northdoor
Store IT · Protect IT · Use IT

Air-gapped backups: a last line of defence

Northdoor helps business defend against ransomware and other cyber security threats with innovative cyber recovery solutions.

No network perimeter security can ever be 100% effective. No organisation can absolutely protect itself against accidental or deliberate damage to data or systems by employees or partners. No matter how good your cyber security policies and technologies, vulnerabilities will always remain.

While the headlines naturally focus on high-profile losses — such as the £600 million impact of NotPetya malware on Merck — the reality is that organisations of all types and sizes are at risk. Research by ESG suggests that 43 percent of breaches involve small businesses, and a cyber attack takes place on average every 39 seconds.

A well-designed backup and recovery solution can provide good protection against errors made by business employees or IT staff, enabling you to roll back to a known good version of data. But what happens when sophisticated malware also targets those backups?

With an air-gapped backup solution from Northdoor, you gain:

- A last line of defence against ransomware and other malware
- Automated checks on the integrity of your backed-up data
- Intelligent tools for rapid recovery in the event of a cyber breach.

Cyber security breaches are a matter of “when”, not “if”. Don’t leave the security of your business to chance: contact Northdoor to arrange a free initial consultation about our cyber recovery solution.

Immutable data storage

Organisations of all kinds are already largely dependent on reliable access to shared data for normal operations. And as digital transformation continues, the degree of dependence will only increase. This means that a single sufficiently serious cyber attack can represent an existential threat. Ask yourself: how long could we stay in business without access to key systems and data?

The number and diversity of cyber security threats are constantly increasing, from vandals using paid malware to ethical “hacktivists”, and from disgruntled employees with insider access to nation states employing cutting-edge technology. Whatever your organisation does, it’s important to recognise that you’re in the crosshairs too. Research by Dell EMC suggests that 82% of organisations have already suffered a cyber breach on a production system.

Traditionally, organisations have assumed that they can turn to their data backups if disaster strikes. However, backup and recovery environments are also vulnerable to attack, not least in organisations that have invested in sophisticated cross-site replication.

When data is automatically replicated from one data centre to another, corrupt data and malware are also duplicated. Malware typically sits undetected for 200 days on average, giving it plenty of time to infect multiple copies of your data.

What's more, a growing number of cyber attacks specifically target both the backup data and the backup catalogues — that is, the records that make sense of the backups and enable them to be recovered rapidly and selectively. In many organisations today, the backup catalogue has no effective defence against encryption or destruction.

To address this risk, organisations need a way to back up data so that it can't be changed — an immutable backup — together with the ability to understand when production data has been corrupted. This requires you to create an off-network vault where your most important data can reside outside of normal backup and recovery processes. And built into this vault, you need automated tools to prevent the entry of malware and to help with rapid, targeted recovery of known good data.

Cyber recovery from Northdoor

According to a 2019 McKinsey statistic, more than 40% of cyber security breaches stem from insider threats. Given that the backup infrastructure in most organisations is easily accessible from the corporate network, this represents a major risk, highlighting the need for an off-network location in which to maintain "golden copies" of your most important data.

When considering a cyber recovery solution of this kind, Northdoor recommends you focus on five elements:

- Solution design: Identify the critical data sets and applications, and determine the appropriate recovery time and point objectives (RTOs and RPOs).
- Data isolation: Create an environment that is separate and unconnected to corporate and backup networks, and restrict user access to it.
- Automated copying: Store immutable copies of data in a secure digital vault, and design processes to create an operational air gap between your main network environment and the vault.
- Intelligent analytics: Achieving high-speed recovery depends on understanding what data has been corrupted, so you need automated integrity checks to determine whether vaulted data has been affected by malware.
- Rapid remediation: Design workflows to enable rapid post-incident recovery through dynamic restore processes.

At Northdoor, our approach starts with a thorough analysis of your current environment to help you identify the data you need to protect, and then to size and deploy the appropriate solution. We partner with leading global technology vendors to offer air-gapped solutions that combine immutable backup, replication, recovery, deduplication, instant access and restore, search and analytics.

For more information

Contact Northdoor today to learn more about our Cyber Recovery solution and to arrange a free initial consultation.