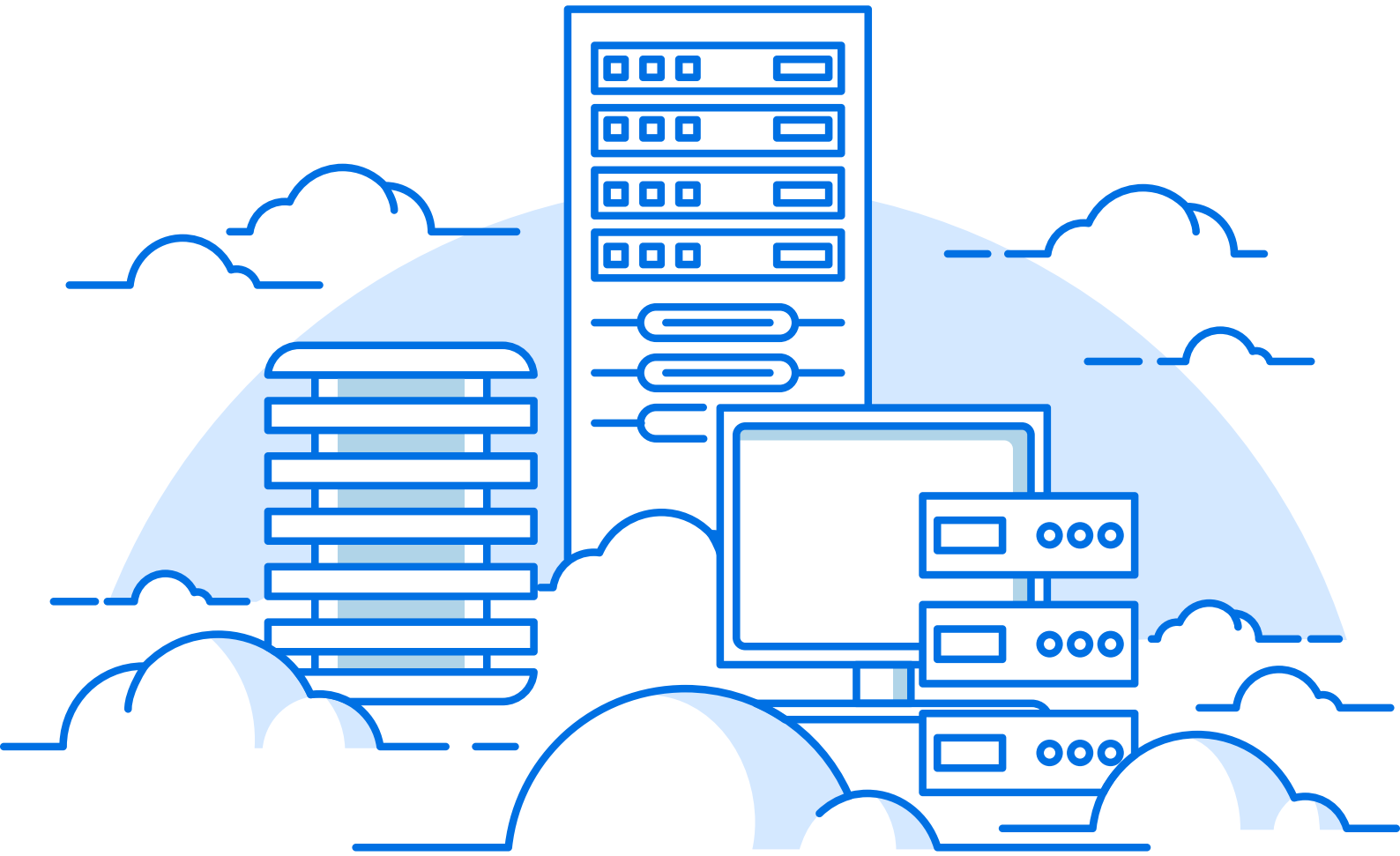
CISO Lessons Learned

Ransomware-Proofing Storage & Backup Systems

CONTINUITY



Chapter 1:

The Major Gap in the Security Posture of Organizations: Storage & Backups

Organizations are continuously looking for better ways to close security gaps. Targeted attacks on data have been on the rise over the past several years. As a result, cybercriminals have become increasingly more sophisticated and successful in their attacks. Included in these increased attacks are tactics targeting storage and backup systems which can cripple organizations.

In this whitepaper, we'll cover CISO lessons on the impact of ransomware attacks on organizations' storage & backup systems, the risks associated in the event of an attack, and provide several lessons learned on how being proactive with the security of storage and backup systems versus reactive can further close security gaps.

Ransomware Can Cripple Organizations

Designed to hold data at a ransom, threat actors will often target storage and backup systems first. Once successfully deployed into the system, most of today's ransomware is targeted at eliminating backups first and then encrypt data, demanding payment from organizations.

Marc Ashworth
CISO
First Bank

"Veeam has done a study that showed that 93% of all ransomware attacks target backups," states **First Bank CISO, Marc Ashworth**. Attacks to the storage and backups can force victims to start from scratch again.

For many large enterprises, a ransomware attack can devastate operations and result in the shutdown of facilities.

Ashworth shared some additional examples of the impact of ransomware on organizations. "In 2021, Lincoln University, which had been around for 160 years, was forced to close their doors. Another example is Saint Margaret's Hospital in Illinois shut down operations after a ransomware attack." This closure left the citizens within the town of Spring Valley forced to find basic healthcare needs in neighboring towns after the hospital closed. These examples of ransomware attacks that breach storage and backups have only increased over time.

Numerous Risks Associated With Storage & Backups

As threats continue to evolve, the risks organizations face will constantly change. When looking at the average number of vulnerabilities in storage & backup systems, there is still a major gap for many enterprises. "Protecting backups is extremely important because if you get hit by ransomware, your ability to restore is critical," says CISO Marc Ashworth.

Key Findings

9,996

9,996 discrete security issues were analyzed

14

An enterprise storage & backup device has on average 14 vulnerabilities

3

Out of 14 vulnerabilities, 3 are high or critical risk

Source: The State of Storage & Backup Security Report 2023

Data has shown that many enterprises lack the proper security to protect their storage and backup systems. Threat actors often target data backups and storage first to ensure that organizations are more eager to recover it quickly. However, enterprises that cannot afford or refuse to pay ransoms face a risk of complete loss of their data.

For organizations that cannot restore and recover their data, there are ways they can offload that risk, says Ashworth. He states that, "one way to do that is with cyber insurance." The goal of cyber insurance is to help afford the ransomware cost in order to recover your data successfully. However, Ashworth warns that "in certain industries, it is becoming more difficult to secure insurance. Also, the cost of it keeps going up due to the volume of ransomware attacks faced today."

There is some risk associated with relying on cyber insurance for ransomware payments, recovery, and remediation. As stated by former CISO and cybersecurity expert John Meakin, he's seen that cyber insurers over the past few years have shifted their pre-proposal questionnaire from asking companies if they have backups to "How good are those backups and how well-protected are those backups?" This is because many of the cyber insurance firms are mandating stricter security controls of their storage and backup systems, to better protect themselves against cyberattacks.

John Meakin
Former CISO
Standard Chartered,
GSK, & Deutsche
Bank

As stated by **former CISO at Standard Chartered, GlaxoSmithKline and Deutsche Bank, John Meakin**, "One cyber incident I was involved in, the organization had backups but they weren't available anymore. This wasn't because they were wiped out by the hackers, but in this case, they weren't protected against system changes – which made them unreadable.

This is a dark area in the world of backup and data protection, but it can be the defining moment that ends up biting you on the backside."

Meakin's point further emphasizes the need for securing storage and backup systems continuously. He states that, "this should be tested, ensuring accessibility to it", in the event of an incident affecting access to the storage and backup systems.

Being Proactive vs. Reactive Helps Close Security Gaps

In the security space, there is often a sense of reactiveness when it comes to closing security gaps. Many organizations only face the repercussions of incident post-discovery. This can make protecting your data through backup and storage more challenging if your security controls are protecting effectively. As CISO Marc Ashworth states, “at some point if you’re not checking those boxes off, then you won’t qualify for cyber insurance.” This can mean that organizations that are not implementing proactive security controls will struggle to receive support via insurance in the event of cyber attacks.

For companies and their teams to embrace more pro-activeness in security, it can start with understanding their threat landscape. This also emphasizes the need to go beyond only the necessary control that meet regulatory and compliance standards. With a threat landscape that can pivot rapidly nowadays, there is a greater need that leadership be tuned into the risks the company may face. This can include common attack pathways and any other exploits that they are and others in their respective industries are experiencing.

Closing security gaps in your overall security posture before the risk of attack is the best line of defense for organizations globally. An organization’s storage and backup systems are their final line of protection against attacks. CISO John Meakin emphasizes this point by stating, “Many security guys don’t see backups yet as being one of the key assets at risk. And the IT Infrastructure guys don’t see backups as being a key security mechanism. And both those attitudes need to change.”

Securely configuring these mission-critical systems plus verifying they are a part of the security testing process can better protect organizations from the devastating consequences of losing that last line of defense.

Chapter 2:

Aligning with Evolving Security Priorities: How CISOs Balance Changing Compliance, Risk & Regulations with Business Need

The risks seen these days require security leadership to maneuver in a complex landscape of emerging cyber threats, ever-changing regulations, and the necessity to protect sensitive data. This includes the growing need for greater security posture of backup and storage systems.

Navigating the Changes in Compliance & Regulation Standards

Jim Shook
Cybersecurity & Compliance Director
Dell Technologies

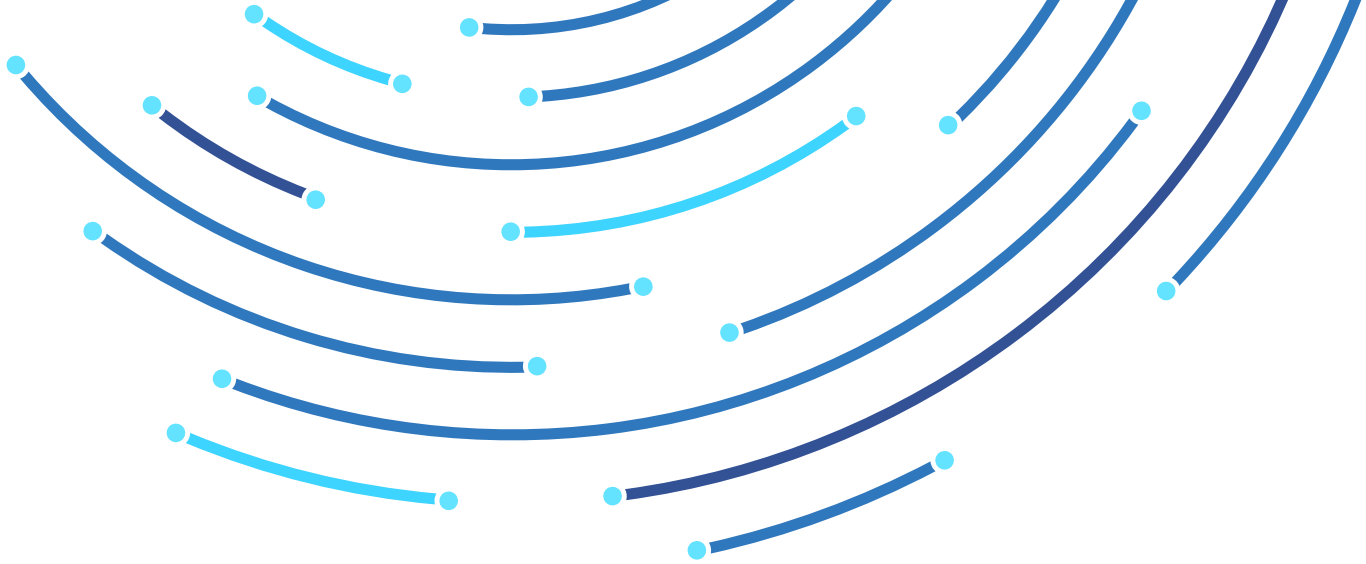
Cybersecurity and Compliance Director for Dell Technologies, Jim Shook recognizes many regulatory shifts that impact security of storage & backup systems.

"A lot of these requirements, such as ISO/IEC 27040 and DORA, require organizations to regularly assess their storage & backup environment and risk appetite." As a result, CISOs must work with other IT and GRC stakeholders to ensure regulations are met.

Shook also advises, "Organizations should regularly review their industry regulations as they change often. This is also the case when working with specific security frameworks, even if you don't adopt them all. It's critical to understand that regulations are there to protect you in the event of a breach." Shook further emphasizes the need to better navigate regulatory changes by adding, "it protects if you have a legal claim. If there is a breach and you have to defend the organization in court and necessary standards have been met, that's going to be a shield working on your behalf."

As security leaders and industry experts have witnessed more recently, governments are tightening security measures on organizations post-breach. This is especially the case seen in recent breaches such as Uber and SolarWinds. In the aftermath of these breaches, CISOs have been held more legally accountable for not properly adhering to regulatory standards or properly addressing the organizational risks faced by their respective industries.

Ultimately, CISOs along with their teams should proactively work with other IT and GRC stakeholders to ensure that regulations are not only met, but the controls are working effectively.



Adapting to Increasing Cyber Insurance Requirements

Along with consistent changes to compliance and regulation obligations, many CISOs are also faced with managing the increase of cyber insurance requirements. Many cyber insurers are now requiring organizations to address their risks to their storage and backup system security. **First Bank CISO Marc Ashworth** also provided some expert commentary on the value that cyber insurance can provide to organizations by stating, "Protecting backups is critically important because if you get hit by ransomware, having the ability to restore is crucial. Your cyber insurance can help with the ransomware cost."

While cyber insurance can help support some of the cost associated with a cyberattack, Ashworth cautions leaders by stating "It's becoming harder to get insurance in certain industries given the cost continues to increase due to the losses organizations are experiencing." Ashworth also states, "Insurers are taking the lead and looking at the standards and requirements that are being proposed. Whether it's the White House Executive Order or other international regulations, insurers are incorporating those questions within the questionnaires."

In addition to the challenges faced with securing cyber insurance, **former CISO and security expert John Meakin** advises CISOs to ensure that "meeting expectations should include meeting the bar set by our insurers." He also states that "in recent years cyber insurers have shifted their pre-proposal qualification questionnaires from asking do you have backups to how good are those backups and how well-protected are they."

"Cyber insurers are becoming more and more restrictive," says Ashworth. He also alerts CISOs that "if you're not doing those recommended practices, meeting the regular backups necessary, and other data storage requirements, you may not receive coverage. Taking that risk and self-insuring for potential losses could cost organizations hundreds of thousands, if not millions of dollars. Depending on the size of the organization."

Adapting to ever-increasing and stricter cyber insurance requirements does not work efficiently with last-minute preparations. Proactive security, detailed documentation, and readiness to assess your risk posture are the keys to ensuring insurability and protecting your organization's assets. Organizations that evolve with regulatory and insurance changes benefit from quicker remediation for security incidents.

Chapter 3:

The Developing Role of the CISO: Expanded Security Responsibilities in an Evolving Threat Landscape

One of those conversations in a CISO panel hosted by Continuity, delved into the responsibility of securing storage and backups. As stated by First Bank CISO Marc Ashworth, “Security is everyone’s responsibility. However, security shouldn’t single-handedly hold the ownership of securing storage & backup systems. They should be providing security oversight and guidance to the IT Infrastructure & Operations team. Then it is up to them to implement the necessary controls to harden these systems, and then verify the security of them”

Former CISO and security expert John Meakin states that “many CISOs may not see backups yet as being one of the key assets at risk for a company. Then the infrastructure folks fail to see backups as being a key security defense. Both those perspectives need to shift.”

Meakin goes on to state that, “if the security team is going to see backups as a key asset risk, then this is under the assumption that, ideally, there should be continuous scanning of these assets for vulnerabilities. Also, there is a need for setting baseline secure configurations for all of your storage & backup assets, and monitoring them for security events.” For many CISOs defining and clarifying the ownership of storage and backup security is key. By doing this it allows both the IT Infrastructure and Security teams to work collaboratively with establishing processes and controls for better security posture.

Understanding the Additional Factors with Storage & Backup Security

In our panel discussion the **Director of Cybersecurity and Compliance, Jim Shook** cautions CISOs and IT leaders to better prioritize the security of storage and backups collaboratively. He advises, "The goal should not be to just check the box. CISOs should understand the threat vectors that they are concerned about. It's great having backups, but are they secure? It's important to also test if they are secure from a threat that might be a cybercriminal overwriting the data versus a threat that somebody comes in as an administrator and deletes the backups."

Additionally Shook emphasizes that when understanding the additional factors of storage and backup security, CISOs should work with their teams to ensure that the controls teams put in place should also be tested regularly. He states, "I have seen organizations who have another copy of their backup in a cloud, or hosted in a different system or location. But the question to be asked the most is have the recovery requirements and controls been tested for their effectiveness?"

There are many additional factors that can impact the security of storage and backup systems. As **John Meakin** shared, "In an incident I was involved in previously, backups were not available because they were not protected against system changes, which rendered them unreadable for recovery." CISOs must ensure their team is checking that the controls implemented from the IT Infrastructure team are working effectively, beyond the threshold of an attack.

Establishing the Security Baselines for Storage & Backups

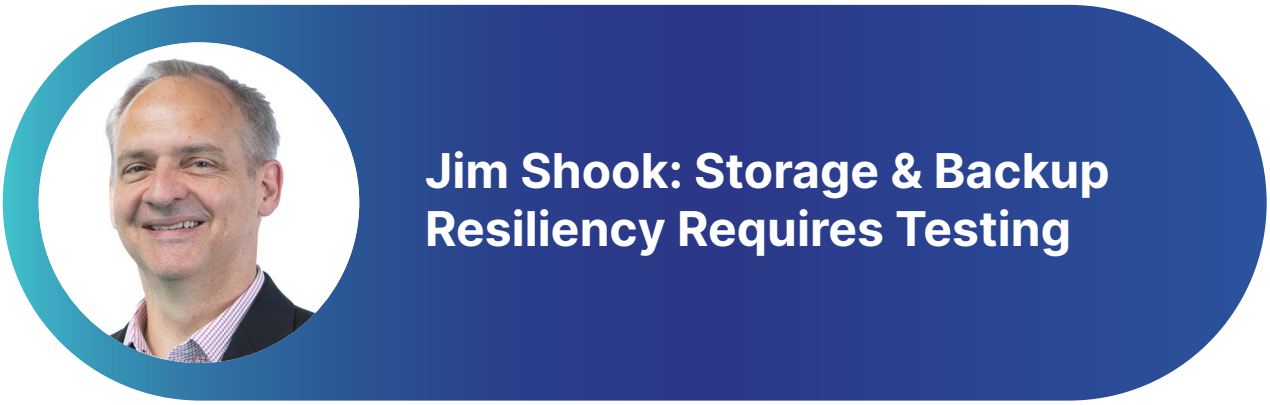
As stated by CISO Marc Ashworth, "for both the storage and backup environments, it's important to ensure that the proper controls are applied and tested." Ideally, this should be done whether or not the security team owns the security of storage and backup systems. Ashworth also advises CISOs, "testing your restores is critical, both from your offline access capabilities and of your online backups. Continuously monitoring the status of those systems is key – from an operational and a security component. This includes who is accessing it and looking for those anomalies within the environment to ensure its security."

Former CISO and security expert John Meakin gets the message across by stating, "if you're securing your production data but not properly securing your backups, it's a bit like putting half your money in the bank and the other half under your mattress! Its clear which half is insecure."

Chapter 4:
Best Practices & Recommendations

Backup breaches and storage vulnerabilities frequently make headlines nowadays. The risks are real and the consequences can be serious. Storage and backup systems are your last line of defense against cyberattacks.

This chapter explores CISO recommendations on securing storage and backups.



Cybersecurity and compliance practice director Jim Shook of Dell Technologies, advises CISOs, "It's great having backups, but are they secure? Have you tested them? You need confirmation that there's no configuration drift within your backup and storage environments. All those things require daily diligence." Shook also recommends that organizations "turn on your immutable capability in your backup environment. Even some imperfect immutability implementations on various platforms are better than none at all."

Shook also advises IT and security teams that they need to communicate effectively with leadership if there are challenges to testing storage and backup security. He states, "I still see this idea all the time that the executives aren't going to tolerate any data loss or any downtime after an attack. This is cyber recovery, cyber resilience. Organizations will lose data and have downtime. They have to accept that and then be able to build around it to figure out what the solution looks like." Communication and consistent testing can be key to storage and backup resiliency.

Joel Fulton: Today's Threat Actors Target Storage Systems

Joel Fulton, Former CISO at Symantec and Splunk recommends organizations put greater emphasis on their storage and backup security. As he states, "the most successful attacks over the last 1 to 2 years were either caused by attackers killing your storage or they stole it. It's the easiest way to take an organization down. It's the easiest way to take your data out."

Additionally he advises that security leadership needs to define and clarify the ownership of it. "If I think that IT has it, IT thinks that the SRE team has it, and the SRE team are confident that the business owners will have a way of recovering it, then we look like that Spiderman meme all pointing at each other. All the while our data goes out the window in the event of an attack," he states. Ultimately Fulton believes that it's imperative to verify that the proper controls are in place.

Fulton strongly believes that today's threat actors are more focused on breaching the most lucrative assets in an attack: data. One example he gives is of the famous bank robber Willie Sutton. "He was the most prolific thief in history and was asked why he robbed banks. His answer was attributed to because that is where the money is at. Most of that money was stored in the vault, that's where he went and that's where the most significant," states Fulton. Understanding that today's threat actors aim for where the data is stored is critical in order to enlist controls in order to better protect it.

Marc Ashworth: Security Controls & Testing are Critical

First Bank CISO Marc Ashworth recommends that organizations assess their security controls surrounding storage and backups, including testing them regularly. He advises organizations that "protecting backups is extremely important because if you do get hit by ransomware, your ability to restore is critical." Ashworth also cautions organizations that any backup systems are better than none at all. "Veeam has done a previous study that showed that 93% of all ransomware attacks target backups. Having that offline, off-network copy of your backups, where you can restore from – even if it's a couple days old is important."

Ashworth further emphasizes the critical need for proper backup system controls and testing. He advises organizations that, "whether it's the storage or the backup environment, you want to make sure you apply the proper security controls around them. You want to segment those systems off and possibly even micro segment it with MFA access. Testing your restores is critical, both from your offline capabilities and online backups."

Ashworth also stresses that teams must test the controls they have in place for their effectiveness. "Continuously monitoring the status of those systems - both from an operational and a security component, who's accessing them, and looking for anomalies within the environment are important," he states.

Additionally, he recommends that security and IT teams that operate backups communicate issues to leadership regularly. "It's critical to understand what risks are seen in their environment and what mitigation plans they need to implement. In either case, a 2-year plan or a quick fix must be communicated to the CISO. Communicating those risks to leadership and incorporating them into an existing plan can ensure proper mitigation of them," he states.

John Meakin: Storage & Backup Security Requires Multi-Team Collaboration

Former CISO at Standard Chartered, GlaxoSmithKline and Deutsche Bank, John Meakin recommends that CISOs clarify the ownership of backup and storage security as well as collaborate with IT if ownership is their responsibility. “Many security teams may not view backups yet as being one of the key assets at risk. And the IT infrastructure operation team may not consider the backups as being a key security mechanism. It is important to change both of those attitudes,” he advises.

Meakin also states, “Assets should include backups as much as anything on the frontline of the IT service you provide. I believe the significant thing is that the CISO needs to tell their security team that these are our crown jewels. CISO needs to tell the operations teams, these are very valuable assets you’re handling. It should be reinforced to both teams that it is imperative that we work together to secure them as much as we secure anything else.”

Ultimately data storage and backup systems can require multi-team collaboration in order to ensure controls and testing are done successfully. As the last line of defense for proper restoration and recovery, security of these systems are paramount for organizations globally.

Continuity's StorageGuard ensures your storage & backup systems will never be the weakest link in cybersecurity. Its comprehensive approach to the scanning of storage and backup systems offers complete visibility into blind spots, automatically prioritizing the most urgent risks, and remediating them.

StorageGuard verifies that your storage and backup systems are hardened, configured according to industry and vendor security best practices, and are not vulnerable.

CONTINUITY

www.continuitysoftware.com