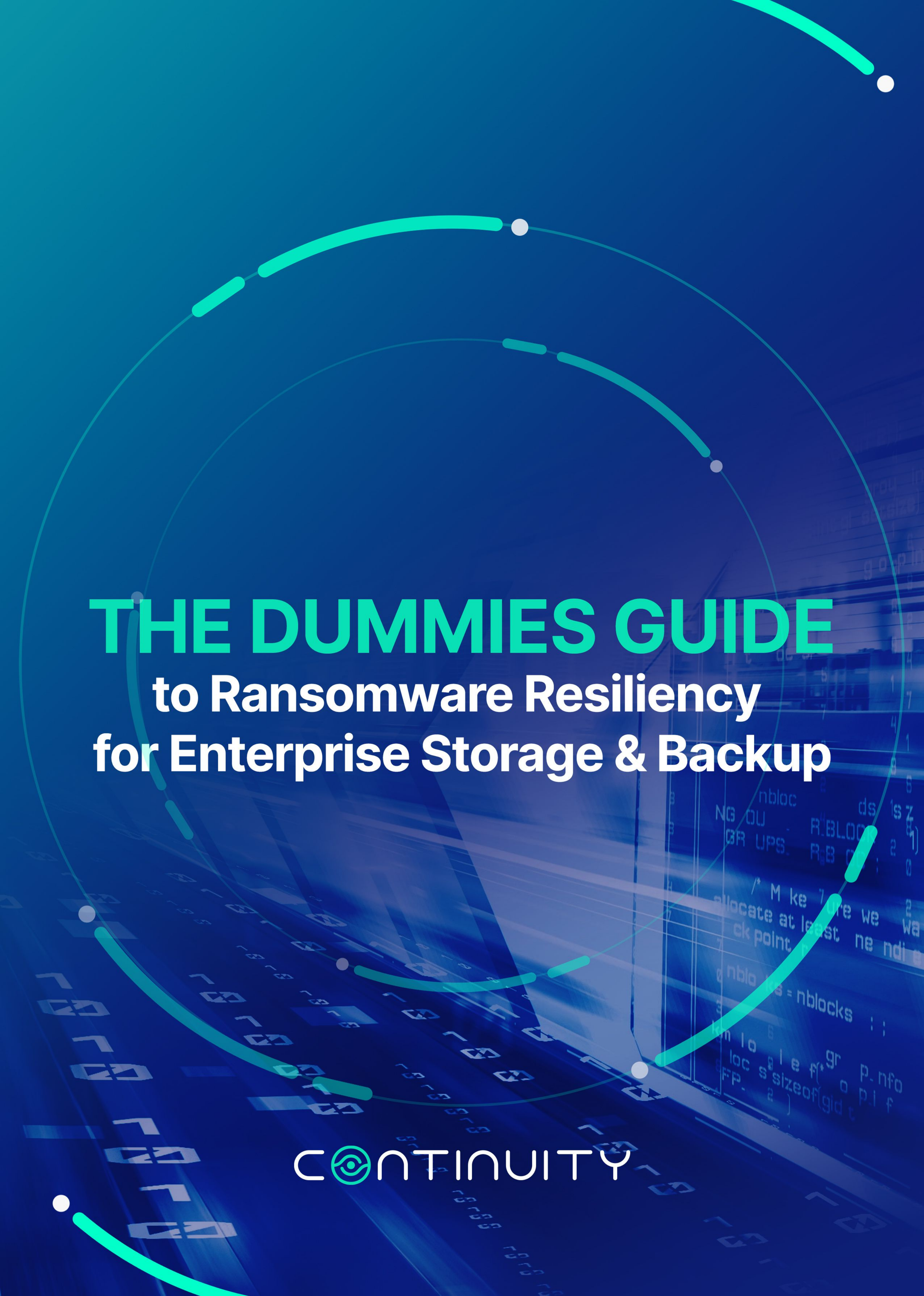


THE DUMMIES GUIDE

to Ransomware Resiliency for Enterprise Storage & Backup

CONTINUITY

Its all about the data

One thing is clear. The *"business value"* of data continues to grow, making it an organization's primary piece of intellectual property.

From a cyber risk perspective, attacks on data are the most prominent threat to organizations.

Regulators, cyber insurance firms, and auditors are paying much closer attention to the integrity, resilience, and recoverability of organization data – as well as the IT infrastructure & systems that store the data.

So, what does this mean for the security of enterprise storage & backup systems?

Just a few years ago, almost no CISO thought that storage & backups were important. That's no longer the case today.

Ransomware has pushed backup and recovery back onto the IT and corporate agenda.

Ransomware groups (e.g., Conti, Hive and REvil) are targeting enterprise storage and backup systems, to prevent recovery.

Here are some of the headlines from those attacks: https://www.continuitysoftware.com/resources/?resources_category=headlines

These attackers realize that an attack on storage or backup systems is the single biggest determining factor to show if the victim will pay the ransom.

Some ransomwares – Locky and Crypto, for example – now bypass production systems altogether, and go straight for backups.

This has forced organizations to look again at potential holes in their safety nets, by reviewing their storage, backup and recovery strategies.

CISO Point of View

We published a research report at the end of last year, where we surveyed 200 infosec leaders within the financial services sector. One of the most shocking findings was…

"Almost 60% of respondents are not confident in their ability to recover from a ransomware attack"

There's clearly a recognition that as an industry, we have blind spots.

Without a sound storage, backup and recovery strategy, companies have little chance of surviving a ransomware attack, even if they pay the ransom.

SURVEY REPORT
Sponsored feature
CISO MAG
CONTINUITY
SECURITY INTELLIGENCE REPORT
CISO Point of View:
Analysis of Storage & Backup Security in the Financial Services & Banking Sector
Maturity, challenges, and gaps

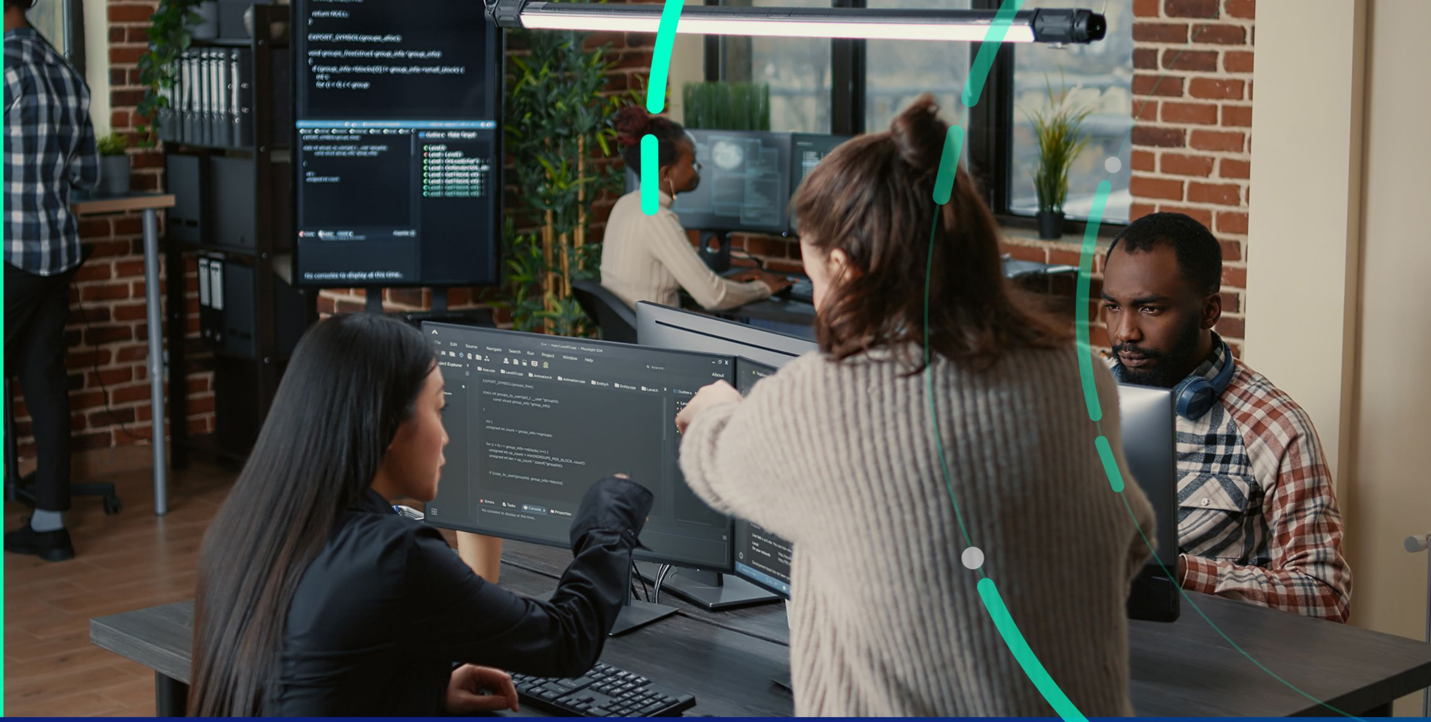
Isn’t my storage & backup vendor responsible for fixing security configurations and vulnerabilities?

Many storage managers and backup admins mistakenly believe that since their storage & backup vendors already provide patching and ongoing upgrades, they must also check for vulnerabilities and misconfigurations. Unfortunately, that’s not quite the case.

While storage & backup vendors provide excellent tools to manage availability and performance of their infrastructure, they DO NOT do the same for the security and configuration of those same systems.

Some storage and backup vendors publish security best practice guides. However, implementation and monitoring of security features, and configurations is the responsibility of your organization’s infrastructure and/or security departments.

There are, however, a number of cybersecurity capabilities, ransomware protection solutions, and also configuration management features, provided by the storage vendors.



Here are 4 of the most common ransomware resiliency solutions for storage & backup:

Air-gapped data copies

Adding an air-gap means separating backups from production data. This means that if the production environment is breached, attackers don't immediately have access to backups.

You can also keep storage accounts separate.

Immutable storage & vault

Immutable storage is the simplest way to protect backup data. Data is stored in a Write Once Read Many (WORM) state and cannot be deleted for a pre-specified period.

Policies are set in backup software or at storage level and it means backups can't be changed or encrypted.

The only downside is that it will increase how much data is stored. In addition, one of the criticisms of immutable storage is that it is slower. Immutability increases how much data is stored, so it is often pushed off onto the slower, archive tiers of storage.

Storage snapshots & replication

Snapshots record the live state of a system to another location, whether that's on-premises or in the cloud. So, if ransomware hits the production system, there is every chance it will be replicated onto the copy.

However, some ransomware – Locky and Crypto, for example – now bypass production systems altogether, and go straight for backups!

This has forced organizations to look again at their storage & backup security strategies.

Vulnerability Management for storage & backup

Vulnerability management solutions help you get a full view of the security risks in your storage & backup systems. It does this by continuously scanning these systems, to automatically detect security misconfigurations and vulnerabilities.

It also prioritizes risks in order of urgency and business impact, and provides remediation guidance.

Ransomware resiliency solutions provided by the storage & backup vendors

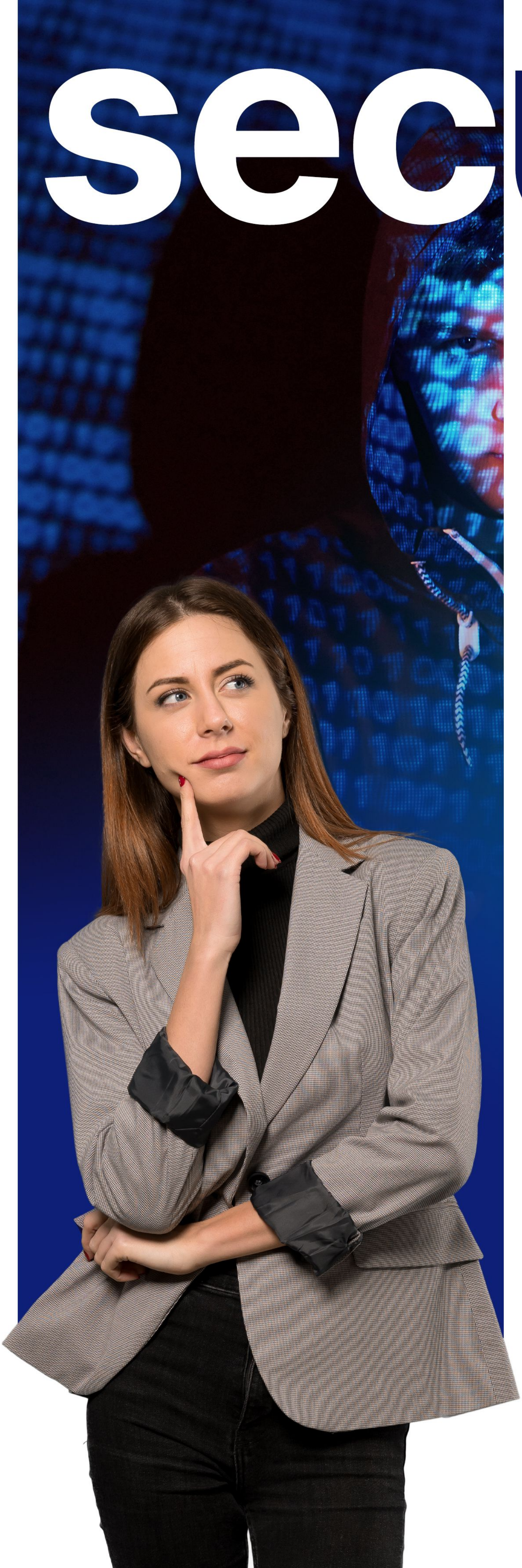
Enterprise storage vendors

- Dell's PowerProtect Cyber Recovery offers an air-gapped solution with data isolation and immutability, while also detecting suspicious activity.
- IBM's Storage Insights monitors SAN switch configuration, health and performance.
- NetApp's SnapCenter provides snapshots, to facilitate rollback to point-in-time copies. This helps to simplify backup and restore of data.
- NetApp's CloudSecure analyzes data access patterns to identify risks from ransomware attacks.
- Infinidat's InfiniSafe provides immutable snapshots, air-gapped protection, and fenced forensic network.
- Broadcom's Storage Protection offers malware detection and prevention for cloud services, NAS devices, and Amazon S3 buckets.
- Pure Storage's Purity SafeGuard snapshots lock down critical data you need to recover from a cyberattack, by creating an immutable copy that cannot be corrupted or encrypted by any attack.

Enterprise backup vendors

- Rubrik – ZeroTrust Data Management protect enterprise data from cyberattacks with an air-gapped, immutable file system that can't be modified, deleted, or encrypted by hackers.
- Rubrik also offers Cloud Vault, a managed cloud storage service to keep a secure, isolated and logically air gapped data copy to recover quickly in the event of a cyberattack.
- Cohesity's DataProtect offers immutable backup snapshots, data encryption, and AI-based detection
- Commvault's Complete Data Protection also provides encryption, immutability, and air gap backup copies, along with machine learning-based anomaly detection

secure



So, I’m completely secure, right?

While immutability is helpful in remediating cyberthreats, it is only the beginning of a comprehensive protection practice. And its certainly not bullet proof.

Immutable storage can be ‘poisoned’, enabling hackers to change the configuration of backup clients and gradually replace stored data with meaningless information.

In addition, once hackers gain access to the storage system, they can easily wipe out snapshots. So they’re also not bullet proof.

The one MAJOR thing missing from all these vendors is the ability to continuously scan the storage & backup infrastructure for security misconfigurations and vulnerabilities.

These security risks can likely be exploited by attackers to compromise production and recovery systems – and the data on them.

This is not just theoretical. Its already happening. Just take a look at some recent examples: https://www.continuitysoftware.com/resources/?resources_category=headlines

You wouldn’t dream of not continuously scanning your endpoints, OS and network layers for security risks. So why wouldn’t you do it for your most important layer of IT?

This is why I recommend deploying a vulnerability management solution to help you continuously scan your storage & backup systems, to automatically detect security misconfigurations and vulnerabilities.

These solutions also prioritize risks in order of urgency and business impact, and some of them even include remediation guidance and auto-remediation features.

6 Recommendations

A Dummies Guide

01 Assign higher priority to improving the security of enterprise storage and backup systems

02 Build up knowledge and skill sets – and improve collaboration between your Infosec and IT infrastructure teams

03 Define comprehensive security baselines for all components of storage and backup systems

04 Use automation to reduce exposure to risk, and allow much more agility in adapting to changing priorities. Vulnerability management solutions can go a long way to helping you reduce this exposure.

05 Apply much stricter controls and more comprehensive testing of storage security and the ability to recover from an attack. This will not only improve confidence, but will also help identify key data assets that might not meet the required level of data protection

06 Include all aspects of storage and backup management, including often-overlooked key components such as fiber-channel network devices, management consoles, etc.

CONTINUITY

WWW.CONTINUITYSOFTWARE.COM