The Storage Manager's Guide to Ransomware Resiliency

CONTINUITY

Author

Joel Reich

Former Executive Vice President,
NetApp

Part 1

Why Storage Managers Need to Prepare for the Ransomware Scourge

Certain parts of the enterprise are more concerned about ransomware than others. The security, networking, and help desk teams are very much in tune with the threat that ransomware poses on a daily basis.

Storage managers, however, don't tend to pay as much attention based on the belief that their systems lie at the backend and don't pose the same level of risk as other layers of IT. **Research from Continuity**, however, makes it clear that this is not the case.

An average enterprise storage device has 15 vulnerabilities / security misconfigurations. 3 can be considered high or critical risk. Therefore, it is vitally important that storage managers understand the magnitude of the ransomware menace and what they need to do about it.

Let's begin with a few facts about ransomware. An **Enterprise Strategy Group (ESG)** study found that cybersecurity has replaced cloud and artificial intelligence (AI) as the top area for IT spending. With almost two-thirds of organizations intending to increase IT spending this year, 69% said they are spending more on security this year compared to last. Only 2% said they will pay less for cybersecurity in 2022 compared to 2021.

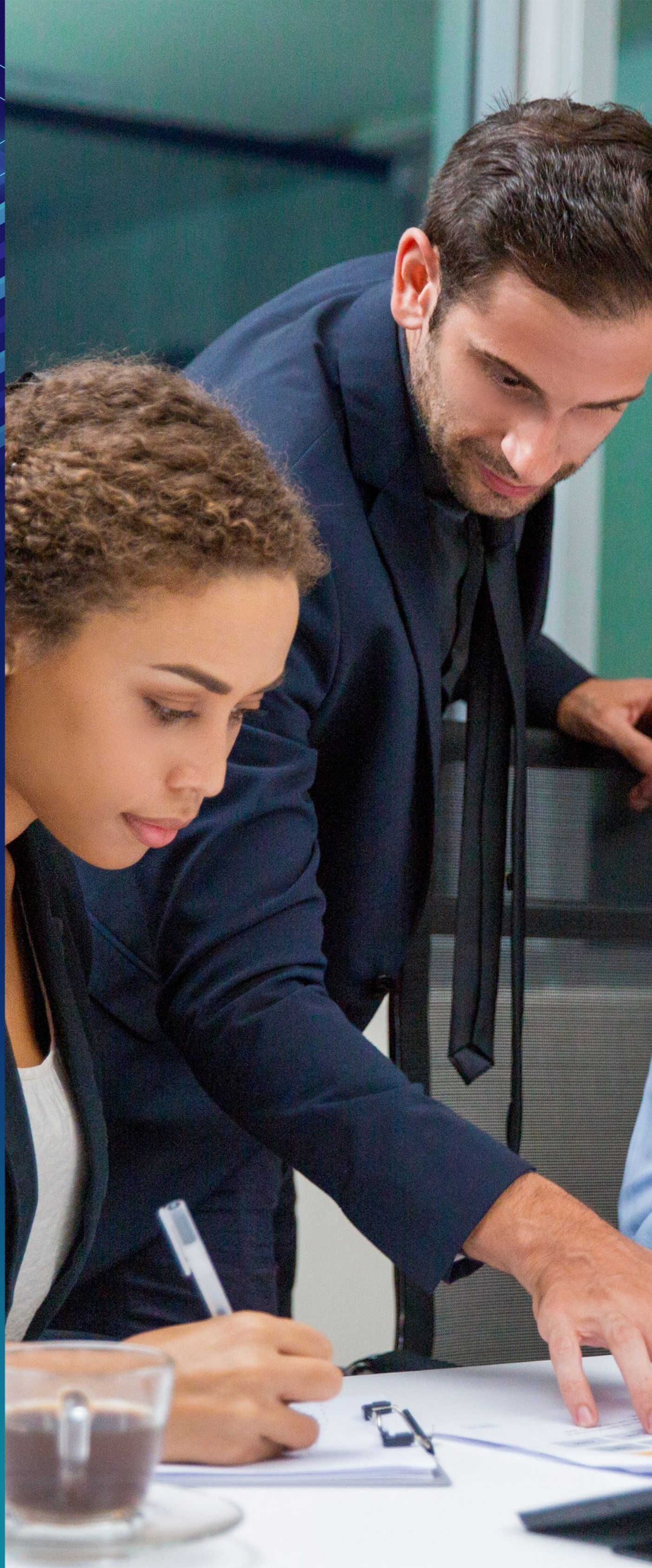
According to the study, 54% of respondents said the main driver of technology spending was the achievement of stronger cybersecurity and improved resiliency against cyberattacks. Why?

ESG discovered that 48% had been the victim of at least one successful ransomware attack. Two thirds of those attacked had paid a ransom to recover access to their data, applications, and systems.

Despite all the attention given to digital transformation, the transition to the cloud, and the need to deploy analytics and AI to extract real-time insights from organizational data, 22% of businesses named ransomware protection as their top business priority. Another 46% named it among their top five priorities.

These finding are corroborated by another research study by **Arcserve and Dimension Research**. It found that 50% of organizations worldwide had been targeted by ransomware. These attacks are continuing at a high frequency, yet most organizations are unprepared.

The financial fallout can be staggering. 20% of organizations reported that their organizations were asked to pay $1 million to $10 million. Another 35% faced demands of more than $100,000. Understandably, they are responding with higher investment in better security tools, managed security services, improved backup/DR, and training for personnel. 64% are spending more to upgrade existing security software and add new security applications.



False Sense of Security

These increases in cybersecurity investment are important. However, those numbers might lure storage managers into a false sense of security.

Historically, storage has been viewed as a discrete unit within IT infrastructure. The old silos between networking, security applications, development, compute, and storage may be diminishing, yet storage largely remains a separate unit, particularly in larger organizations or those managing a lot of data.

Added to that is the burden of responsibility that falls upon the shoulders of storage managers. It is heavier than ever. In modern IT, they are required to manage mountains of data with far fewer personnel than in the past. These two factors can sometimes make security and storage worlds apart. That needs to change.

Take the case of the many vulnerability scanning, configuration management, and patch management tools that currently exist.

Yes, they are great at inventorying and scanning networks, systems, operating systems (OSes) and enterprise applications. But they do don't do a thorough job on storage. Shockingly, they often miss security misconfigurations and CVEs (Common Vulnerability and Exposures) on storage systems.

Yet some storage managers continue to believe they are immune to ransomware and that systems from the likes of Dell EMC, NetApp, Pure Storage, and HPE are out of the reach of cybercriminals. Nothing could be further from the truth. Hackers are notorious for finding ways to obtain administrative privileges. Once they possess them, they can easily find their way into storage systems and wreak havoc.

The fact is that hundreds of active security misconfigurations and CVEs currently exist in various storage systems. Yet some storage managers are unaware of them. Our research shows that on average, about 20% of storage devices are currently exposed. That means they can be attacked successfully by ransomware.

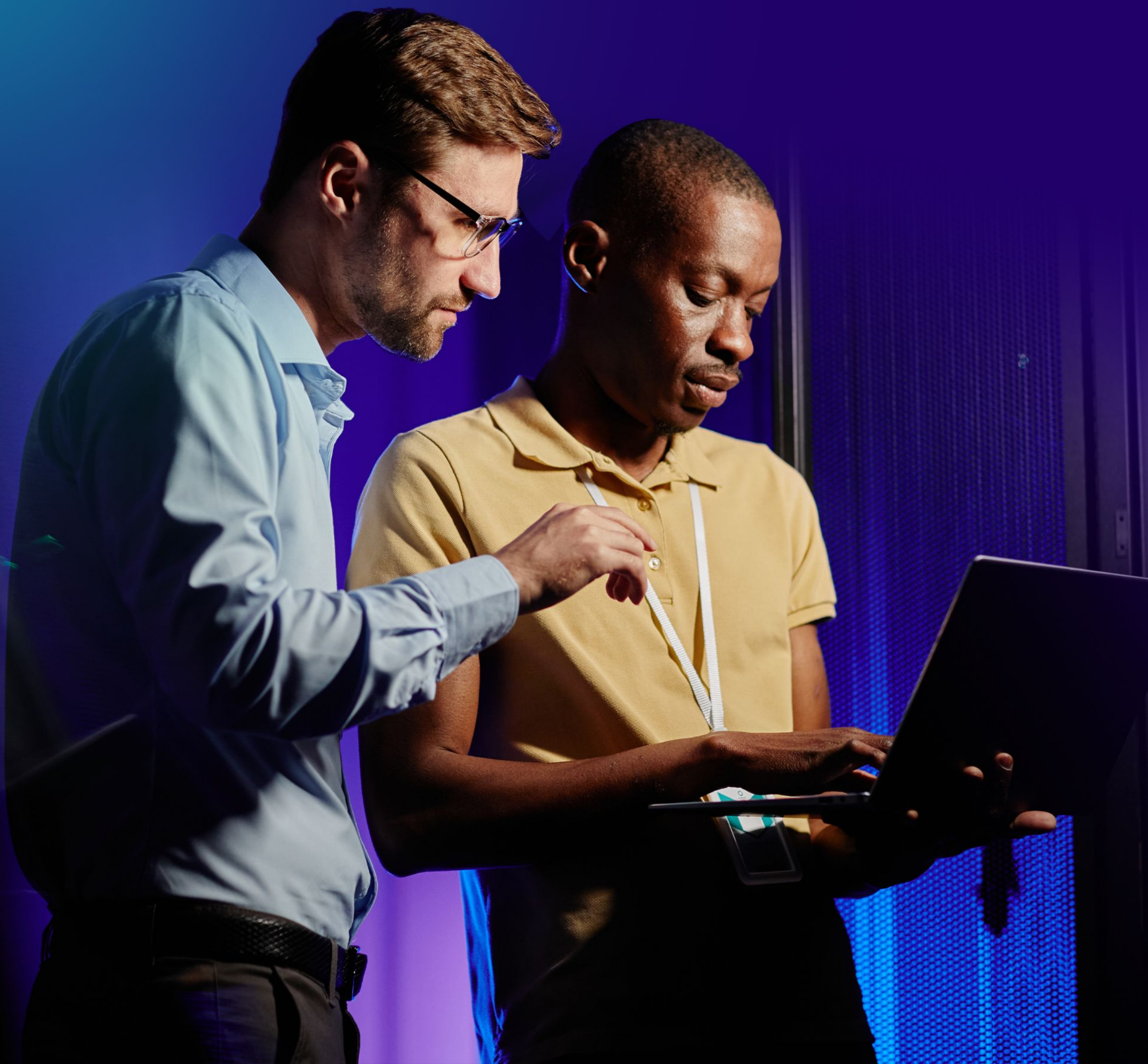
Part 2

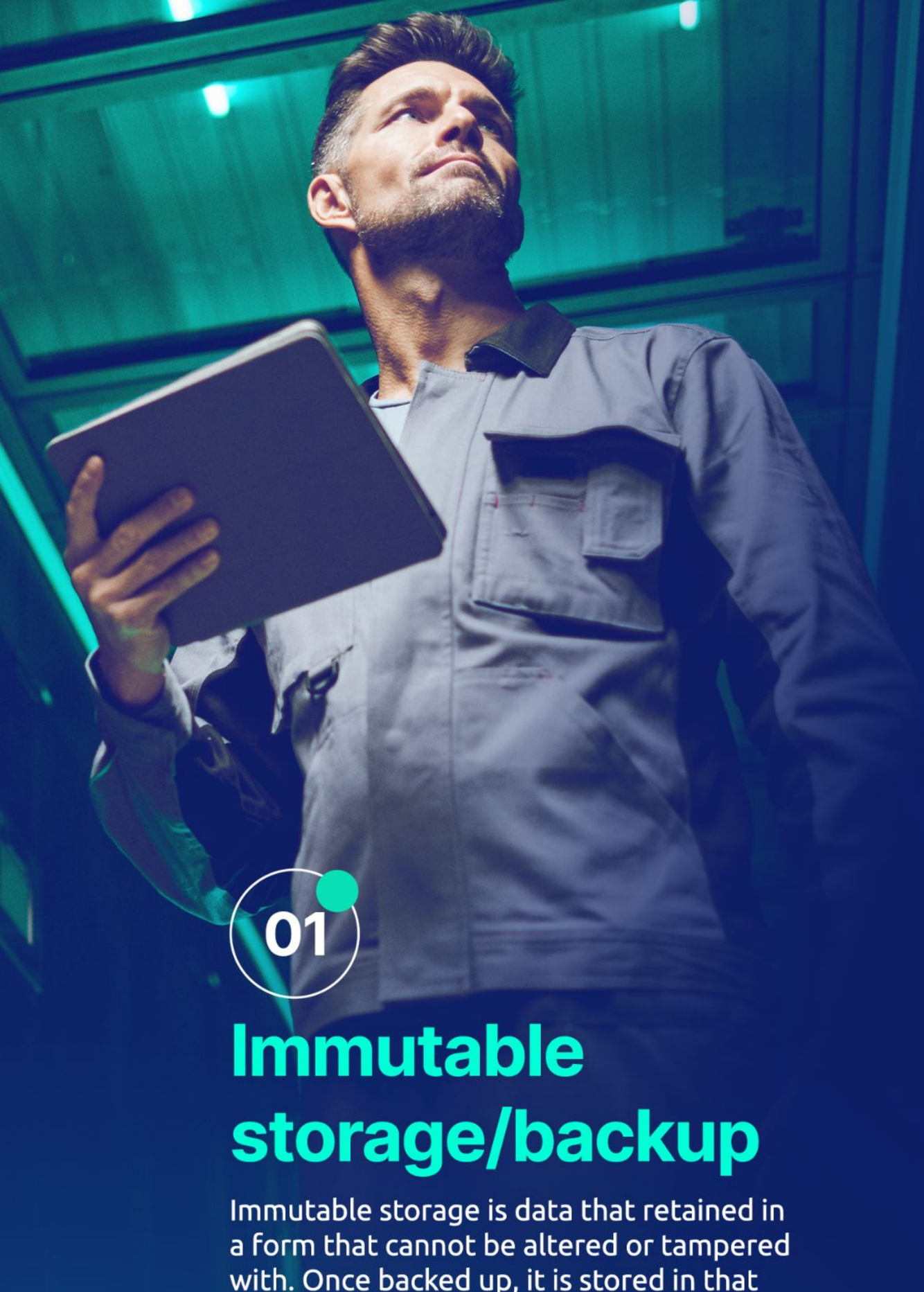
How Storage Managers Can Achieve Ransomware Resilience

Various surveys make it clear that the rising frequency of ransomware attacks is steadily eroding confidence in being able to cope. **Almost 60% of respondents are not confident in their ability to recover from a ransomware attack**.

How should they deal with the problem?

Here are 6 ways organizations can improve how they detect and prevent ransomware attacks, how to mitigate the impact if they suffer from one, and how they can recover their data.





01

Immutable storage/backup

Immutable storage is data that retained in a form that cannot be altered or tampered with. Once backed up, it is stored in that same format and can't be changed. It can be implemented on tape, disk, SSDs, or in the cloud as a defense against ransomware. Some tools even incorporate machine learning features that can detect any signs of interference from ransomware.

02

Snapshots and replication

Replication is about sharing data between redundant resources, such as software or hardware components or between servers or data centers to provide fault tolerance and business continuity. If one server goes down, the other holds the same data, for example. Snapshots are typically used in replication to provide near-instantaneous data protection. Point-in-time copies are replicated to other systems. If data is loss, they can be used to rapidly restore it. Backups, too, can be transmitted to an offsite location using replication.

03

Network Segmentation

Network segmentation is a tactic that can greatly reduce the impact of a ransomware attack. By separating the network into smaller, distinct areas, the spread of a malware is minimized if one area is compromised.

04

Data Vaulting and Air-Gapped Solutions

Data vaulting is a good way to avoid the possibility of ransomware infecting backup files. Cybercriminals increasingly target backup environments with ransomware as a way to guarantee the success of their extortion attempts. Vaulting addresses this via air gapping i.e., a copy of the backup is kept offline, separated from other systems. This is best achieved via tape backups that are retained offline. As there is no physical connection to the internet, ransomware has no chance of infecting it.

05

Data security

Data security is about protecting valuable data. There are different procedures, standards, and technologies to choose from.

These include encryption (in transit and at rest), file scanning, malware detection and prevention, network security such as firewalls, intrusion detection, data privilege, access management, and more.

Their goal is to ensure that only authorized parties can access and use the data and that its integrity is maintained at any given moment.

06

Storage and Backup Security Posture Management

There are a great many patch management and vulnerability management tools out there. They continually scan networks and systems for security risks. They do a fine job with operating systems (OSes) and enterprise applications. However, they often miss security misconfigurations and vulnerabilities in storage and backup systems.

There are currently thousands of active CVEs out there that relate to storage and backup systems. They can be used to exfiltrate files, initiate denial-of-service attacks, take ownership of systems, block devices, and delete data. Overall, about 20% of storage devices are exposed and can be attacked successfully by ransomware.

In fact, many organizations fail to configure immutable backups properly – possibly the result of insufficient understanding of the technology and its limitations. This allows adversaries to compromise those backup systems.

Continuity's **StorageGuard** was designed to comprehensively scan all data storage, storage management, storage networking, and backup systems to look for security misconfigurations and vulnerabilities. It offers enterprises complete visibility into storage and backup security blindspots, automatically prioritizing the most urgent risks. As the industry's only security posture management solution for storage and backup systems, it provides:

VISIBILITY.

For the first time, detect all security misconfigurations and vulnerabilities in your storage & backup systems

PRIORITIZATION.

Act upon your most urgent security misconfigurations and vulnerabilities, where you're most at risk

PROTECTION.

Ensure all your storage & backup systems can withstand ransomware and other attacks, to prevent data loss

COMPLIANCE.

Guarantee storage & backup systems are compliant with security regulations and standards

StorageGuard also complements data security and file-based security solutions. Files eventually are stored within storage devices. If you break into a storage device, you can still delete, alter or block all files stored within the device – even if those files are encrypted.

Discover how secure your storage & backup systems are.

Click here for a free trial of StorageGuard.

CONTINUITY

www.continuitysoftware.com