EVOLVING SOLUTIONS

CYBERSTORAGE - A BLUEPRINT FOR PROACTIVE DATA PROTECTION & RECOVERY

CONTENTS

INTRODUCTION

Modernization has pushed the envelope of what organizations can accomplish with technology. Meanwhile, threat actors have stayed a step ahead by taking advantage of nearly every technical and human vulnerability they can leverage to disrupt business and government.

Especially since the pandemic, when endpoints became a popular target of attack, threat actors have begun to use automation to attack more organizations faster. And if they get the chance to learn about your environment, they'll go after your most sensitive, business-critical systems and data, which underlie every technology you have.

In what appears to be a never-ending cycle, bad actors are relentlessly exploiting vulnerabilities to steal, delete, or encrypt data, oftentimes to extract a ransom in return for restoration, which may or may not happen. **If a serious incident occurs, you may not get your data back.**

Organizations need to take a *'defense in depth'* approach against ransomware and other cyberattacks, especially as malware becomes increasingly sophisticated.

- Dave Pearson,
Research VP, Infrastructure, IDC

And while data is unavailable, your organization is actively losing revenue and may suffer reputational damage, which could be severe enough to affect the valuation of your company. There's no limit to the possible impact of a cyberattack.

The result of the current risk environment is that new operational resilience guidelines and regulations are being put into place that require organizations to prove they can withstand a cyberattack. Stiff fines are in store for any organization that can't comply — up to $10 million or more.

Now, more than ever, there is a need for integrated data security and protection. Dave Pearson, Research VP, Infrastructure, IDC, says, "Organizations need to take a 'defense in depth' approach against ransomware and other cyberattacks, especially as malware becomes increasingly sophisticated."

This is why we believe organizations need a Cyberstorage approach to protect data and withstand a cyberattack. **Cyberstorage is an important layer of the defense-in-depth approach to data resilience that wasn't available until recently.**

WHAT IS CYBERSTORAGE?

In September 2023, MGM Casinos suffered a disabling attack, which the company estimated had a $100 million impact. Threat actors gained access by convincing the MGM helpdesk to give them a password. In other words, the hackers bypassed human security controls to launch an attack. It took weeks for the company to get back to normal business operations.

According to the International Monetary Fund, cyberattacks are inevitable. It's not a question of if, but when. Given the global scope and fast pace of attacks, most organizations can count on enduring a significant cyberattack every 2-3 years.

When all else fails, you need a process and a plan to restore critical operations as quickly as possible — in hours instead of days or weeks. Pearson says, "Storage infrastructure is another layer where cyber resilience can improve to speed ransomware detection, reduce the spread and impact, and accelerate recovery."

Cyberstorage is a framework for protecting data when all else fails. Cyberstorage is part of an overall cyber resilience strategy that addresses security and data resilience.

According to Gartner, Inc., Cyberstorage protects storage system data against ransomware attacks through early detection and blocking of attacks and aids in recovery through analytics to pinpoint when an attack started. The company reports that all storage products will include Cyberstorage capabilities by 2028, up from 10% in early 2023. The company says most major vendors and innovative startups are currently working on incorporating Cyberstorage capabilities into their products.

WHY YOU NEED CYBERSTORAGE

Over the years, data has become increasingly important to organizations. According to "Achieving Business Impact with Data" from McKinsey & Company, "Data is generated by everything from cameras and traffic sensors to heart rate monitors, enabling richer insights into human and "thing" behavior. As a consequence, data has become the new corporate asset class."

"As data becomes embedded in every decision, interaction, and process, managing data effectively and ensuring data privacy will be crucial," McKinsey & Company states in its "Data Driven Enterprise of 2025."

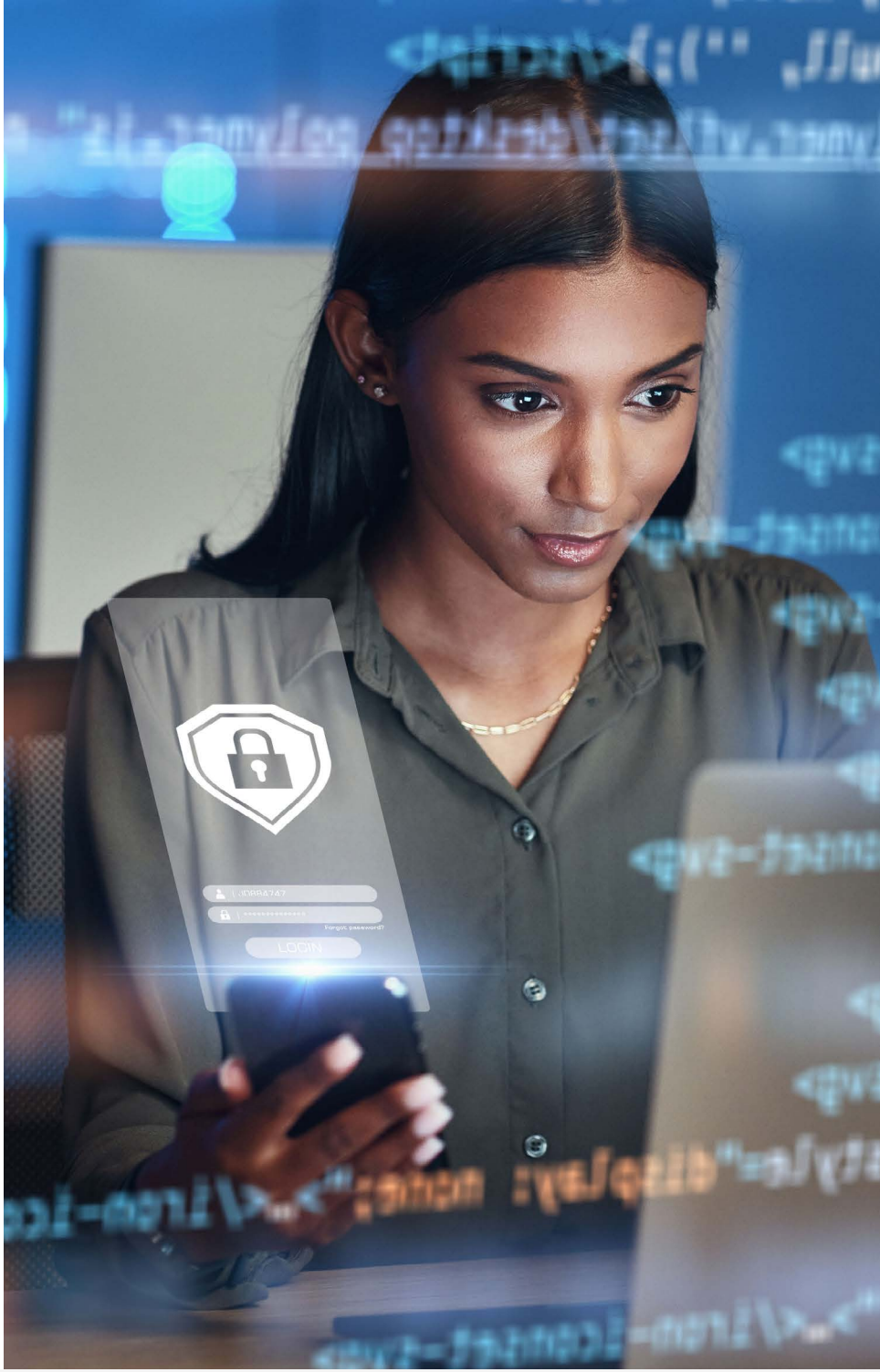
And, as enterprises become more reliant on data, vulnerability increases, which increases the importance of having a modern IT operations environment that has a Cybestorage approach at its core.

Ten or more years ago, resilience for storage was about creating backups as part of a disaster recovery (DR) strategy to restore operations during a natural disaster, loss of connectivity due to an accident, or other unforeseen circumstances. Events like this only happen every 25-50 years. While most companies have a DR plan, the chances of actually using it are low.

We've seen situations where organizations try to use their recovery techniques to restore a system or a file, only to discover that the recovery plan doesn't work. Until recently, storage has been a "set and forget" type of solution, where organizations haven't had the time to test recovery processes, ensure that the storage appliances are in good working order, or ensure that snapshots and backups are taking place and are recoverable.

Today, a cyberattack is a statistical inevitability. Within the next 3-5 years, the chances of your organization needing to respond and recover from an attack is nearly inevitable. So, the industry is evolving to address this very real risk.

Now that threat actors are actively targeting data in storage, it's become necessary to have automated processes for data resilience that include faster data recovery — the ability to recover in minutes rather than days or weeks. This will minimize risk when incidents occur.



HOW CYBERSTORAGE SUPPORTS MODERN OPERATIONS

Modern Operations supports business continuity and resilience to ensure reliable, available, and secure IT operations across hybrid cloud environments. Because storage is the basis for data availability, Cyberstorage is crucial to maintaining a secure, reliable environment.

Observability is fundamental to Modern Operations and includes the ability to automate the detection of system anomalies. What's new with Cyberstorage is the ability to detect anomalous behavior right at the flash drive itself. If, for example, the flash drive detects unauthorized encryption, it will shut down access to the array immediately. Without Cyberstorage, it could take hours to correlate an alert from a detection tool to problems with storage, requiring IT teams to restore hours of corrupted data. Cyberstorage detection and response happens immediately. **So, Cyberstorage enhances and complements the work of other detection and cybersecurity tools by providing additional automated detection and response.**

Data availability and protection is also a key pillar of Modern Operations, and Cyberstorage is all about having the data you need available when you need it. Once an event has been detected and contained, Cyberstorage provides a framework for quick recovery because your critical systems have likely been targeted. A serious business impact may be looming.

Another pillar of Modern Operations is automation, which enables IT teams to automate operations, including automated cyber resilience. If a network breach is detected, for instance, automation can immediately take storage offline or immediately take a snapshot, so you have a record of the data before the attack has the opportunity to progress.

And in a world where a breach is a statistical certainty, automation also enables fast recovery, which protects business continuity, revenue, and the organization's reputation. Cyberstorage gives you a framework to automate recovery and ensure speed.

HOW TO ACHIEVE RESILIENCE WITH CYBERSTORAGE

Cyberstorage is the last line of defense. When threat actors can bypass your controls to get unauthorized access to your systems, you need a way to detect data alteration and an automated way to restore the last known clean copy of data.

Invest in Resilient Storage Devices

Cyberstorage works best when system design and architecture support overall resilience. Malware and ransomware aren't the only risks. Physical data center failures can impact the business, too. The storage itself must be resilient and available under normal operating conditions. If a single drive failure brings down the whole storage array or a single workload suddenly hammers storage so hard that it brings down other workloads, you have a resilience issue.

In addition, if snapshots are on the same storage array as corrupted data, then not only is the current real-time data compromised, but all the historical data as well.

IBM recently released a new version of its storage platform, IBM FlashSystem, which has always placed the workload for compression and encryption on the drive rather than the RAID controller. However, now, IBM has enabled the drives themselves to actively examine the IO characteristics of the writing process to detect and shut down unauthorized encryption.

This is a crucial level of detection and response in situations where a threat actor is actively in the system trying to encrypt data for ransom.

Update Your Processes

While Cyberstorage draws on decades of industry experience in making backups, backup processes must be modernized to support it. Backups must be tested to ensure they work, and backup scheduling and retention should be modernized to ensure that data for recovery is fresh enough to keep the business running.

Real-time recovery using Cyberstorage requires having clean, tested copies of data always available for restoration to recover right at the point of corruption. Strategies and processes for backup need to be modernized to support this capability.

Your Biggest Storage Vulnerability Isn't Technical

While most cybersecurity point solutions are sourced and managed within the four walls of IT, a data resilience approach requires a wider scope of input from across the organization. That's because when a cyberattack threatens business continuity by rendering data inaccessible, it affects the whole organization more profoundly than a compromised endpoint or account. The entire enterprise is actively creating and managing data as part of their work, so everyone has a stake in what IT does to recover from an attack.

Cyberstorage is a copy/backup/restoration ecosystem that serves the needs of all stakeholders, including senior management, compliance officers, middle management, sales, operations, and front-line workers, along with your applications team, virtualization team, security team, IT operations team, and storage team.

You can't solve for this at the storage level alone. To restore the business quickly, IT professionals need to know how workloads support different business functions, such as revenue generation and operations, and how to prioritize restoration when an attack compromises storage. If you hand Cyberstorage off to the storage team, you'll get a solution that works great for them but may not be useful in restoring the business when the time comes.

IBM STORAGE DEFENDER - A COMPLETE CYBERSTORAGE SOLUTION

The baseline for recovering from an incident includes complete sets of data stored as immutable copies. An immutable copy can't be changed, even by an administrator, and can't be altered by criminals. The immutable copies should be air-gapped from the production environment to ensure they're not accessible. Air gapping can be done logically or physically.

But true resilience goes beyond the baseline. A complete Cyberstorage strategy includes evaluating the quality of copies to ensure that backups can actually restore operations.

IBM Storage Defender is an all-encompassing solution for Cyberstorage that supports processes for data immutability with IBM Safeguarded Copy and quick restoration using IBM Cyber Vault.

The platform is designed to integrate with existing SIEM (security information and event management), SOAR (security orchestration, automation and response), EDR, NDR, and other detection, automation, and orchestration platforms to help organizations improve their ability to detect and respond to cyberattacks and other adverse conditions.

Immutable Backups with Safeguarded Copy

After a cyberattack occurs, you don't want to discover that your snapshots are corrupt or missing. Safeguarded Copy from IBM provides immutable points of data recovery — point-in-time snapshots of data that are protected from being modified or deleted due to user errors or cyberattacks. Safeguarded Copy can take up to 500 snapshots of any individual volume to back up your entire storage.

The IBM Cyber Vault Framework for Quick, Reliable Restoration

Fast-moving ransomware attacks can spread throughout your infrastructure in minutes or seconds leaving IT staff with no time to respond. Snapshots taken after an attack will contain the errors or malware you want to eliminate.

Safeguarded Copy enables nearly instant recovery of immutable copies to IBM Cyber Vault, an environment to do forensic analysis on snapshots to test for corruption and identify the most recent uncorrupted version safe for recovery. Once validated as good, a snapshot can be stored as a backup to be used for recovery.

The automated system also mounts and runs workloads in a test environment to ensure they work before being identified as good, restorable copies. The goal is to have a complete copy of your production environment ready to restore when needed.

Automation and Orchestration with Cyber Vault

A common goal among businesses and IT departments is to be agile. Much of this is done through automation to compress the time to value for extraordinary customer service and a competitive advantage.

The ability to recover from an attack must be equally agile, which is why Storage Defender includes capabilities for automation and orchestration — key components of a successful Cyberstorage initiative. All steps in the backup, validation, and recovery processes should be automated and tested so that, at any given time, the organization has a clean copy of data that can be restored in minutes.

Storage Defender helps automate every step of the process:

- Take snapshots at a predetermined frequency
- Validate that snapshots are free from malware or corruption
- Identify the last best snapshot for recovery
- Test that the identified snapshot will boot and run its workload
- Restore the validated snapshot to production
- Lock up the validated snapshot as an immutable copy

WHAT TO EXPECT FROM A CYBERSTORAGE APPROACH

By designing and architecting your storage strategy using tools under the IBM umbrella, organizations can raise their level of competence and be assured that their data is secure and available. And in the event of an incident, a well-developed Cyberstorage strategy will give organizations confidence they can be up and running without significant impacts on business operations and continuity.

Early Detection

When a cyberattack or physical data center failure occurs, time is of the essence. The earlier you detect it, the more you can contain the problem and get ahead of what could become a catastrophic compromise. Cyberstorage gives organizations the ability to detect attacks or physical failures with storage before they threaten to cripple the business.

Faster Restoration to a Tested Copy

Manual processes for restoration can take weeks. Cyberstorage is designed to restore corrupted or deleted data in minutes for surgical restorations and hours for catastrophic restorations.

Reduced Complexity for IT

The automation that enables early detection and fast restoration also reduces complexity and workload for IT personnel. Reduced complexity enables IT teams to focus on getting ahead of an attack instead of wondering how to do it.

Improved Compliance

More customers, industries, cyber insurance companies, and governments expect organizations to prove resilience. It's only a matter of time before noncompliance with resilience standards will result in heavy fines and penalties or a lack of insurance. Cyberstorage is a pathway to compliance for resilience.

More Confidence

Many organizations spend significant amounts of money to get a feeling of security through large-scale disaster recovery and replication projects. Cyberstorage provides its own proof that your systems are resilient to catastrophic events, giving organizations more confidence that their systems are safe and that business continuity isn't at risk.

HOW EVOLVING SOLUTIONS CAN HELP

Storage, data protection, and cybersecurity are deeply embedded in our company's DNA. This makes Evolving Solutions uniquely able to help organizations develop and implement a Cyberstorage approach and solution that will work for its entire lifetime using a proven methodology to successfully bridge the worlds of cybersecurity and Cyberstorage.

We can help you determine Cyberstorage's role in your overall cybersecurity strategy and help you identify and implement the integrations needed in your environment. We can also help you implement automation capabilities that will reduce complexity and workload for your IT teams and help you make good choices in balancing performance with resilience.

And through our work and relationships with IBM, we know what it takes to help organizations build a Cyberstorage strategy using IBM Storage Defender and how to integrate the platform with your existing cybersecurity and storage technologies.

PEOPLE SIMPLIFYING TECHNOLOGY

Our team members are among the most experienced in the industry. We bring together our industry expertise with real-world experience with organizations of all sizes and complexities. This gives us a unique understanding of our clients' challenges and the outcomes they want to achieve.

ABOUT EVOLVING SOLUTIONS

Evolving Solutions helps clients modernize and automate mission-critical applications and infrastructure to support business transformation. We provide consulting services and technical solutions to enable Modern Operations in a hybrid cloud world.

www.evolvingsol.com

EVOLVING SOLUTIONS

IBM Platinum Partner

Let us help you get started down the right path to Cyberstorage that protects your organization and provides the resilience that you need.

Let's get to work!