COHESITY

TIPSHEET

5 Ways Ransomware Renders Backup Useless

Overview

Your backup and recovery solution should protect your organization, but sophisticated malware like Locky and Crypto, now target backup data. Today's more frequent and widespread ransomware attacks are more precise, going beyond locking up your data and holding it until you pay ransom to compromising the very system designed to safeguard your data. According to Cybersecurity Ventures, ransomware was on pace to attack a business every 11 seconds by the end of 2021. That's why it's important to keep these five considerations in mind when you're strategizing about how best to protect your backup data so that if the worst were to happen, you could rapidly respond to a ransomware attack.

Ransomware by the Numbers

- Every 11 seconds, ransomware attacks[1]
- $10.5 trillion in worldwide damage by 2025[1]
- 1,070% year-over-year increase between July 2020 and June 2021[2]
- 10x to 15x more financial damage than actual ransom demand[3]

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

Cyber criminals are now aggressively targeting 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% of enterprise data is now stored—deleting or compromising everything there before taking over the production environment. What's needed to prevent ransomware from 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. Rules such as write once read many (WORM), data encryption, built-in fault tolerance, and modern data isolation as part of your backup solution provide an additional layer of protection against a ransomware attack.

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

2. Expanding attack surfaces expose backups to ransomware attacks

IDC reports 64.2ZB of data was created or replicated in 2020, and estimates 175+ zettabytes of data will exist by 2025. To protect growing data, companies have historically depended on multiple point products (e.g., media and master servers, target storage, etc.) for backup, and because these products create sprawling silos, spanning on premises and multiclouds, they widen your organization's attack surface, making your backup data more accessible to cybercriminals. Preventing ransomware from getting in starts with reducing your enterprise attack surface and addressing the challenge of mass data fragmentation, including knowing what data you have and where it's located. A unified solution that boosts visibility across infrastructure, workloads, and backup locations better defends your data against ransomware.

[1] Cybersecurity Ventures
[2] Fortinet 2021 Ransomware Survey Report
[3] Gartner: How to Prepare for Ransomware Attacks, November 2020

3. Compromised user credentials become a ransomware gift that keeps giving

Stolen credentials are the holy grail for ransomware attackers because they provide uninterrupted access into various parts of the IT environment, including backups, and allow cybercriminals to exfiltrate data for greater profit. Compromised credentials were the most common data type in intentional breaches this year, involved in a staggering 61% of breaches, according to the 2021 Verizon Data Breach Investigations Report. Organizations deploying modern backup with strict controls over user access—including role-based access controls (RBAC), multi-factor authentication (MFA) and continuous monitoring capabilities—can more effectively counter ransomware attacks, preventing the downtime and negative impact to productivity that come with them.

4. Lack of visibility and early detection give attackers a head start

Ransomware attackers thrive in dark data. They can lock up backups and move to production systems to surreptitiously remove and sell your data on the dark web. Early detection using a reliable backup and next-gen data management solution is a good start to slowing down bad actors but to discover ransomware exfiltration attacks requires near real-time detection powered by artificial intelligence and machine learning (AI/ML). Automated intelligence, including alerting, helps ensure faster attack discovery while giving your IT staff nights and weekends back.

5. Long recovery cycles add to your ransomware pain

If your enterprise—relying on legacy products that require a synthetic full backup—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 a clean copy of data across your global data footprint—including public clouds. You also need an instant mass restore capability because it enables you to recover hundreds of virtual machines (VMs), databases and a large volume of unstructured data instantly, to any point in time.

Stop Cyber Extortion and Defend Your Data From Ransomware

If you want to reduce your cyber risk exposure and have the confidence to refuse ransomware payment demands, make sure your backup and data management solutions are cyber resilient. Only a comprehensive approach to defending against ransomware attacks includes protecting your backup against becoming a target, stopping encroachment with complete visibility and early detection, and reducing downtime and data loss with rapid and clean recovery at scale.

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

COHESITY