aws | COHESITY

GUIDE

Ransomware Readiness: An In-Depth Evaluation Guide

Strengthen your data security
& cyber resiliency

Contents

The evolution of ransomware	3
Critical actions countering ransomware	3
Ransomware isn't going away	4
Protect your backup data and system	4
Reduce the risk of unauthorized access	7
See and detect attacks to stop encroachment	8
Strengthen your security posture with platform extensibility	10
Ensure you can rapidly recover data at scale	11
Checklist: ransomware readiness evaluation	13

The evolution of ransomware

Cybercriminals are becoming more sophisticated in their attacks against the data that powers your business. How successful they'll be at extorting ransom depends on what you do today to fortify your environment and improve your ability to respond should an attack occur.

Ransomware threats are evolving. Targets and tactics are expanding. If it hasn't happened already, soon you'll be asked how you're countering the various ways in which cybercriminals are aiming to disrupt your operations.

	Ransomware 1.0	Ransomware 2.0	Ransomware 3.0
Malware target	Production data	• Backup data • Backup systems • Production data	• Backup data • Backup systems • Production data • Data to illegally remove
Method of attack	Encryption	Encryption	Encryption and exfiltration
How companies are countering the attack	Backup & recovery system	Immutable backups and data isolation	Early detection and continuous monitoring

Critical actions countering ransomware

If you're unsure what to do first to strengthen your organization's cyber resiliency, this guide is for you. It's full of practical information and evaluation criteria about what to look for in a data management solution to bolster your data security strategy. You can also use it to complement the tools your SecOps team uses as you work together on how best to respond to ever-changing ransomware threats. This guide also features a checklist to reference as you compare the effectiveness of your existing solutions against next-gen data management solutions.

Better protecting your data and your company's reputation starts by understanding how these five critical actions empower your organization to counter ransomware:

- Protect your backup data and system
- Reduce the risk of unauthorized access
- See and detect attacks to stop encroachment
- Strengthen your security posture with integrations and APIs
- Ensure you can rapidly recover data at scale

Ransomware isn't going away

1,070%

The percent ransomware grew between July 2020 and June of 2021[1]

82%

The percent average ransomware payments climbed since 2020 to a record $570,000 in the first half of 2021[2]

>$1.85 M

The average cost to rectify ransomware attack impacts without paying the ransom[3]

>$265 B

The amount global ransomware damage costs—lost revenue and productivity as well as rebuilding—are predicted to exceed by 2031[4]

aws

Protect your backup data and system

Data safeguards are fundamental to preserving customer trust and keeping your competitive edge. They counter evolving ransomware threats, including new ones such as "Lockers" that completely shut you out of your system files and applications while showing you a countdown clock to an expected ransom payment date and time. Without improving your safeguards, your business has no way of protecting your data from being encrypted—or worse, stolen—by cybercriminals.

For optimal data resiliency across hybrid and multicloud environments, be sure these six non-negotiable backup security capabilities are part of any data management solution you're seriously considering.

Immutable snapshots

Software-based, native immutable backup snapshots effectively throw up a wall against ransomware attacks because they can't be encrypted, modified or deleted—all common tactics cybercriminals use to force a ransomware payment. This is extremely important for protecting the authenticity of data, particularly massive amounts of unstructured data such as audio and video files as well as images required in certain industries such as law enforcement and healthcare.

Unlike hardware-based immutability, the native read-only snapshots housed onsite or in clouds are never exposed nor mounted externally to any application; they can't be tampered with, altered or removed. That makes it hard for malware to target your backup data.

[1] FortiGuard Labs. "Global Threat Landscape Report," August 2021.
[2] Palo Alto Networks. "Extortion Payments Hit New Records as Ransomware Crisis Intensifies," August 9, 2021.
[3] Sophos. "The State of Ransomware 2021," 2021.
[4] Cybersecurity Ventures. "Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031," June 3, 2021.

WORM

Mechanisms such as write once, read many (WORM) technology provide another layer of protection against a ransomware attack. They allow teams to create and apply a time-bound lock on data through policies and then assign them to selected jobs to enhance immutability for protected data. As this is a protection that neither security officers nor security admins can modify or delete, you don't have to worry as much about potential insider threats.

Data encryption

There's encryption and then there's software-based FIPS-validated, AES-256 standard encryption for data in flight and at rest. You want the cryptographic module validated by the United States National Institute of Standards and Technology (NIST) at the Federal Information Processing Standards (FIPS) 140-2 Level 1 standard. FIPS 140-2 is a U.S. government standard for cryptographic modules providing assurances that the module design and implementation of cryptographic algorithms are secure and correct. FIPS validated encryption is more secure because products with this distinction pass a rigorous set of tests to be certified to the extent that this has become valued globally.

Configuration audit and scanning

Your IT team is likely now operating many different systems and tools—all with their own set ups, policies and management interfaces. The manual processes to run them often introduce avoidable human error. Wouldn't it be nice if there was a more efficient way? An automated system with guided scanning that audits various data security and access control settings helps you avoid costly human mistakes while simplifying your data operations from set up to policies to management processes.

Fault tolerance

Because data resilience should always be a guiding security principle, you also need a fault-tolerant system that helps ensure data integrity and successful backups even in the harshest conditions. Some of those are when your systems are near full compute, memory or storage capacity; when you have considerable network congestion; or when you unexpectedly experience a hardware failure. Look for a solution built with fault tolerance that allows backups to continue in spite of a failed component/node.

Modern and flexible data isolation

A companion consideration as you modernize your data management approach is updating your data isolation strategy. Traditionally, organizations have relied on tapes to maintain air gapped copies, but that method can no longer keep up with today's demanding service-level agreements (SLAs) when it comes to recovery times—particularly those experienced during a widespread ransomware attack. Despite the term "air gap" protection now being widely misused to describe techniques that do not maintain an actual gap, don't be misled. Be sure your next data management solution offers both real air gap protection as well as modern options to achieve data isolation. These balance modern recovery time objective and recovery point objective (RTO/ RPO) requirements with appropriate security controls by storing backup data in the cloud or at another location with a temporary and highly secure connection. You then get a tamper-resistant environment, preventing ransomware and insider threat disruption while optimizing for meeting your organizational SLAs. Best of all, you always retain a copy of your data in an immutable format.

Top 4 questions to ask about backup data and systems

- What does your data management solution do to protect your backup data against ransomware attacks?
- How does your solution continuously back up workloads even after the failure of a hardware or software component?
- How does your solution balance needs for stronger security with ever-faster digital business RTOs/RPOs that meet SLAs?
- In what ways does your solution provide visibility into the security gaps in the system configuration and operational design?

Reduce the risk of unauthorized access

Bad actors are working for themselves, syndicates and nation states. That's why it's an increasingly strategic move for your business to have a data management solution with strict access controls. These capabilities can more effectively stop unauthorized access from external hackers or rogue internal professionals taking advantage of compromised credentials.

To lower your risk of data theft and loss, look for a solution that builds in the principles of least privilege and segregation of duties with granular security—including the following four must-have capabilities. They keep your data safe and your customers confident.

Multi-factor authentication

Regularly compromised, even the most creative passwords can provide only a minimum layer of security protection for digital businesses. Multi-factor authentication (MFA) is a step forward in mitigating against phishing schemes and other password hacks. It requires everyone accessing your backup or data management solution to undergo a multi-step verification requirement process. They must authenticate—with both something they "know" (e.g., a password) and something they "have" (e.g., a thumbprint validated by a single sign-on [SSO] provider) to prove they are who they say they are. Insist any of your short-listed solutions require MFA.

Monitored modification

Because someone watching can be enough to thwart an attack, you will want a capability that prevents one compromised credential or individual from modifying critical elements of your data management solution. Insist on having a platform that helps enforce safeguards, for example, requiring a root-level or any other critical system change to be authorized by more than one person so you can protect against malicious intent and stolen credentials.

Granular role-based access control

When it comes to data, effective management of identity and access are increasingly the cornerstones of good cyber hygiene. Reducing ransomware and insider threats now depends on IT staff granting each person a minimum level of access to all of the organization's data needed to do a particular job and at the same time spreading critical data processes and functions across IT roles so no single administrator can compromise your whole business. Organizations with data management solutions that simplify approaches to granular role-based access control (RBAC) do a better job of thwarting unauthorized access and risking data while efficiently granting their users appropriate privileges to do their work.

Top 3

questions to ask about reducing risk of unauthorized access

- What does your backup or data management solution do to prevent unauthorized access to business data?
- How does your solution protect against both ransomware and the insider threat?
- How do I set up multi-user approval for critical operations?

See and detect attacks to stop encroachment

Digital business moves fast. Business owners increasingly need to know what sensitive data they have, where it's located and who has access to it. This is key to complying with industry or government regulations, maintaining trust and rapidly responding to double-extortion (a.k.a. data exfiltration) attacks.

To minimize the potential impact of ransomware, look for a data management solution with intelligence baked in so you can automatically discover and classify sensitive data while enjoying near real time threat detection. Find a solution that helps your team work smarter, not harder, and includes four critical capabilities for proactive response—no matter what threats come your way.

Artificial intelligence/machine learning powered

Your organization needs data to thrive. But that data is exponentially increasing, making it impossible for some data management solutions to perform effective pattern matching and data classification so you know what matters most. In contrast, a next-gen data management solution powered by artificial intelligence and machine learning (AI/ML) assists your organization to more accurately detect variations and reduce false positives without adding staff. You can take advantage of AI/ML techniques to match to "known good" sets of data and do that more effectively and efficiently as your "known sensitive data" is matched and fed back to the AI/ML algorithm. Think of it this way, you want to find the needle in the haystack without a lot of heavy hay-bale lifting.

Anomaly detection in near real time

The faster you find an intrusion, the less damage it can do to your business—and the fewer nights and weekends you burden your IT pros. Powerful automated anomaly detection in near real time as part of a data management solution continually tracks normal system operations to quickly spot irregularities and abnormal user behaviors that can signify a ransomware attack. Coupled with alerting, these capabilities don't just signal potential danger but can also initiate remediation. With anomaly detection in near real time, you enjoy fast discovery of both encryption-style and data exfiltration attacks in progress and that helps you minimize ransomware's impact.

Automated alerts

Just because it's fast and simple, doesn't mean there isn't complex operational power behind data management alerting. Find a solution with both anti-ransomware and risk-driven, predictive analytics-based alerts. The first informs you not only that data was accessed, but what that data contained and where it was located; the latter helps you identify suspicious user behaviors that warrant further investigation such as who accessed sensitive data, when, and what they did with it.

Cyber vulnerability discovery

Cybercriminals are known to exploit software and cyber vulnerabilities—often left open due to unpatched software—to gain access to your production environment. The most effective backup and data management solutions should help your team gain visibility into those vulnerabilities. It should also help you proactively address them as well as avoid reinjecting already addressed cyber vulnerabilities back into your production environment while recovering from an attack.

Top 4

questions to ask to help stop encroachment

- How does your solution help classify data and identify sensitive information that may be at risk?
- What does your backup or data management solution do to provide deep visibility to help identify software and cyber vulnerabilities, and offer near real time anomaly detection?
- How does your solution incorporate AI/ML to detect anomalies that can signify a threat or a ransomware attack?
- How does your solution detect system-level and user behavior anomalies that indicate different attack vectors?

Strengthen your security posture with platform extensibility

Ransomware isn't a single threat. It's evolving and becoming more sophisticated with every iteration. That means your data management solution cannot be inflexible nor work in isolation; it needs to be future-proof and extensible. Integrated and interoperable solutions empower your organization to detect, investigate and confidently respond to threats faster. They're also the most likely to defeat bad actors.

Look for a modern data management solution that supports third-party collaboration to enhance your data security; one that ensures flexibility yet provides secure ways to simplify operations and make your data productive. To build a strong security posture, any solution you consider should include these three must-have capabilities and play nicely with others.

Pre-built integrations

Data security concerns keep business leaders up at night. They could sleep better if they had confidence their trusted security products were working seamlessly together to fight cybercrime. Find a data management solution that's already tightly integrated with leading security orchestration, automation and response (SOAR) as well as security information event management (SIEM) solutions. It will accelerate time to discovery, investigation and remediation of ransomware attacks. And be sure it also has pre-built, integrated workflows that are extensible, enabling SecOps to augment them for automated incident response and unified operations across security, IT and networking teams.

Customizable integrations

Change is constant. But not all data management platforms help you keep up with it. Your organization needs a cyber resilient solution that works to counter ransomware while also addressing unique business requirements. Make sure in addition to pre-built integrations that the solution you select has a secure software development kit (SDK) and customizable management APIs that give you the flexibility to operate your environment the way you want.

Value-added applications interoperability

In addition to pre-built and customizable integrations within an API-rich architecture that helps streamline operations, you need a platform that offers ways to future-proof while enhancing data security. Instead of making copies of data and moving them around, find a solution that allows you to reuse the data in-place by bringing value-add applications to data for routine and more challenging tasks—from virus scanning and data masking to analyzing file audit logs and classifying data. An extensible platform will help reduce your data footprint and attack surface as well as empower you to derive more value from your investments.

Ensure you can rapidly recover data at scale

Should the worst-case scenario happen and ransomware find a way into your production environment, you need a solution that gives you the power to refuse to pay ransom. Look for a solution with these three nonnegotiable data recovery capabilities to give you that confidence.

Instant recovery at scale

If ransomware attackers strike, they aren't targeting one or two virtual machines (VMs) or databases anymore. Rather, they want to lock up as much of your data in systems as possible. That's why organizations today need a data management solution that can quickly recover hundreds of systems. An instant recovery at scale capability allows you to rapidly restore hundreds of VMs, large databases or large volumes of unstructured data instantly, at scale, to any point in time and location.

Top 4 questions to ask to ensure extensibility and interoperability

- What security integrations does your backup or data management solution support?
- How does your solution work with other leading security products and platforms?
- How does your solution extract insights while keeping data safe?
- How does your backup or data management solution improve team collaboration by eliminating platform, people and process silos?

Clean recovery

In the process of a restore, you need to know the data you are using to recover quickly is also free from potential malware. Your data management solution should help you identify compromised snapshots. Find a solution with a built-in machine learning (ML) engine to recommend the last known clean copy so you know when you perform the restore that the snapshot data is free from anomalies and potential cybersecurity threats. This will accelerate your recovery time and give you the confidence that you're not reinjecting potential malware back into your production environment.

In-place recovery

Provisioning a clean environment after an attack can take time, and restoring to the original environment could compromise forensics efforts. This can slow down your recovery efforts (something you definitely don't want when you're working hard to get back to business). Find a data management solution that allows you to recover data directly in-place on the same platform—without spinning up a new server or database. It will save you time and money.

Top 4 questions to confirm you can rapidly recover at scale

- What does your backup or data management solution do to help you rapidly, cleanly and predictably recover data at scale?
- Does your backup system have sufficient resources to support rapid recovery to any point in time and to any location?
- What capabilities does your solution support to assess a snapshot's health and recover unstructured data without additional investment?
- How does your data management solution perform in-place recovery of unstructured data to reduce downtime?

Checklist: ransomware readiness evaluation

Cybercriminals are hard at work. You need a data management and data security strategy that can help you keep up with evolving threats and minimize the impact of ransomware. Rethinking your data management solution is a good place to start. As you evaluate your options, this checklist of key capabilities can help you zero in on the best-fit solution for your organization.

Action	Key capability	Vendor 1	Vendor 2	Vendor 3	Vendor 4
Protect Your Backup Data and System	Immutable Snapshots				
	WORM				
	Data Encryption				
	Configuration Audit and Scanning				
	Fault Tolerance				
	Modern and Flexible Data Isolation				
Reduce the Risk of Unauthorized Access	Multi-factor Authentication (MFA)				
	Monitored Modification				
	Granular Role-based Access Control (RBAC)				
See and Detect Attacks to Stop Encroachment	AI/ML Powered				
	Anomaly Detection in Near Real Time				
	Automated Alerts				
	Cyber Vulnerability Discovery				
Strengthen Your Security Posture with Platform Extensibility	Pre-built Integrations				
	Customizable Integrations				
	Value-added Applications Interoperability				
Ensure You Can Rapidly Recover Data at Scale	Instant Recovery at Scale				
	Clean Recovery				
	In-place Recovery				

Be ready for ransomware with Cohesity next-gen data management

Cohesity makes it simple for your organization to backup, manage, secure, and derive value from your data—in the data center, edge, and cloud. Use Cohesity software to manage data infrastructure directly, or have it managed for you through a Cohesity SaaS service, or both. Cohesity solves mass data fragmentation, makes data compliance a snap, and helps businesses thwart ransomware attacks.

Cohesity was named a Leader on the Gartner Magic Quadrant for Data Center Backup and Recovery Solutions and a Leader in “The Forrester Wave™: Data Resiliency Solutions.” The company is featured in the 2020 Forbes Cloud 100, CRN’s Coolest Cloud Companies of 2020, and is the top-ranked Leader among 16 vendors in the GigaOm Radar for Unstructured Data Management.

See how Cohesity helps defend your business against sophisticated ransomware attacks

Get started with Cohesity today in AWS Marketplace

Available in AWS Marketplace

Cohesity.com | 1-855-926-4374 | 300 Park Ave., Suite 1700, San Jose, CA 95110