

Continuity's Industry-First Research Shows Enterprise Storage Security Significantly Lags Behind Computer & Network Sec

Analysis of More than 400 Enterprise Storage Devices Detected 6,300 Discrete Security Issues; On Average, Analyzed Devices Had 15 Security Vulnerabilities



NEW YORK, NEW YORK, UNITED

STATES, October 13, 2021 /EINPresswire.com/ -- [Continuity™](#), a leading provider of cyber resilience solutions, today issued [The State of Storage Security Report](#). The first research to examine the security of storage systems, this new report provides an analysis of the vulnerabilities and misconfigurations of enterprise storage systems. The findings revealed that

storage systems have a significantly weaker security posture than the other two layers of IT infrastructure: compute or network.

“

Organizations must act immediately to better protect their storage – as well as backup systems - to ensure their data is secure against ransomware and other cyberattacks”

Gil Hecht

These findings are alarming given the fact that, unlike an attack on individual endpoints or servers, which can cause problems, an attack that targets storage systems can be truly devastating. A compromise of a single storage array can bring down thousands of servers – and wipe out petabytes of data, a frightening prospect given the rise in ransomware attacks over the past three years that target

corporate data.

For The State of Storage Security Report, Continuity's automated risk detection engines analyzed data from more than 400 enterprise storage devices from vendors including Brocade, Cisco, Dell EMC, IBM, Hitachi Data Systems, NetApp, and others.

Key research findings include:

- ☐ More than 6,300 discrete security issues, such as vulnerabilities and misconfigurations, were detected;
- ☐ More than 170 security principles were not adequately followed;
- ☐ On average, enterprise storage devices had 15 security vulnerabilities. Approximately three of

those were considered a high or critical risk rating -- meaning they could present a significant compromise if exploited.

□ The five most common types of vulnerabilities included: use of vulnerable protocols/protocol settings, unaddressed common vulnerabilities and exposures (CVEs), access rights issues (over exposure), insecure user management and authentication, and insufficient logging.

“Of the three main IT infrastructure categories -- compute, network, and storage -- the latter often holds the greatest value, from both security and business perspectives,” said Gil Hecht, founder and CEO of Continuity. “Security vulnerabilities and misconfigurations of storage devices present a significant threat, especially as ransomware attacks have taken hold of businesses over the past few years. Yet based on our analysis, the security posture of most enterprise storage systems is strikingly weak. Organizations must act immediately to better protect their storage – as well as backup systems - to ensure their data is secure against ransomware and other cyberattacks.”

To help organizations gain the visibility they need to understand their storage vulnerability risk and avoid blind spots, Continuity recommends that they evaluate existing security processes and ensure that the storage layer be secured and hardened to a similar - if not greater - extent as compute and network assets.

Continuity's StorageGuard is the only solution that checks for thousands of possible misconfigurations and vulnerabilities at the storage system level that pose a security threat to organizations' data.

Methodology:

Continuity compiled anonymized inputs from more than 20 customer environments across North America and EMEA, covering the banking & financial services, transportation, healthcare, telecommunications and other industry sectors. A total of 423 enterprise storage devices were analyzed from vendors including Brocade, Cisco, Dell EMC, IBM, Hitachi Data Systems, NetApp, and others. The analysis covered the configuration of block, object and IP storage systems, SAN / NAS, storage management servers, storage appliances, virtual SAN, storage network switches, data protection appliances, storage virtualization systems and other storage devices. Continuity's automated risk detection engines checked for thousands of possible misconfigurations and vulnerabilities at the storage system level that posed a security threat, of which was tagged with a security index (1-5) and tracked so as to allow for detailed assessment, aggregation and drill down.

Additional Resources:

□ Read the [NIST Guide for Storage Security](#) – co-authored by Continuity.

□ Download the Storage Security Handbook for an overview of the evolution of the storage technology landscape, and a set of practical recommendations on avoiding emerging threats.

□ Visit our blog for storage security insights and advice from company executives and experts.

About Continuity

With the rise in cybersecurity threats, Continuity is the only solution provider that helps enterprises protect their data by securing their storage systems – both on-premises and in the cloud. Continuity's StorageGuard complements existing data-protection and vulnerability management solutions, by adding a layer of security that prevents attackers from penetrating storage and backup systems which can result in gaining control over practically all of an enterprise's critical data.

Among Continuity's customers are the world's largest financial services firms and Fortune 500 enterprises, including six of the top 10 US banks. For more information, please visit

www.continuitysoftware.com

Sarah H Hawley

Mockingbird Communications for Continuity

+ +1 4802924640

[email us here](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/553675608>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2021 IPD Group, Inc. All Right Reserved.