

5 Ways Next-Gen Data Management Boosts Cyber Resiliency



Overview

Data is under attack. The 1,070% year-over-year uptick in ransomware threats proves it¹. And today's bad actors aren't just encrypting data. They're destroying backups and exfiltrating data so they can profit and damage brand reputations at the same time. That's increasing the ransomware blast radius. Don't let ransomware attackers win. Instead, fortify your environment and improve your response strategy with five next-gen data management powers.

Global ransomware damage costs, including lost revenue and productivity, are predicted to exceed \$265 billion by 2031.²



1. Protect your backup data and system

Legacy backup isn't architected to defend data against ransomware. That's why companies still pay ransom. What's needed is data safeguards built into your backup that help preserve customer trust and competitive edge. Look for a solution with native immutable backup snapshots because those can't be encrypted, modified or deleted, protecting the authenticity of your data. Gain additional layers of protection by ensuring your backup has rules such as software-based write once, read many (WORM) with time-bound, data policy locks and FIPS-certified encryption as well as modern and flexible data isolation onsite and in public clouds that helps you meet your recovery time and point objectives plus organizational SLAs. Also find solutions that are fault tolerant, allowing you to operate despite a failed component, and let you configure automated security controls, including auditing and scanning, to eliminate human error.



2. Reduce the risk of unauthorized access

Compromising user credentials has become a top attack vector for bad actors seeking a payday. A data management platform with strict access control capabilities more effectively stops unauthorized people from taking advantage of compromised credentials. Counter insider threats and external hackers with a next-gen data management platform that supports granular role-based access control (RBAC) as part of a least-privilege, zero trust principles model; multi-factor authentication to verify who people say they are; and monitored modification that requires two sets of eyes approving every critical system change.



3. Stop encroachment by seeing and detecting attacks

According to the experts at Cybersecurity Ventures, a ransomware attack now targets a business every 11 seconds.¹ No organization has enough employees to react, which is why you need a next-gen data management solution with proactive and predictive capabilities. Look for a solution with intelligence built in, not bolted on, that allows your team to automatically discover and classify sensitive data and take advantage of near-real time threat detection. Using the solution's baseline information, your team can both receive predictive analytics-based alerts and gain early visibility into anomalies as part of both in-progress encryption-style and data exfiltration attacks.



4. Integrate your data management solution seamlessly with existing security systems

Evolving quickly, the ransomware threat isn't going away. That puts the onus on your internal teams—Infrastructure and Operations (I & O), Security Operations (SecOps) and Governance/Compliance—to work better together to prevent and respond quickly to breaches. Look for a data management solution that helps you break down data silos and functional barriers. Find an integrated and extensible solution that empowers your organization to detect, investigate and confidently respond to threats faster. The solution you choose should let you take advantage of leading security tools and give your developers a rich set of RESTful APIs to continue adding value while countering threats.



5. Rapidly recover your data at scale

Because cyber extortionists are inventive, the worst-case scenario is possible. That's why you need a data management solution that allows you to quickly recover as you refuse to pay ransom. What's needed is a solution that rapidly restores hundreds of VMs, large databases or large volumes of unstructured data instantly, at scale, to any point in time and location. And to be sure you aren't reinfecting your environment with malware, find a solution that also provides a snapshot health assessment and then allows you to perform clean and predictable data recovery directly in-place on the same platform—saving you resources and time.

Strengthen Your Cyber Resiliency With Cohesity

Discovering a solution to combat ransomware is becoming business imperative. Next-gen data management provides the data security, ransomware recovery, and cyber resiliency capabilities your organization needs to stay competitive and confidently refuse to pay ransom.

1. [FortiGuard Labs 2021 mid-year Global Threat Landscape Report](#)

2. [Cybersecurity Ventures](#)

Learn more about next-gen data management at [Cohesity.com](https://cohesity.com)

COHESITY

© 2022 Cohesity, Inc. All rights reserved.

Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated. This material (a) is intended to provide you information about Cohesity and our business and products; (b) was believed to be true and accurate at the time it was written, but is subject to change without notice; and (c) is provided on an "AS IS" basis. Cohesity disclaims all express or implied conditions, representations, warranties of any kind.

