5 Ways to Protect, Detect and Recover Boosts Cyber Resiliency

Overview

Data is under attack. The 1,070% year-over-year uptick in ransomware threats proves it[1]. 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 protect, detect and recover.

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 the ransom. What's needed is data safeguards built into your backup that help preserves 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. You can also add layers of protection by ensuring your backup has software-based write once, read many (WORM) and FIPS-certified encryption. Meet your recovery objectives and organizational SLAs with modern, flexible data isolation onsite and in public clouds. Finally, seek fault-tolerant solutions that allow you to operate despite a failed component and let you configure automated security controls like 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. Look to counter hackers and internal threats with zero trust principles. This should include role-based access controls, multi-factor authentication, quorum approval to prevent unilateral administrative changes, and monitoring with automated security scoring of your environment.

3. Stop encroachment and detect 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, so you need AI/ML-based detection to detect emerging attacks and unusual activity and illuminate sensitive data. 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 receive predictive analytics-based alerts and gain early visibility into anomalies as part of in-progress encryption-style and data exfiltration attacks.

4. Seamlessly integrate with existing security systems

The ransomware threat isn't going away and continues to evolve. 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 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 and 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 provides a snapshot health assessment and 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 a 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

COHESITY