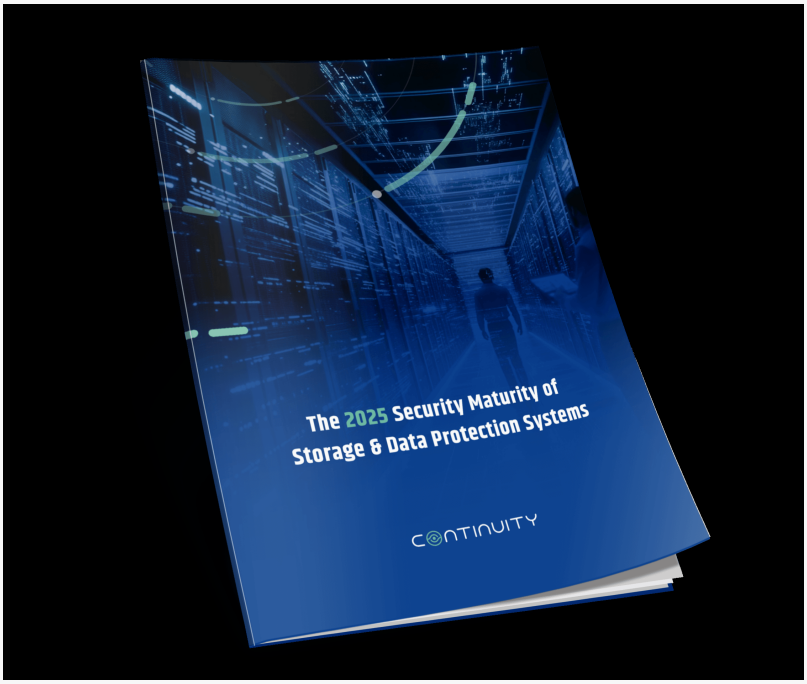
New Report Reveals Critical Security Risks in Enterprise Storage and Backup Systems

Continuity announces third edition of 'The 2025 Security Maturity of Storage & Data Protection Systems'



The Security Maturity of Storage & Data Protection Systems 2025

NEW YORK, NY, UNITED STATES, June 12, 2025 /EINPresswire.com/ -- Continuity, a leading provider of cyber resilience solutions, today published the 3nd edition of "The 2025 Security Maturity of Storage & Data Protection Systems." The research showed that an average enterprise storage and backup device has 10 vulnerabilities. 5 are high or critical risk, which could present a significant compromise if exploited.

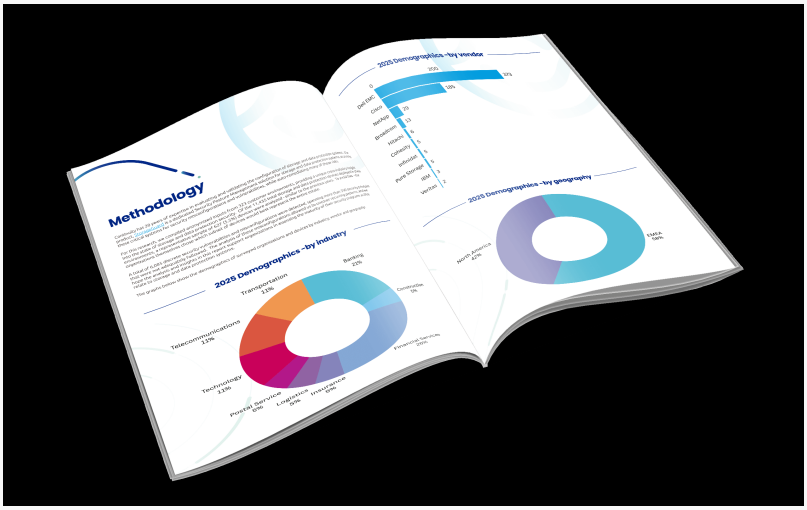
Over the past two months, targeted cyberattacks on enterprise storage and backup systems have surged, with a sharp rise in exploited vulnerabilities across major platforms like Commvault, Hitachi Vantara, Dell, Veeam, and Veritas, along with a rise in breaches caused by misconfigured storage and backup systems. This report shows that these critical IT systems are falling dangerously behind in security.

> We conducted this analysis to offer greater insight into the problems in data storage and backup security, and underscores the importance of taking a proactive approach to fixing these risks"
>
> *Gil Hecht*

"Securing enterprise storage and backup systems has become a critical part of organizations' cyber resiliency strategies," said Dennis Hahn, principal analyst, Data Center Storage and Data Management for analyst firm, Omdia. "As important as rapid data recovery is to business continuity if data is lost or stolen, it is arguably even more important to protect data anywhere it lives and not let storage and backup systems themselves become an entry point for attack."

Key Findings

The third annual Security Maturity of Storage & Data Protection Systems Report assessed 323 enterprise customer environments with 11,435 storage and backup devices from leading providers including Dell, NetApp, Veritas, Hitachi Vantara, Pure, Commvault and others. 53% of organizations were from the Financial & Banking sector. Other industries included Transportation, Telecommunications, Logistics, Technology and Postal Services. Key findings include:



Inside The 2025 Security Maturity of Storage & Data Protection Systems

• A total of 6,085 discrete security issues (e.g., vulnerabilities and security misconfigurations) were detected, spanning 390 security principles that were not adequately followed
• On average, an enterprise storage and backup device has 10 security risks, of which 5 are of high or critical risk rating, meaning each would present a significant compromise if exploited. This finding is slightly higher than previous years.
• While deployment of immutable storage is rising, this can lead to a false sense of security if not implemented properly, and unfortunately, the analysis detected a significant number of misconfiguration issues specific to these features
• Unpatched vulnerabilities in storage and backup systems are one of the main points of attack for most ransomware. Users are not aware of the fact that traditional Vulnerability Management tools do not cover those systems well

The top five security risks found in this year's analysis were:

1. Authentication and Identity management
2. Unaddressed CVEs
3. Network and Protocol Security
4. Encryption and Key Management
5. Access Control and Authorization

The report provides additional details about these risks and recommends best practices for remediation. Other resources include the NIST SP-800-209 Security Guidelines for Storage Infrastructure, co-authored by Continuity, and ISO 27040 (2024), where Continuity was on the editorial board, as well as a selection of practical guides on www.continuitysoftware.com.

"We conducted this research to offer greater insight into the scope of the problems in data

storage and backup security," said Gil Hecht, CEO of Continuity. "Not only did it help to quantify the high level of vulnerabilities and security misconfigurations in the average enterprise storage and backup system, it also underscores the importance of taking a proactive and automated approach to fixing them."

Continuity's flagship product, StorageGuard, scans, detects and fixes security misconfigurations and vulnerabilities across storage and backup devices. StorageGuard gives customers complete visibility of security risks in their storage and backup environment, while hardening these critical systems and guaranteeing compliance with security regulations and industry standards.

The "The 2025 Security Maturity of Storage & Data Protection Systems" and more information about Continuity's StorageGuard are available online.

About Continuity

With the rise in cybersecurity threats, Continuity is the only solution provider that helps enterprises protect their data by securing their storage and backup systems. Continuity's StorageGuard provides organizations with visibility of all security misconfigurations and vulnerabilities in their storage and backup systems, while automating regulatory compliance.

Among Continuity's customers are the world's largest financial services firms and Fortune 500 enterprises, including six of the top ten U.S. banks. For more information, please visit www.continuitysoftware.com.

Doron Youngerwood
Continuity Software
+1 6462168628
dorony@continuitysoftware.com
Visit us on social media:
LinkedIn
Facebook
YouTube
X
