5 Ways Ransomware Attacks Backup... And How You Can Prevent It

Overview

Backup and recovery solutions are designed to protect your organization, but sophisticated malware like Locky and Crypto are now targeting your backup data. Not surprising, considering the rise in frequency and breadth of ransomware attacks. The first ransomware payment—circa 1989—set the stage for hackers everywhere to begin locking up the data of unsuspecting targets and holding it until owners paid to get it back. According to Cybersecurity Ventures, in 2019 businesses were attacked by a ransomware attack every 14 seconds. That's why it's important to keep these five considerations in mind when you're strategizing how best to prevent, detect, and rapidly respond to a ransomware attack on your backups:

1. Sophisticated ransomware attacks make your insurance policy—your backups—a liability

Cyber criminals are now aggressively targeting shadow copies backup data—to gain full control, or worse, destroy what has long-been considered your insurance policy to business continuity. Their more sophisticated attacks enter a primary environment from an endpoint and head straight for your backups—where 80 percent of enterprise data is now stored—deleting or compromising everything there before taking over the production environment. What's needed to prevent ransomware attacking your backup is a multi-layered defense. Original backup data should be kept in an immutable state, and the gold copy of the data should never be mounted by an external system. Also, role-based access control (RBAC), multi-factor authentication (MFA) and write once read many (WORM) capabilities for the snapshot are must-have features.

2. Expanding attack surfaces expose backups to ransomware attacks

Exploding data growth (IDC estimates 175+ zettabytes of data will exist by 2025) and mass data fragmentation—the dependence upon multiple point-products (media and master servers, target storage, etc.) for backup across, spanning across different sprawling silos—have combined to widen your organization's attack surface. As a result, your backup data has become more accessible to cybercriminals. Preventing ransomware from succeeding in the first place starts with reducing your enterprise attack surface and knowing what data you have and where it is located. A unified solution for connecting infrastructure, workloads, and backup locations arms your organization against ransomware by eliminating mass data fragmentation.

Ransomware by the Numbers

- Every 11 seconds, ransomware attacks[1]
- $20 billion damage in 2021[1]
- 715% year-over-year increase since 2020[2]
- 10x to 15x more financial damage than actual ransom demand[3]

"

> Ransomware writers are aware that backups are an effective defense and are modifying their malware to track down and eliminate the backups.
>
> **CSO Magazine**

[1] Cybersecurity Ventures

[2] Bitdefender's Mid-Year Threat Landscape Report 2020

[3] Gartner: How to Prepare for Ransomware Attacks, November 2020

3. Attacks on backups made easier by intermittent monitoring

Cyber threats don't always originate from outside of an organization; they can be launched internally, too. Imagine a disgruntled employee trying to modify or delete a large set of data. Relying exclusively on backup data-ingest change rates to detect such behaviors is insufficient, hence your organization must be able to detect an attack in real time. What's needed is a solution that can continuously monitor and detect smaller change rates by analyzing files and audit logs—even when you're not paying close attention. The right backup solution will protect your organization from cyber attacks every second of every day.

4. Lack of visibility for clean restore

Recovering after a ransomware attack is stressful and time-sensitive. With a lack of visibility into the backup snapshots, what if you accidentally restore a compromised snapshot and end up re-injecting software vulnerabilities and cyber threats back into the IT production environment. While the recovery needs to be rapid, it also needs to be clean. A backup solution needs to provide deep visibility into the health and recoverability of snapshots and recommend a clean point in time to restore.

5. Long backup and recovery cycles adding to your ransomware pain

If your enterprise relies on legacy backup that require synthetic fulls and falls victim to a ransomware attack, your IT team can spend days (even weeks!) in recovery mode. A recent Ponemon Institute report puts the average cost of a single ransomware attack at $5 million due primarily to productivity loss, systems downtime, and theft of information. What's needed is a backup and recovery solution that responds fast to ransomware attacks and lets you quickly locate and delete infected files across your global data footprint—including the public clouds. Also needed is instant mass restore capabilities, which enable recovery of hundreds of virtual machines instantly, at scale, and to any point in time.

Protect, Detect, and Rapidly Recover from a Ransomware Attack

Organizations like yours want to experience zero data loss from cyber attacks and they want to have the confidence to refuse demands for a ransomware payment. Build cyber resiliency with a comprehensive approach to defending against ransomware attacks. Start by protecting your backup against becoming a target, deploy early detection, and reduce downtime and data loss with rapid and clean recovery at scale.

Download this eBook here to learn more about defending your data.

COHESITY