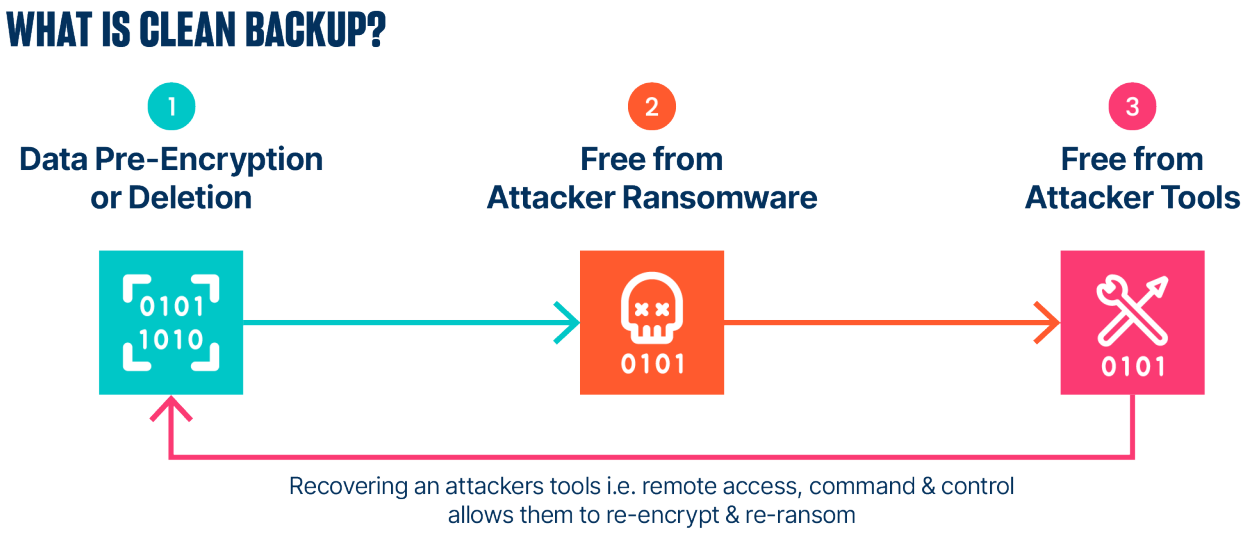


Find Your Clean Data

Finding clean data is the most obvious—but also most important—requirement for recovering from a cyberattack. But ironically, it's also the most challenging thing to do.

This is why having cyber-resilient backups is a critical element of every recovery plan.

First, you need to define what a clean backup is. Your most recent backup may not be clean, however. How do you know you're not reintroducing the attacker's malware, the attacker's back door, or their remote access tool?

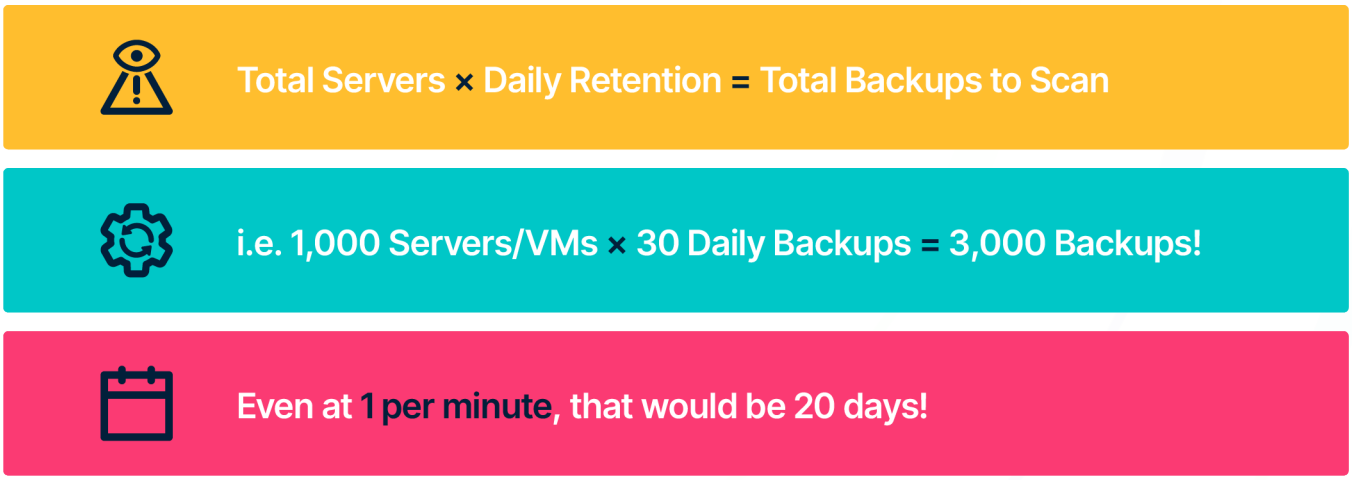


The 3 essentials of a clean backup

To find clean backups, you must be able to quickly identify indicators of compromise (IOCs) within your backup data. Many known malware families are defined by a unique HASH or YARA, so if you can't scan your backups for a HASH as well as YARA, you won't be able to find a clean recovery point.

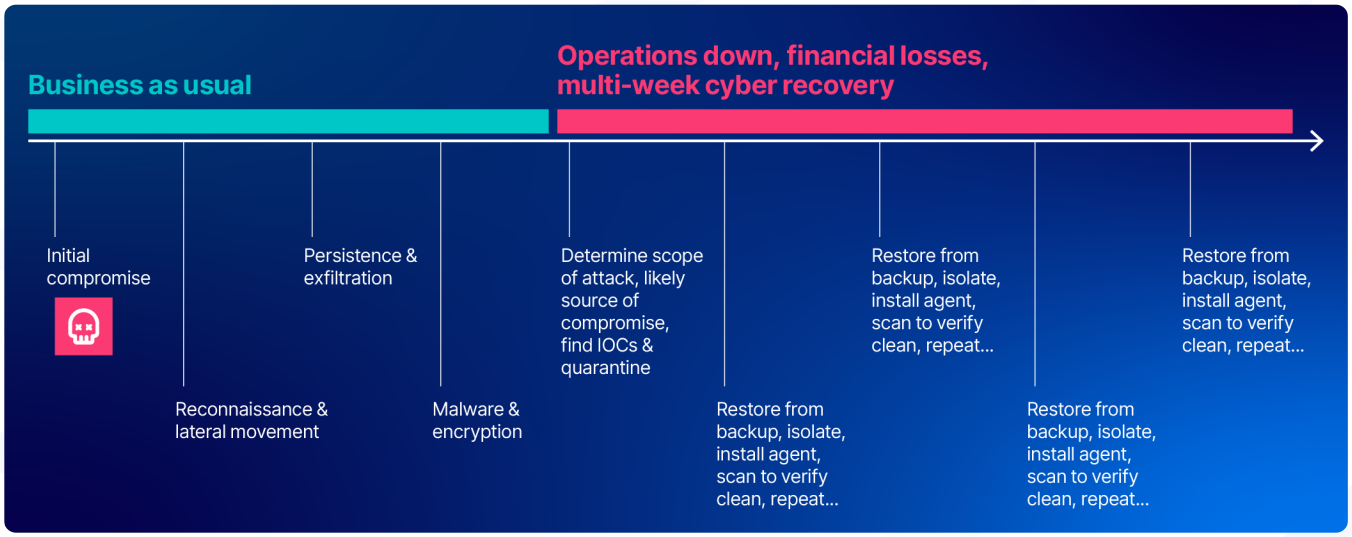
Beyond simply scanning backups, the next question you need to ask yourself is: How quickly can you scan them to find the most recent clean recovery point?

This presents a daunting challenge, as you need to rapidly scan thousands of backups across multiple systems.



Time to scan backups for IOCs

If you don't know whether you can rapidly scan your backups, you cannot truly communicate your cyber RTO to your stakeholders or your board, and you won't be confident in your cyber recovery plan.



The downside if you can't find clean data

This means if you can't find a clean recovery point, you'll experience prolonged disruption and uncertainty.

Once a clean backup has been identified, the focus shifts to recovering systems and data as quickly as possible. This requires a well-defined and tested recovery process that can be executed rapidly. Automation plays a key role in optimizing the recovery process, enabling you to restore systems and data at scale with minimal manual intervention. Regular testing and refinement of the recovery plan are also essential to ensure that it remains effective as the threat landscape evolves.

Building a Business Case

Cyber recovery requires collaboration and input from several stakeholders across the organization.

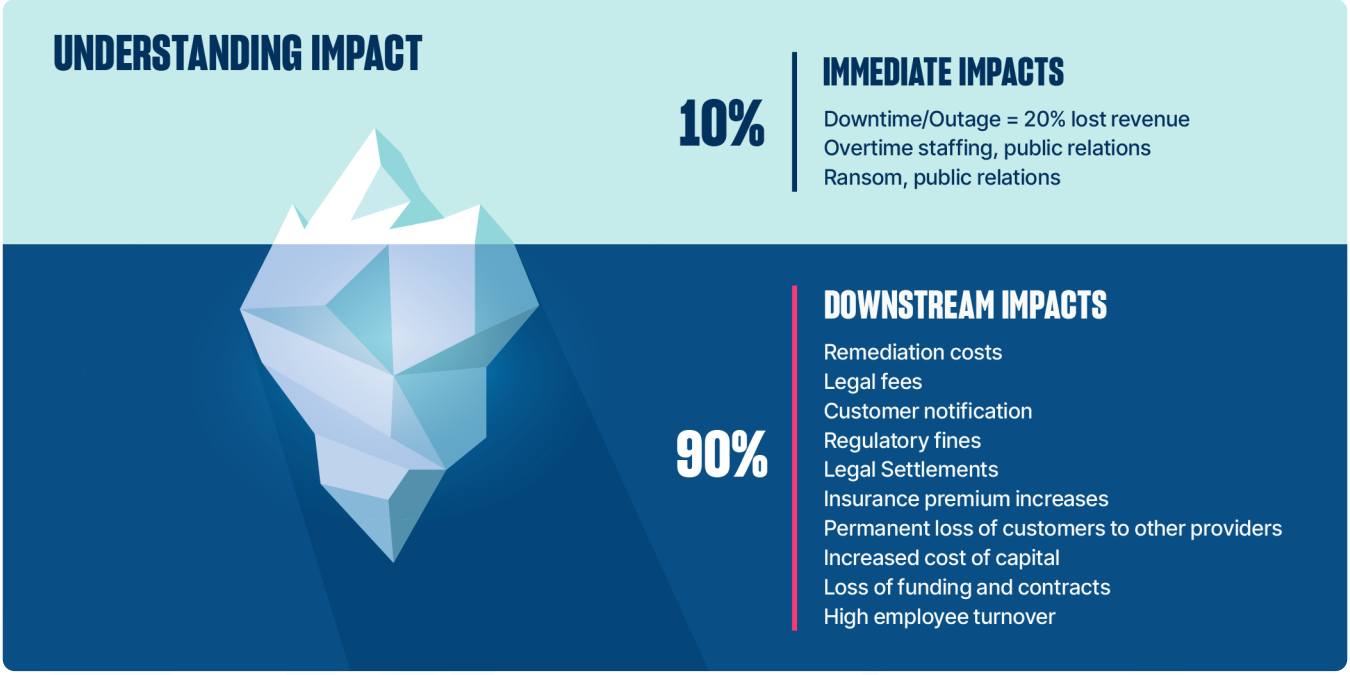
To secure executive buy-in and budget for a cyber recovery solution, your IT and security leaders must be able to articulate the potential impact of a cyber attack on your organization. This requires quantifying the financial, operational, and reputational risks associated with prolonged downtime and data loss.

You need to be explicit about the potential risks to business operations in terms of downtime and the cost associated with it. One approach is to calculate the average cost of downtime for your organization and multiply it by the expected duration of an outage in the absence of a robust cyber recovery solution. This can help to illustrate the potential financial impact of an attack and the value of investing in rapid recovery capabilities.

The average length of time for an outage by industry

The cost of downtime by industry

You also need to keep in mind that the impact of an attack may not happen all at once. While downtime and a damaged reputation might be priority concerns, communicating downstream effects—such as regulatory fines, lower quality service, legal settlements, higher cost of capital, and employee turnover—can affect your ability to bounce back in full. Communicating those concerns can go a long way in proving the risks associated with not investing in cyber recovery.



The immediate and long-term impacts of inefficient recovery and extended downtime

By framing cyber recovery as a strategic imperative rather than just an IT issue, leaders can build a compelling investment case.

What Now?

The threat of cyberattacks is not going away anytime soon. If you want to do more than just survive the next one, you must recognize that cyber recovery is not a one-time event but an ongoing process that requires continuous vigilance and optimization.

Don’t wait until it’s too late.

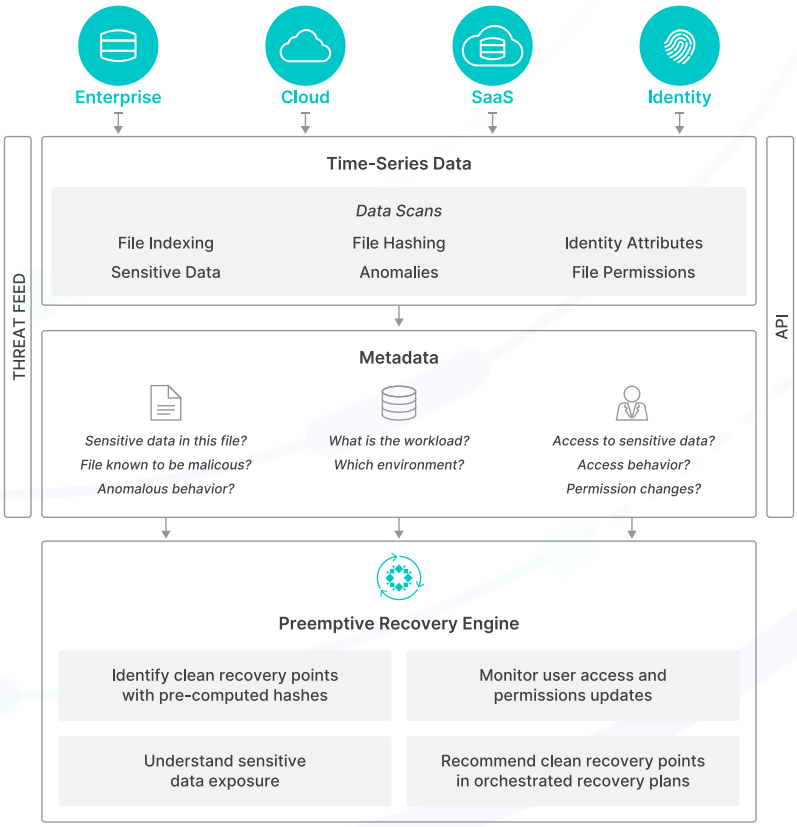
Talk to a Rubrik cyber resilience expert
to see how you can start building your own blueprint.

The Rubrik Approach to Cyber Recovery

Rubrik offers a comprehensive approach to cyber recovery that aligns with the key capabilities and features outlined in this ebook.

Data Protection
Rubrik protects your data from insider threats or ransomware with air-gapped, immutable, access-controlled backups.

Preemptive Recovery Engine
This engine performs the necessary prework to identify clean recovery points—before a cyberattack occurs.



Recovery Simulation
Improve your cyber readiness and incident response by creating, testing, and validating your cyber recovery plans in isolated environments.

Anomaly Detection

Assess the attack scope and impact by identifying the point of infection and quickly pinpointing infected applications.

Threat Monitoring

Proactively and continuously scan backups for the presence of IOCs based on intelligence from Google Mandiant and Rubrik Zero Labs.

Threat Hunting

Scan thousands of backups in seconds across all environments, checking against precomputed hash rather than relying on time-consuming file-by-file scans.

Threat Containment

Isolate infected snapshots and reduce the recovery risk of reintroducing the malware into the environment during a recovery operation.

Recovery Orchestration

Execute pre-validated recovery plans with the necessary resource mapping for a clean, rapid, and reliable recovery—prioritizing critical applications first to minimize disruption

Incident Response Support and Artificial Intelligence

Rubrik Ransomware Response team and Ruby AI companion provide you with the support, guidance, and expertise in turning a cyber crisis into your finest resilience story.

One Platform, Complete Response

Rather than navigating 4-7 different tools during a crisis, Rubrik delivers the entire recovery journey in one unified workflow—eliminating handoffs that waste critical response time. Detection of anomalies can trigger threat hunting from the same interface, allowing for the pinpointing of infected systems, quarantining of malware, and identification of clean recovery points—creating a continuous response flow.

rubrik

Global HQ
3495 Deer Creek Road
Palo Alto, CA 94304
United States

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

ebk-your-cyber-recovery-blueprint / 20250919