myota™

Who Has Your Back(up):

The Shifting Landscape of Data Security

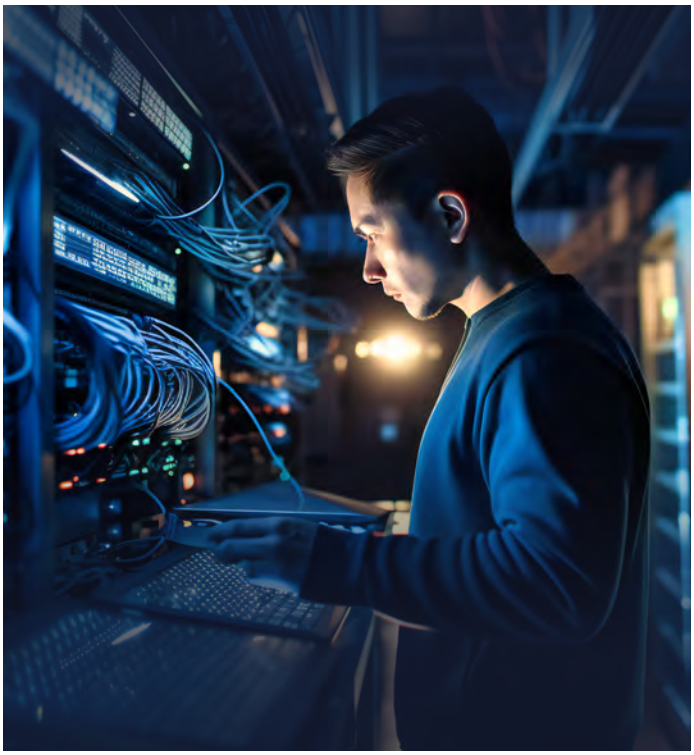
September 2024

Who Has Your Back(up):
The Shifting Landscape of Data Security

Data insecurity has become a matter of life and death for individuals and organizations alike, and most IT systems are ill-equipped for the inevitable. In what's been described as the largest data breach ever, the April 2024 breach of the National Public Data database exposed nearly 3 billion U.S. social security numbers on a dark web forum. From social media giants to telecommunications companies to healthcare providers, traditional data protection strategies aren't keeping pace with the aggressive innovation of nefarious hackers.

Sabotage aside, modern IT systems are becoming increasingly at risk of unintentional error or malfunction as they grow in size and complexity. The more reliant tech systems become on cloud-based systems and third-party supports, the more vulnerable they are to data disasters like the CrowdStrike update error that precipitated a global tech outage.

From global corporations to local school systems, the stakes have never been higher. The scary truth is that the average organization entrusts its data to legacy security protocols that have not kept pace with the growing complexity of its operations, much less the accelerated innovation of bad actors. The good news is that innovators in the tech security space are reconceptualizing data protection and reducing vulnerabilities by filling the gaps between reactive failsafe measures and preemptive safeguards.



3-2-1: Deconstructing the legacy backup and recovery strategy

A long-held convention in data protection, the 3-2-1 approach has served us well: three copies of the data, two of those copies saved on different media types, and one copy held in off-site storage. Although costly and time-consuming, the strategy has been simple and effective against physical threats like internal technology failures, natural disasters, or human error.

Adaptations of the 3-2-1 system allow for variation in the number of storage media types and locations. Limiting to a single media type (3-1-2) can reduce cost but compromises system agility. Doubling or tripling off-site storage locations (3-2-2 or 3-2-3) enables greater data recovery capacity, but it comes at a higher storage cost and makes the data subject to more off-site exposure.

As an organization's IT system grows in complexity, the simplicity and effectiveness of the 3-2-1 strategy and its variations diminish. Data set sizes increase, and the feasibility of the multiple-backup approach to data security becomes a system of diminishing returns.

From physical vulnerabilities to digital threats

As long as the risks remained physical in nature, the three-copy-backup approach to data security has been an effective—albeit costly at times—strategy to protect an organization's data. But the digital age has introduced a higher order of data vulnerability and, with it, significantly higher stakes. A report released last year revealed that the average company downtime after a cyberattack is 22 days, and the financial cost of that downtime can be as much as 50 times the ransom amount.

Of course, the cost is significantly higher in cases where the ransomed data is irrevocably destroyed or—worse still—released to the public. If organizations entrusted with regulated personal data fall out of compliance with data privacy laws, they expose themselves to severe penalties and legal liability. For government agencies, healthcare authorities, and educational systems where regulated personal data is held in high volumes, stakeholders responsible for IT security shoulder an incredible responsibility.

Ransomware became a $1 billion business last year, so it's fair to say the traditional multi-copy, multi-site backup approach to data security is no longer serving its intended purpose. The new reality is that, although every organization is successfully backing up their data, they're not all successfully recovering that data after a cyber-incident. Nefarious actors go beyond stealing your backups; they target those backups with the goal of ensuring the company can never recover it.

22 days the average company downtime after a cyberattack

Rethinking the CIA triad

Modern solutions to data security reconceptualize the standard three pillars of data protection: confidentiality, integrity, and availability. The CIA problem, as it is commonly known, is generally solved with encryption and immutability technologies to address the confidentiality and integrity risks, respectively. The availability problem is solved as long as the data backup is stored offline.

When it comes to digital threats, encryption and immutability are the trusted solutions, but they carry significant caveats:

Encrypted data can be re-encrypted
Your data doesn't have to be readable to be attractive to bad actors. Stealing your data and making it available to the public is only one form of cyber-attack. Your encrypted data has ransom value as soon as it is rendered unusable by you.

Traditional immutability can be bypassed
Unfortunately, even if an immutability solution is in place, hackers can find their way in. Permissions, privileges, and access control vulnerabilities in backup management systems are one primary way. Accidental governance and compliance misconfigurations are another. And then, some organizations get attacked from within; a disgruntled employee with access to the data source would be able to gradually poison the data without detection.

These solutions address the CIA problem, but security breaches continue. Why? It has to do with how the problem is solved. When confidentiality, integrity, and availability are treated as three distinct solutions, an attacker can pick them off one at a time.

A shift from successful backups to agile recovery

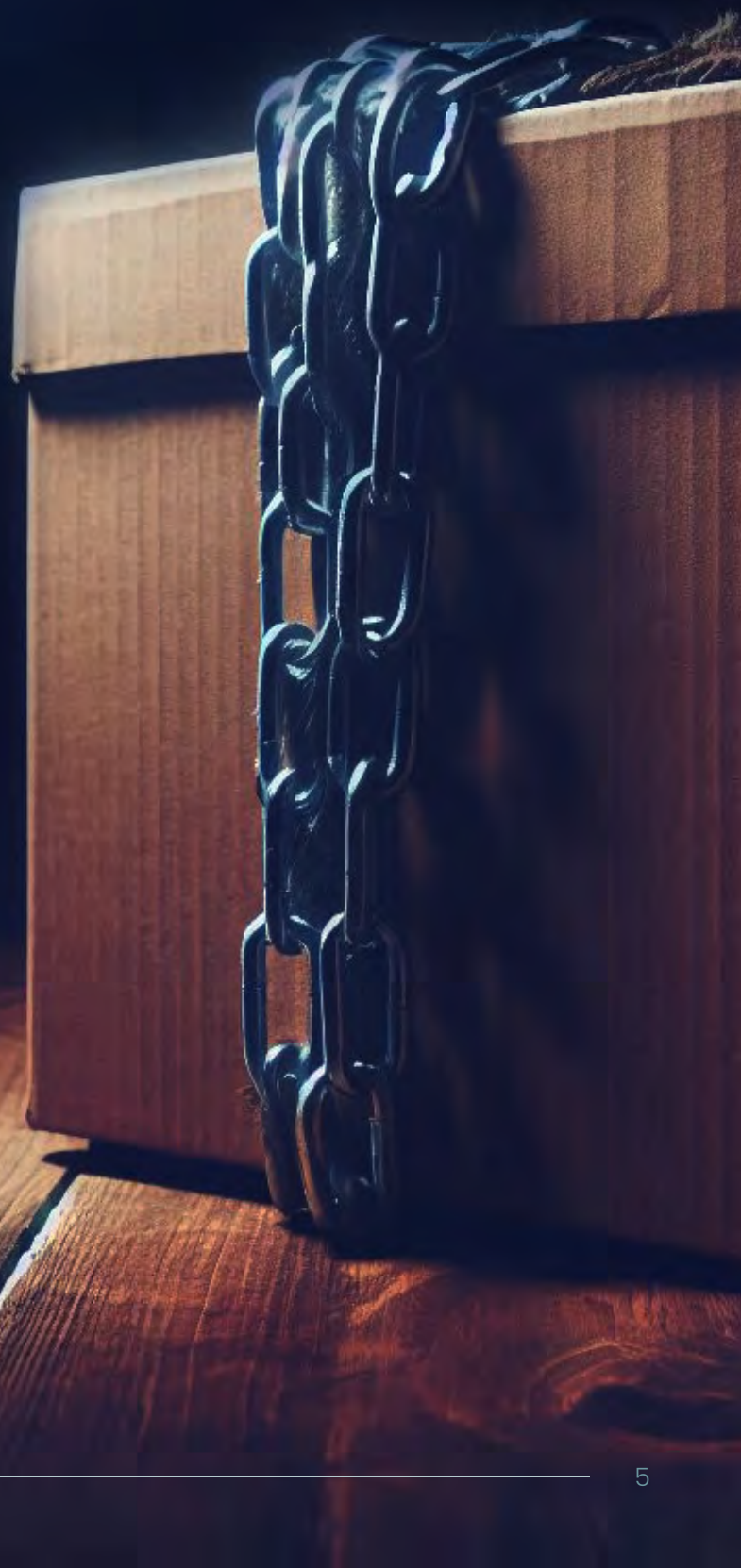
True data security does more than safeguard your data against nefarious activity. It also minimizes downtime, restores confidence, and protects the organization against reputational harm. That's why modern security protocols address both backup and recovery.

Security and IT engineers are already wise to the reality you can't survive on backups alone, but the recovery strategy is the piece that many companies are missing. An effective data recovery strategy streamlines the process of getting your data back in action. By prioritizing the data restoration flow, it can enable an efficient resumption of business activities.

For most organizations, the extent of their recovery strategy is a periodic backup testing schedule. A regularly scheduled backup test will always work under controlled conditions, providing a false sense of security. What it doesn't tell you is whether that backup has the resilience to withstand an unforeseen event like a ransomware attack.

Few organizations are addressing questions like:
What happens if the recovery environment is attacked?
What happens if the recovery orchestration platform itself is attacked?

The chain game: Who really has control of your data?



The crux of the matter is that backups are an IT control, but they are not a security control. The current state of data security is a process of relying on data backups—an IT control—to solve a security problem. Data gets stored in an IT storage product, and then a security product is attached to the storage system. It's like keeping your valuables in a cardboard box and then wrapping a big chain around it. The box is effective for storing and organizing, but it won't prevent the bad guys from stealing its precious contents. Worse yet, attackers can put an even bigger chain around your chain, effectively locking you out of your own box. Now, not only is your data vulnerable to theft, but you've also lost access to it—compromising both the confidentiality and availability of your data.

Of course, it's better to have a chain on a cardboard box than no chain on that box. To carry the physical analogy further, you may think of a vault as the next step in security. Even more secure would be to divide those valuables into separate vaults and then store the vaults in separate places—a diffusive approach,

What does 100% data security and recovery even look like?

As ransomware and other cyber threats evolve, the possibility for an organization to have a security breach has shifted from threat to inevitability. Likewise, the stance of data security service providers has shifted from reactive to pre-emptive. We can no longer rely on backup and recovery solutions to protect against cyberattacks because they were never built to do so.

Here at Myota, we've used our years of experience as ethical hackers to develop an approach that eliminates not one but all pathways to cyberattacks. We've achieved this by unifying the problem of confidentiality, integrity, and availability into one comprehensive solution, as opposed to three distinct components.

How? Myota secures your data by encrypting it, sharding it into tiny pieces like digital sand, and spreading it across multiple storage nodes, rendering it 100% useless to unauthorized access or breaches.

We've taken the hacker's eye view and looked at the data security and recovery from the outside in, starting with the availability of data, moving through its vulnerability to being stolen or corrupted, and ending at the value that data holds for the organization. Our innovative solution has taken security to a new level in the following ways:

Vaulted availability
Myota's solution airgaps all changes to the data, so it is separated from the administrative level where permissions, privileges and access control vulnerabilities exist.

Enhanced immutability
Our Shard & Spread™ technology eliminates a common attack vector by removing networked access to data. There is no key infrastructure to target, and hackers can't even exploit code to breach the data because it is reduced to worthless components.

No privileged access
By employing zero trust architecture to separate the data from the Myota shards, we block potential attackers from having knowledge of the location—or even the existence—of the sharded data.

Multi-layer encryption
Our end-to-end encryption includes zero-knowledge protocol, so no single Myota shard holds enough data to rebuild your information. In the unlikely event of a breach, the shard would be worthless to the attacker. Zero-knowledge protection means not even Myota can hack your Myota-secured data.

Myota's innovative approach takes data security beyond traditional strategies that leave your backed-up data vulnerable to re-encryption and immutability bypass scenarios.

Re-evaluating the costs of backups

Data security is a non-negotiable, even when you're working with a finite budget. Keeping pace with anti-hacker technology while sustaining organizational backup requirements is a mounting financial challenge for CISOs. Myota's solution provides the alternative to costly duplicative backups and complex security solutions.

The traditional 3-2-1 backup approach requires three volumes of identical data—that means the cost of replication, transition, egress, and API transaction fees every time that data is updated or moved around. Add to these expenses the cost of storing three copies of data.

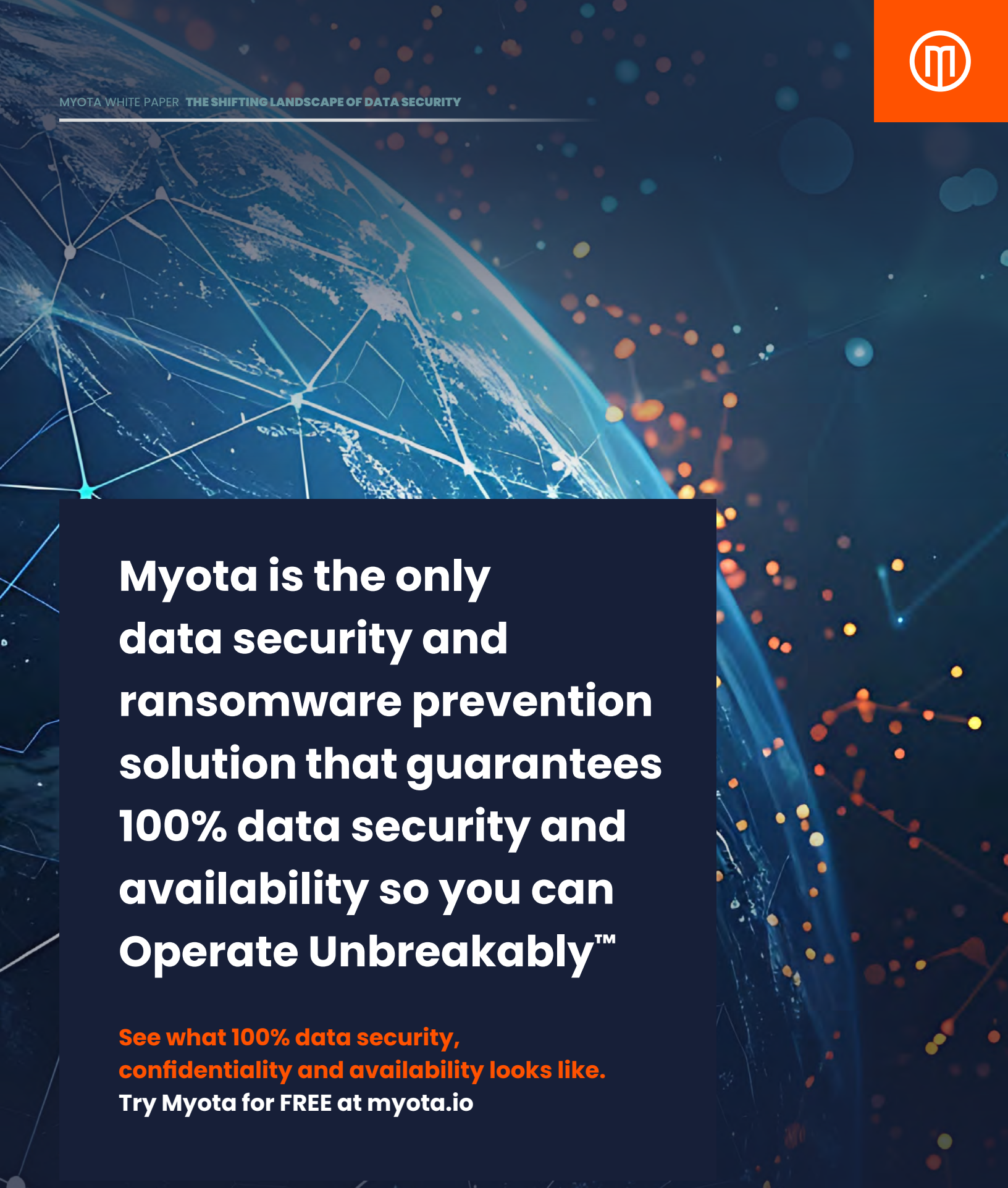
Traditional multi-copy backup solutions were a reasonable investment—back when they worked. Today, larger data loads and more sophisticated digital hazards have weakened the cost-benefit ratio of legacy backup systems.

For decades, IT infrastructures have relied on costly—not to mention cumbersome—storage and retrieval solutions. Myota has created a more agile and cost-efficient solution, fit for the next era of data security. Our system shards the encrypted data, divides it into four distinct components—each worthless to cyber-attackers—and disperses them for separate storage. Myota enables you to store 100% of the original data in one copy only but holding it securely in four pieces. We provide next-level data protection with no need for three full backups and all the associated costs.

The future of data security: guaranteed recovery

Data disasters are as certain as bad weather. That's why, if I could set a motto for the future of data security, it would be guaranteed recovery. As much faith has been placed in backup processes and systems in the past half-century, that's how much faith should now be placed in recovery systems. Failures of recovery are the reason why people are paying ransoms, they're the reason why some companies never get their stolen data back. Backups are necessary, but recovery isn't guaranteed.

In traditional security practices, the IT backup system was central, and the security solution was grafted onto it. Advanced security technology says: what if, instead of strapping a security system onto your IT infrastructure, data recovery could be baked into its DNA?



Myota is the only data security and ransomware prevention solution that guarantees 100% data security and availability so you can Operate Unbreakably™

See what 100% data security, confidentiality and availability looks like.
Try Myota for FREE at myota.io