Backup and Security Converge as World Backup Day Reinforces Requirement for Secure Data Protection

Annual Reminder to Backup Important Data Now Complicated with Growing Cybersecurity Threats Attempting to Prevent Recoveries

TORONTO, ONTARIO, CANADA, March 31, 2022 /EINPresswire.com/ -- Asigra Inc., a leader in cyber-secure backup and recovery, welcomed the arrival of World Backup Day as cybersecurity threats to corporate data have increased globally with backup data being targeted to prevent successful recoveries. Taking place on March 31st, 2022, the organizers advise anyone with important data to adopt a proper backup strategy, while industry experts recommend security-enabled data protection that integrate cybersecurity with backup.

According to Gartner®, "Ransomware attacks against corporate data centers and cloud infrastructure are growing in complexity and sophistication, and are challenging the readiness of data protection teams to recover from an attack."(1)

In alignment with World Backup Day 2022, where persons with valuable or sensitive information are admonished to protect that data with a modern backup solution, Asigra recommends the use of a cyber secure solution that counters both data loss and data corruption. Working with tens of thousands of organizations globally, the company continues to receive feedback that a cybersecurity integrated backup platform is the best way to protect a company's last line of defense in recovering mission critical data.

With advanced ransomware a primary threat to backup data and the continuity of business

operations, protection against destructive cyberattacks is a top priority for managed service providers and their business customers to focus on reducing the damage caused by such events. In the most notable ransomware attacks on backup data, ransomware first entered the network and was then backed up, where it remained silent and undetected before detonating. Then, when a recovery was required from the infected backup set, the system restored that long-hidden, dormant ransomware, triggering a costly attack loop that took down the IT department. In other cases, ransomware has deleted the entire backup repository.

Defensive tactics like air-gapped and immutable storage are effective protection against natural disasters and older forms of ransomware but fall woefully short when facing today's weaponized ransomware and other advanced persistent threats (APTs). Asigra takes a completely different approach to protecting data. A multi-layered proactive approach featuring several layers of cybersecurity and anti-ransomware protections integrated into the solution. Asigra hunts and terminates attacks targeting backup data and addresses all areas with proactive data security such as integrated anti-malware and Deep MFA (multi-factor authentication).

"Advanced ransomware attacks utilize trojan horse strategies with detonation delays of weeks or months, ensuring that the dormant malware is implanted in all backups, whether air-gapped or stored in immutable repositories," said Eric Simmons, CEO, Asiga. "Asigra is focused on hunting down those ransomware variants and other threats, whether zero-day or dormant attacks. Our extremely thorough anti-malware scanning complements scans performed at the endpoint by examining the actual backup stream, checking all data to ensure business continuity."

For a demonstration of this enhanced data protection suite, please contact info@asigra.com or visit https://www.asigra.com/contact-us to schedule.

Tweet This: Backup and Security Inseparable as World Backup Day Reinforces Requirement for Secure Data Protection - @Asigra https://bit.ly/2N04LHu

Additional Resources:

- Download a comprehensive paper on this topic titled "Securing your backups against Log4J vulnerabilities" at https://info.asigra.com/lm-log-4j-whitepaper
- Hear what service providers have to say about working with Asigra: https://www.asigra.com/partnership.
- Follow Asigra on Twitter at: http://twitter.com/asigra
- View the enhanced features of the Asigra Hybrid Cloud Partner Program at: https://www.crn.com/slide-shows/cloud/300101651/2018-partner-program-guide-5-star-cloud-vendors-part-1.htm/pgno/0/7

(1) Gartner ®, How to Recover from a Ransomware Attack Using Modern Backup" by Fintan Quinn, https://www.gartner.com/en/doc/738061-how-to-recover-from-a-ransomware-attack-using-modern-backup. GARTNER is a registered trademark and service mark of Gartner, Inc.

About Asigra
Trusted since 1986, Asigra advanced AI-enabled data protection platform is proudly developed in and supported from North America, providing organizations around the world the ability to quickly recover their data from anywhere through a global network of IT service providers. As the industry's most secure backup and recovery solution for servers, virtual machines, endpoint devices, databases, applications, SaaS and IaaS based applications, Asigra protects sensitive data with anti-ransomware defense and 100% recovery assurance. The company has been recognized as a three-time Product of the Year Gold winner by Techtarget for Enterprise Backup and Recovery Software and positioned well in leading market research. More information on Asigra can be found at www.asigra.com.

###

Contact Asigra
Call 877-736-9901 or email info@asigra.com

Joe Austin
Public Relations
email us here
Visit us on social media:
Facebook
Twitter
LinkedIn
