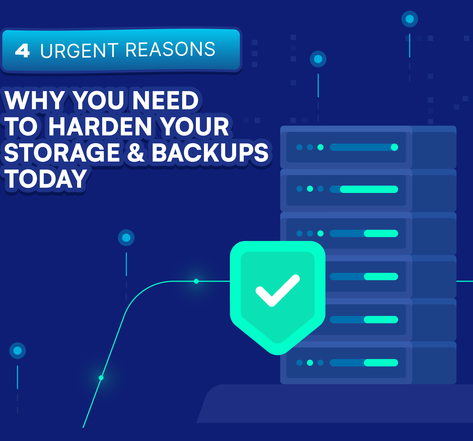
CONTINUITY

4 URGENT REASONS

WHY YOU NEED TO HARDEN YOUR STORAGE & BACKUPS TODAY



1 The Effects Of A Successful Ransomware Attack On A Storage Or Backup System Would Be Devastating

The impact of a compromised storage or backup system is significantly greater than any other IT system. This is because a compromise of a single storage array can bring down thousands of servers.

Furthermore, while recovery of an individual server is relatively straightforward, recovery of a storage array is a complete unknown to many CISOs.

Gigabytes

End-user devices

Terabytes

Compute & Host systems

Petabytes

Data Storage & Backup systems

Amount of data on single devices

2 Storage & Backup Systems Are Vulnerable

An enterprise storage & backup device has on average

14 security risks, of which 3 are critical risk.

The most common type of risks include:
insecure network settings, unaddressed CVEs, access rights issues (over exposure), insecure user management & authentication, and insufficient logging & auditing

3 Ransomware Is Now Targeting Storage & Backup Systems

93% of cyberattacks target backup and storage systems to force ransom payment, and are successful in debilitating their victims' ability to recover in 75% of those events.

https://www.techradar.com/news/ransomware-attackers-are-going-after-backup-storage-to-force-you-to-pay-up

BREAKING NEWS

threatpost

"The Conti ransomware gang has developed novel tactics to demolish backups…. According to Palo Alto Networks; "it's one of the most ruthless of the dozens of ransomware gangs that we follow."

"The ransomware was targeting poorly protected Network-Attached Storage (NAS) devices. The threat actors exploited known vulnerabilities."

BLEEPING COMPUTER

"This new ransomware gang is known to seek out and delete any backups to prevent them from being used by the victim to recover their data."

4 Auditors, Regulatory Bodies & Industry Standards Are Now Taking A Much Closer Look At The Security Of Storage & Backup Systems

NIST National Institute of Standards and Technology

"Periodically and proactively assess configuration compliance to storage security policy."

[NIST Special Publication 800-209; Security Guidelines for Storage Infrastructure]

ISO

"Actively manage the security posture of the storage technology and protection mechanisms… Perform regular security threat assessments to evaluate security readiness… All operating systems, hypervisors and applications should be hardened relative to the use of the storage system."

[ISO 27040; Information Technology Security Techniques: Storage Security – to be published at the end of 2023]

ISO

8.13 - Information backup: "Control Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup."

[ISO/IEC 27001; Information Security Management Systems]

DORA Digital Operational Resilience Act

Article 12.2 - Backup policies and procedures: "…The activation of backup systems shall not jeopardise the security of the network and information systems or the availability, authenticity, integrity or confidentiality of data."

[Digital Operational Resilience Act - DORA]

www.continuitysoftware.com