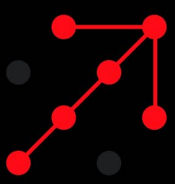
PREDATAR

Recovery Assurance Buyer's Guide.



© Copyright | Predatar Ltd | 2025 | Publication or distribution of this document without permission from Predatar is not allowed

Welcome to the Recovery Assurance Buyer's Guide.

Contents

01
An introduction to Recovery Assurance

What is Recovery Assurance?
First things first: Before we look at the important questions you should be thinking about when evaluating the right Recovery Assurance solution for your organisation, let's start by clarifying the term 'Recovery Assurance.' After all, it's a relatively new concept.

Every organisation has data. Lots of it. And it's vital for day-to-day operations. If your data can't be accessed, everything stops. Critical applications won't run, production lines will halt, teams will be unable to communicate, customers won't be able to place orders. The longer the downtime, the greater the negative impacts will be.

75% of organisations reported that it took more than 100 days to fully recover from a data breach.[1]

1. The Cost of a Data Breach Report 2024. IBM

It's a shocking reality that recovery from a cyberattack typically takes more than 100 days. All too often, when organisations turn to their backups and snapshots to begin their recovery, they discover they have been infected, encrypted, or even deleted as part of the attack.

Put simply, Recovery Assurance is the process of proving your ability to recover from a cyberattack or other data loss event. So, if the worst happens — you're ready to mount a fast and effective recovery without the risk of recovery failure or reinfection.

What isn't Recovery Assurance?

Data resilience is a hot topic right now, and there are lots of emerging technologies (and some well-established ones too) that can help you achieve it.

Frankly, the more defensive layers you have in place, the better. We advocate all of the following approaches as part of a multi-layered approach to resiliency. In many cases these 'resiliency fundamentals' will play a role in the Recovery Assurance solution you choose — but they won't prove your ability to recover quickly, cleanly and completely. Therefore, these fundamentals alone do not provide Recovery Assurance.

3-2-1 methodology

This is a fundamental principle of storage best-practice. Having 3 copies of your data, on 2 different media types, with one stored offsite is strong foundational methodology for protecting your data. However, it is possible for undetected malware to be replicated across your multiple repositories.

While the likelihood of data encryption or deletion across all of your data copies is significantly reduced by this approach, it is not impossible, and the risk of reinfection of production systems remains a possibility.

Immutable Storage (including Immutable Vaults and Immutable Snapshots):

Immutable storage means that once a file has been written it can't be altered. In theory, this means that if a hacker tampers with your production data, your immutable backup/snapshot will remain untouched and recoverable.

While this is true, there is a common scenario where dormant malware has been replicated into the backup or snapshot. In this instance, restoring from the immutable copy will lead to reinfection of your production systems. Simply having an immutable copy does not guarantee clean, successful recovery.

Manual Disaster Recovery Testing (aka DR testing)

Many organisations have DR testing procedures in place. But the reality is, these processes are ineffective in the context of cyber threats. Often, they were designed to validate an organisation's ability to recover from a data loss event such as a natural disaster or data centre failure. Therefore, there are generally no steps in place to identify malicious files within the data.

What's more, because DR testing tends to be a largely manual and time-consuming process, typically organisations will test less than 1% of their backups annually. So, this approach will not validate the vast majority of data that an organisation will need to call on for a complete recovery.

Anomaly detection

Most modern storage technology includes built-in anomaly detection. This is designed to spot unusual and suspicious behaviour in stored data, which can be an early warning sign of an active cyber-attack.

While useful for raising the alarm, anomaly detection is reactive rather than proactive — It can only detect a cyber-attack once it's in progress. Furthermore, anomaly detection alone is unable to validate if the anomalous behaviour is the result of malicious activity and is commonly prone to generating false positives.

Typically, organisations recovery-test less than 1% of their data each year. [2]

2. Based on proprietary research from data monitored by Predatar across more than an exabyte of enterprise backup data.

02
Assessing Your Need

It's important to acknowledge that every organisation that relies on data is a potential target for cybercrime. As such, almost any organisation can benefit from Recovery Assurance.

Proactively proving your ability to recover before a crisis hits is always a good idea, but there are several factors that provide additional compelling reasons to implement a Recovery Assurance solution.

– Are you in a high-risk industry sector?

Cybercriminals are not random or indiscriminate when it comes to targeting their attacks. While no organisation is safe, some are at a higher risk of attack than others. If your organisation operates in a particularly high-risk sector, your need for Recovery Assurance is heightened.

– Do you manage critical infrastructure and services?

Downtime for any organisation will have negative impacts, but in some industry sectors, the inability to deliver services could seriously impact people's health, wellbeing and in some cases could even put lives at risk. It is important that organisations such as healthcare providers, utility providers, and emergency services do everything they can to minimise the impact of a cyberattack for the people that rely on their services. This includes implementing Recovery Assurance.

Top ten most attacked industry sectors: [3]

01	Manufacturing
02	Finance and Insurance
03	Professional, business and consumer services
04	Energy
05	Retail & Wholesale
06	Healthcare
07	Government
08	Transport
09	Education
10	Media and telecomms

3. Distribution of cyberattacks across worldwide industry sectors, 2023. Statista.

– Are you in a regulated industry sector?

Increasingly, industry regulators are stipulating that organisations must be able to demonstrate their ability to recover from a cyber incident. Regulators in the European Union (EU) have led the way with the Digital Operational Resilience Act (DORA), which applies to Financial Services organisations, and the Network and Information Security Directive 2 (NIS2) for organisations considered to be 'critical' to the function and security of the EU.

> ***An Extract from NIS2.***
> **Proof of Resilience:** Organizations are expected to demonstrate the effectiveness of their data recovery strategies to relevant regulatory bodies, especially following a significant incident. Proof may include evidence of testing, compliance documentation, and records showing timely restoration of services and data integrity.

Recovery Assurance can help organisations achieve compliance without additional burden on overstretched teams.

Other countries and industry sectors are following suit with a raft of regulations coming into force including FISMA in the US and PSA in the United Kingdom.

– Do you have Information Security Accreditations?

Leading standards bodies around the world are increasingly incorporating requirements relating to regular validation of successful data recovery into certification programs.

ISO 27001, the world's leading standard for Information Security Managament states that organisations must perform ***'regular testing of data recovery'***, ***'simulate recovery scenarios,'*** and provide ***'evidence of successful recovery.'***

Recovery Assurance technology can meet these requirements without additional burden on storage administrators.

– Do you have customers, employees, business partners, suppliers, and/or shareholders?

Well, of course you do. So, this is just another reminder that almost any business can benefit from Recovery Assurance.

If your digital systems go down and you are unable to restore them for days – or even weeks, ***everyone*** that interacts with your business will be affected.

Recovery Assurance will help you recover fast and minimise impact for:

> ***Your customers:*** Make sure they can access your online services, place orders and contact customer support.

> ***Your suppliers:*** Keep your supply chain moving. Make sure you can track your orders, place new ones, and pay your invoices.

> ***Your employees***: Get HR and payroll systems up and running fast to avoid significant impacts on your team (not to mention potential legal implications).

Any organisation that wants to mitigate the risks of lost revenue, lost trust and reputational damage should consider implementing a Recovery Assurance solution.

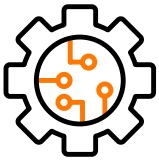
If your digital systems go down, everyone that interacts with your business will be affected.

03
What are the components of a Recovery Assurance solution?

Comprehensive Recovery Assurance is a multi-layered process which brings together multiple technologies to provide users with confidence in their ability to recover systems quickly, cleanly, and completely. Technologies that make up a complete Recovery Assurance solution include:

1 | Threat detection (software)
Look for advanced threat detection that goes beyond basic anomaly detection. Threat detection with ML (Machine learning) or AI (Artificial Intelligence) capabilities provides greatly enhanced detection with fewer false positives.

2 | Anti-virus, EDR/XDR (software)
Not all EDR tools are created equal. Your Recovery Assurance solution should include industry-leading EDR/XDR to ensure maximum protection. The Gartner EDR Magic quadrant is a good reference resource. You should also look for Recovery Assurance technology that incorporates multiple EDR/XDR tools, as one tool may identify a virus that another one has missed.



3 | Integrations (software)
Most modern storage environments include multiple software products across primary and backup environments, not to mention the software in the cyber security stack.

To avoid adding additional complexity, look for a Recovery Assurance solution that works natively with all of the core storage software tools you are using in your organisation.

Integration with your SIEM platform will also help to improve visibility and collaboration between IT and data security teams.

4 | Analytics Dashboard (software)

A great dashboard can turn data into valuable insight, and the UI (User Interface) can make or break any technology solution. Look for a Recovery Assurance solution that helps key stakeholders in your organisation understand the overall cyber resilience posture, and helps you cut through the noise of data complexity to see what really matters.

5 | Automation (software)

Without automation, Recovery Assurance would be almost impossible to manage. To manually undertake the multiple processes required to prove the ability to recover data effectively in a continually evolving data estate, with new threats emerging every day, would require a small army of dedicated technicians. Automation is essential for Recovery Assurance.

6 | Recovery target (hardware)

On-premise, or in the Cloud — an Isolated Recovery Environment (or CleanRoom™) is a critical component for Recovery Assurance. It's a safe and segregated location where processes such as recovery tests and anti-virus scanning can be performed without affecting the performance of your production systems or risking infecting them.

04
Options and Buying Considerations

When it comes to choosing the right Recovery Assurance solution for your business there's lots of options to consider. This section will help you understand the differences and evalute which options are best for you.

Build-Your-Own *vs.* Out-Of-The-Box

As with most technology, it is likely that the only way to achieve a solution that meets 100% of your criteria is to design and build a solution, but of course there are obstacles and important considerations to think about. For example, cost, time, and complexity.

For most organisations, it's possible to meet the vast majority of requirements with an off-the-shelf solution.

Building even a basic Recovery Assurance solution from the ground up will involve many highly specialised skillsets for tasks such as:

- configuration of a hardened recovery environment
- procuring additional licenses for multiple security and storage tools.
- leveraging open and custom APIs to connect those security and storage tools,
- precuring additional licenses for the security and storage tools you are using,
- leveraging automation tools such as Ansible.
- And more

For most organisations it will be possible to meet the vast majority of their requirements with an off-the-shelf solution, which can be deployed in a matter of hours — with the additional advantage of customer support to help with any technical issues.

Manual *vs.* Semi-Automated *vs.* Fully Automated

We've already established that manual Recovery Assurance isn't practical due to the extensive human resources that would be required to continually validate the cleanliness and recoverability of data across a large and constantly evolving storage estate.

A fully automated solution can eliminate the need for manual intervention.

Many Recovery Assurance solutions on the market today are semi-automated. They may flag potential problems and move suspect workloads to an isolated environment, where processes such as anti-virus scanning, recovery testing and deeper forensic analysis can be manually executed using third-party tools.

Once configured, a fully automated solution can eliminate the need for a manual intervention while keeping users informed with notifications in real time.

Storage Vendor Add-Ons *vs* Third-Party Solutions

Most backup and storage vendors offer enhanced capabilities to boost data resiliency as an add-on to their core products. If you choose to implement a solution from your existing storage vendor there are some clear advantages including ease of procurement and confidence that the solution will work effectively with your existing storage technology.

On the downside, if your storage environment includes multiple technologies from different vendors, a solution from one vendor won't cover the other technologies in your stack. To boost resiliency across your whole environment, you'll need multiple solutions, which can quickly become costly and complicated. A third-party solution, like Predatar can provide Recovery Assurance across multi-vendor storage environments.

Proactive *vs.* Reactive

Most Recovery Assurance solutions are reactive. They come into play when there is evidence of a cyberattack in progress. Whether this is an early warning alert from anomaly detection capabilities in your backup software, or a full-scale crisis is already happening — the fact is — the attack is underway. With a reactive solution, you will then begin testing and cleansing workloads, so you are ready to recover them to your production environment should you need to.

Most Recovery Assurance solutions are reactive. They come into play when there is evidence of a cyberattack in progress.

A proactive solution takes a preemptive approach. By continually validating the cleanliness and recoverability of your data across your storage environment (regardless of whether threats have been detected) — and resolving any issues as they are found — you will have a significantly increased likelihood of a fast, successful recovery.

On-Premise *vs.* In The Cloud

Running the processes associated with Recovery Assurance requires compute, and a recovery target. So, you've got a choice. You can run your Recovery Assurance in the Cloud or on-premise. There is no right or wrong answer here. One top tip is to deploy your Recovery Assurance solution alongside the data you'll be validating.

Why? Let us explain. If your backups are on premise, but your Recovery Assurance environment is in the cloud, there would be a need to continually push large quantities of data to and from the Cloud for testing. This would not only limit the speed and efficiency of your validation, but could also incur large Ingress and/or egress fees from your Cloud provider.

Buy It *vs.* Subscription *vs.* Managed Service

For most organisations subscription-based licences have replaced perpetual licencing as the de facto way to licence technology. The main advantages of subscription include the ability to scale up or down easily, and a simplified procurement process without the need for approval of significant CapEx costs.

For organisations with limited IT and security resources, Recovery Assurance delivered as a service is an option worth considering. Backup as a Service (BaaS) has been commonplace for many years, and today some specialist BaaS providers have evolved their offerings to include Recovery Assurance services too.

A full list of Predatar-approved Recovery Assurance service providers around the world is available here.

Typically, a Recovery Assurance service provider will take responsibility for identifying recovery risks in your storage environment (including hidden malware), investigating those risks, and undertaking remedial actions to maintain the integrity and recoverability of your data.

05
Conclusion

Recovery Assurance technology is quickly becoming an essential component for any organisation that understands the risks of cybercrime, and acknowledges that defensive cybersecurity is not infallible.

There are many ways to achieve Recovery Assurance, from fully bespoke solutions to flexible out-of-the-box products that are quick to deploy, provide comprehensive functionality, and start delivering tangible value within days.

To take your first steps towards recovery confidence, you can speak to one of our Recovery Assurance expert partners, or visit www.predatar.com to learn more.

Discover the most comprehensive Recovery Assurance platform available today.

Proactive:
AI-powered automation for always-on data validation.

Unified:
Works with multiple leading backup and storage technologies.

Fast:
Can be deployed in hours. Starts to deliver value in days.

Learn more at Predatar.com