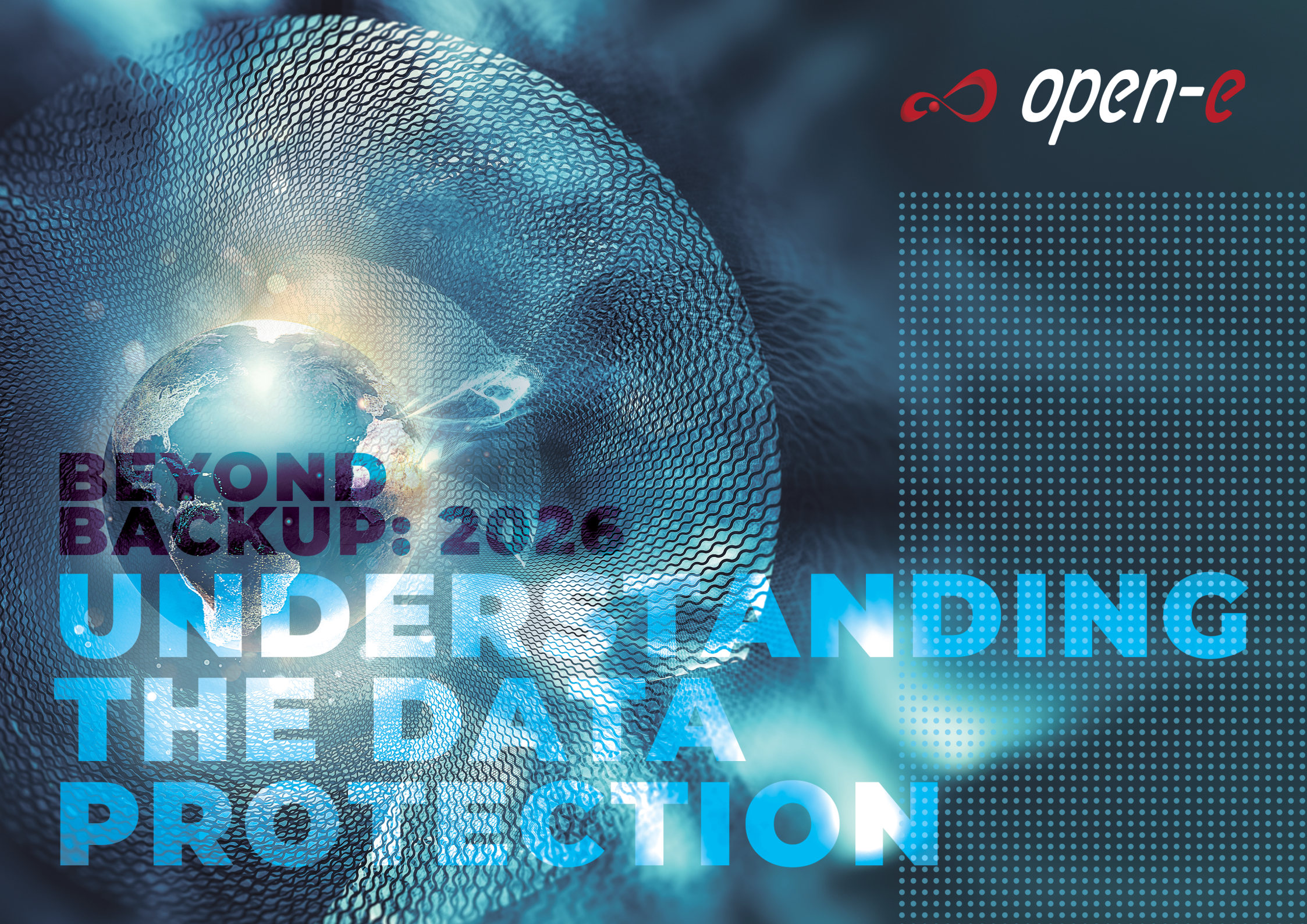
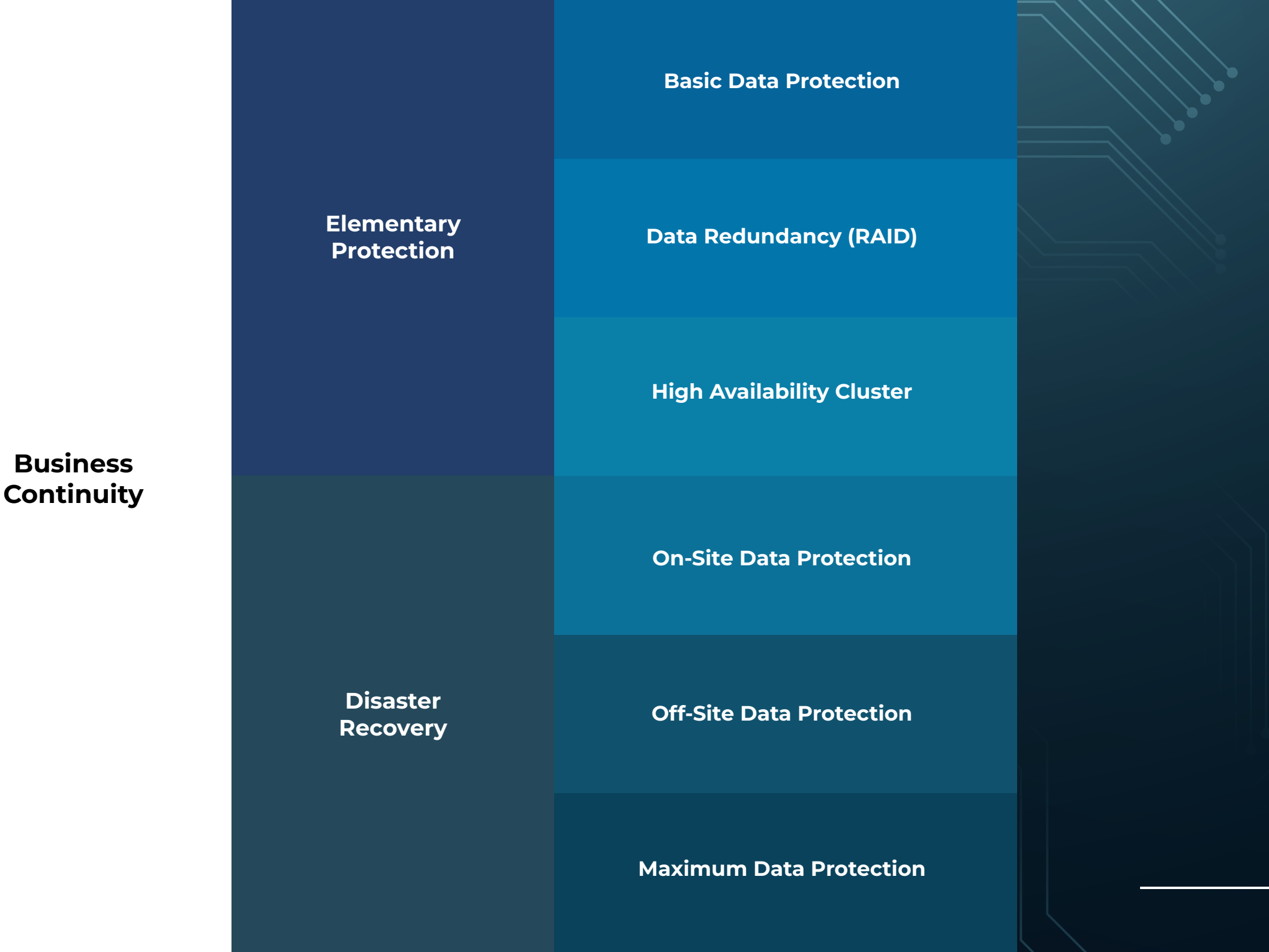

open-e
BEYOND BACKUP: 2014
UNDERSTANDING THE DATA PROTECTION


Business Continuity
Elementary Protection
Disaster Recovery
Basic Data Protection
Data Redundancy (RAID)
High Availability Cluster
On-Site Data Protection
Off-Site Data Protection
Maximum Data Protection

Understanding the Data Protection in 2026

In today's tech-driven world, where technology touches every aspect of our personal and professional lives, having reliable backups is more essential than ever.

The term ‚backup' comes from the verb ‚to back up,' meaning to support or assist, perfectly reflecting its role in our lives. A backup is essentially a copy of anything you consider important, created to safeguard your valuable data against unexpected events like tech failures, natural disasters, or other unforeseen threats.

Considering we're constantly surrounded by data, backups have become a crucial necessity for anyone who stores digital information. This is especially true when it comes to businesses, where data protection is vital.

In this document, we'll explore the world of backups in depth. Let's get started.

"In recent years, our world has encountered unprecedented challenges. At Open-E, we've witnessed firsthand the struggles that our partners and customers face amid continuing market shocks. The data storage industry, including many of our clients, has not only had to adapt to the new realities brought about by geopolitical tensions, but has also navigated through hardware shortages, soaring tariffs, escalating Energy crises, and the ensuing economic downturns. These events, reminiscent of the proverbial horsemen of the Apocalypse, underscore the critical need for robust, reliable data backup solutions." **Kristof Franek, CEO at Open-E.**

Backup Statistics

- On average, all tape drives fail at some point, which implies that they do not provide absolute protection for your data in the event of a natural calamity, fire, or terrorist attack that destroys your office and everything in it. The entrepreneurs who were affected by natural disasters such as Hurricane Katrina learned the importance of keeping remote backups of their data. (Source: VaultLogix)
- Within one year of a disaster, **93%** of companies that experienced data loss for ten or more days went bankrupt, with **50%** of them filing for bankruptcy immediately. (Source: National Archives & Records Administration in Washington DC.)
- Every five years, **20%** of small to medium-sized businesses are predicted to encounter a major disaster that results in the loss of essential data. (Source: Richmond House Group).
- Due to outdated software, misconfigurations, inadequate security protocols, and other factors, cybercriminals can successfully penetrate **93%** of company networks. What is more, 50% of companies will not even notice whether they've been attacked or not. (Sources: GartnerGroup & Keepnet)
- An estimated average drive failure rate is **100%**. Why? It's no surprise – all disks have their limits and all will eventually fail. (Source: VaultLogix)
- It has been stated that only **34%** of businesses run tests of their tape backups. What is more, **77%** of those who run such tests found failures. (Source: VaultLogix)
- Unfortunately, more than **50%** of companies that encounter data loss will be forced to close down. (Source: VaultLogix)
- More than **50%** of critical business data is stored on desktop computers and laptops that do not have adequate protection in place. (Source: VaultLogix)
- The main reasons for data loss include:
  - **78%** Hardware or system malfunction
  - **11%** Human error
  - **7%** Software corruption or program malfunction
  - **2%** Computer viruses
  - **1%** Natural disasters
  - **1%** Other

  (Source: VaultLogix)
- Around **30%** of businesses have not yet established a disaster recovery program. Two out of three feel that their existing plans for data backup and Disaster Recovery are vulnerable to significant issues. (Source: VaultLogix)
- The average cost of a data breach in 2024 was estimated at $4.88 million (Source: Cost of a Data Breach Report, IBM)
- By 2025, the global cost of cybercrime is projected to reach $10.5 trillion, growing at a rate of 15% annually. (Source Secureframe)

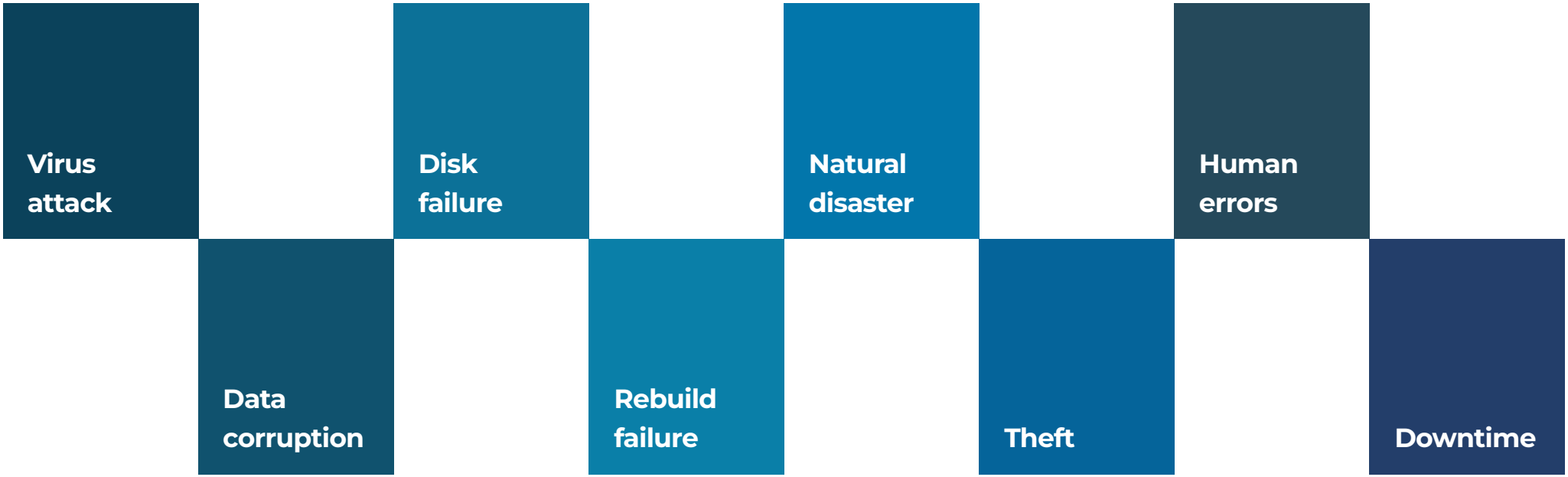
So...

Why Does Your Company Need Backup?

Have you ever wondered how often and why you should do a data backup?

If not, ask yourself a question: "*How much of my work can my company afford to lose, and how fast do we need this data back?*".

The answer seems obvious.



Backup solutions protect your investment in data, usually by keeping several copies of them. With this many copies, having one that is destroyed seems like not a problem. Your data is precious and it will cost you plenty of time and probably even more effort to recover it to avoid data loss consequences.

Data Loss Consequences

- **Financial Loss:** lost business opportunities, the cost of recovery efforts, customers litigation whose data is lost or exposed, and empty-handed employees who still must be paid.
- **Reputation Damage:** it harms an organization's reputation and credibility with customers, partners, other stakeholders, and negative publicity.
- **Legal and Regulatory Consequences:** legal and regulatory penalties for failure to protect sensitive information, such as personal data (i.e., GDPR in the European Union, CCPA in the United States). It can result in lawsuits from individuals or organizations whose data has been lost or exposed.
- **Loss of Intellectual Property:** losing valuable intellectual property, such as trade secrets and proprietary information.
- **Decreased Productivity:** employees struggle to access the information they need to perform their jobs effectively. Relevant departments may have to spend time recreating information which can take away from other important tasks.
- **Unavailability of Essential Information:** which can impact the ability of an organization to make informed decisions, delays in operations, employees may be forced to rely on inaccurate or outdated information, which can result in decreased accuracy and quality of work.

So the main objective for backup is to provide **Business Continuity** by **Data** and **Disaster Recovery.**

Layers of Data Protection

Depending on your company's business needs you can set the relevant Business Continuity procedures for your data storage infrastructure. It is crucial to understand the threats you can face and to be aware of any detail of your infrastructure that needs to be considered before choosing different data storage features. First of all, it's crucial to analyze how and why you store data. To do so, write down all the business processes related to storing data in your company.

- **Which data is critical for your company operations and keeps your business up and running?**
- **Which data is not so important but still necessary to maintain long-term operability?**
- **Which data is irrelevant, meaning you can get rid of it or reduce its costs as much as possible?**

If you answered all these questions, you just started building your Business Continuity Plan. Congrats!

But before you continue to create it, let's **inspect the specific data storage protection features** and the levels of infrastructure security you can achieve using them.

STARLINE

Starline's Flexible Data Storage Solution with Open-E JovianDSS

The NASdeluxe 5724R/Z Data Storage Solution is a part of Starline's 5000 Z-Series which provides a cost-effective and highly available unified storage solution for small and large businesses. It can be used for multiple purposes, including virtualization, VDI, databases, media streaming, and backup. The solution also grants great storage performance, an unlimited number of snapshots and clones, thin provisioning, or compression with deduplication of data. The NASdeluxe 5724R/Z comes in a 4U rackmount case with 24 LFF slots and can be extended with additional interfaces to create a tailored enterprise solution.

Starline
Germany

Basic Data Protection

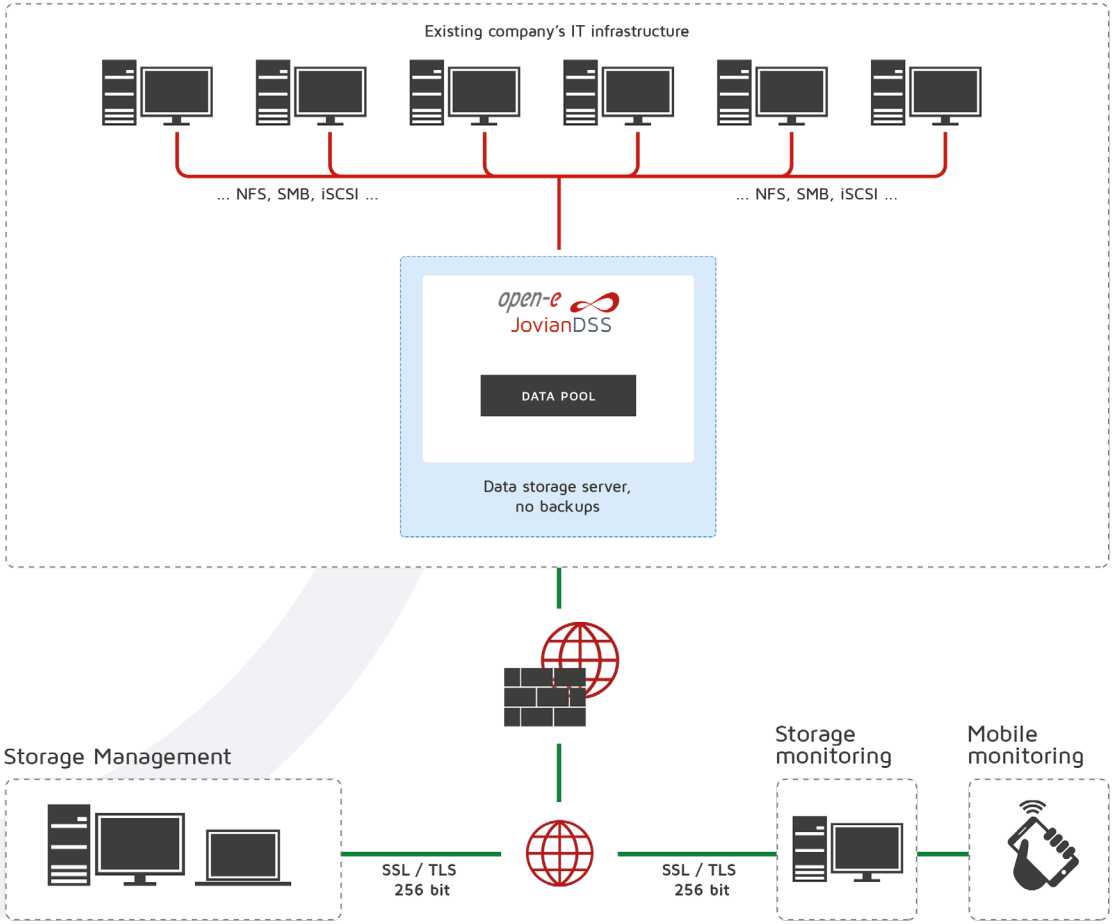
The main things you need to prepare yourself are **silent data corruption** (which can happen in every data storage medium type), **acting against virus attack consequences** (i.e., ransomware), and **human errors and actions**, which are still one of the main reasons for most system failures. The first can be avoided thanks to a **self-healing feature** provided by a ZSF-based software like Open-E JovianDSS. **Snapshots**, on the other hand, protect you against virus attacks and human errors or other actions consequences because there is always a possibility to bring back the system state from before the security accident happened.

No matter what's the relevance level of your data, you would need to keep it secure even on the most basic level, against the:

- **Silent-data corruption**
- **Human error (one of the main reasons for data loss for years) caused by accidental data removal, or deliberate employee action**
- **Ransomware attack effects**

Both are the **basic built-in Open-E JovianDSS options**, so if your data storage has a low priority, you can consider it sufficient. It can work with very simple data storage setups, like a single node server - nothing more, hence the low price of maintaining it.

However, there are some **disadvantages**. From the file system perspective, your data is protected. But the protection is critically dependent on the hardware you use. Once it fails, your data is lost. There is no backup of your data. You won't be able to rebuild the system, so be aware that data loss can be irreversible.



+ allows for recovery with snapshots (access to previously saved data)
+ gives you the possibility to choose snapshot frequency
+ self-healing
+ fast snapshot rollback
+ low costs
– doesn't save you from natural disasters
– doesn't save you from on-site storage unit failure
– no RAID rebuild
– doesn't prevent downtime

WARNING: While it is a cost-efficient solution that protects data against the most common data threats like human error, ransomware attacks, and silent data corruption, the hardware you use is a single point of failure that can lead straight to data loss. **It is not an actual backup, and no Disaster Recovery is provided.**

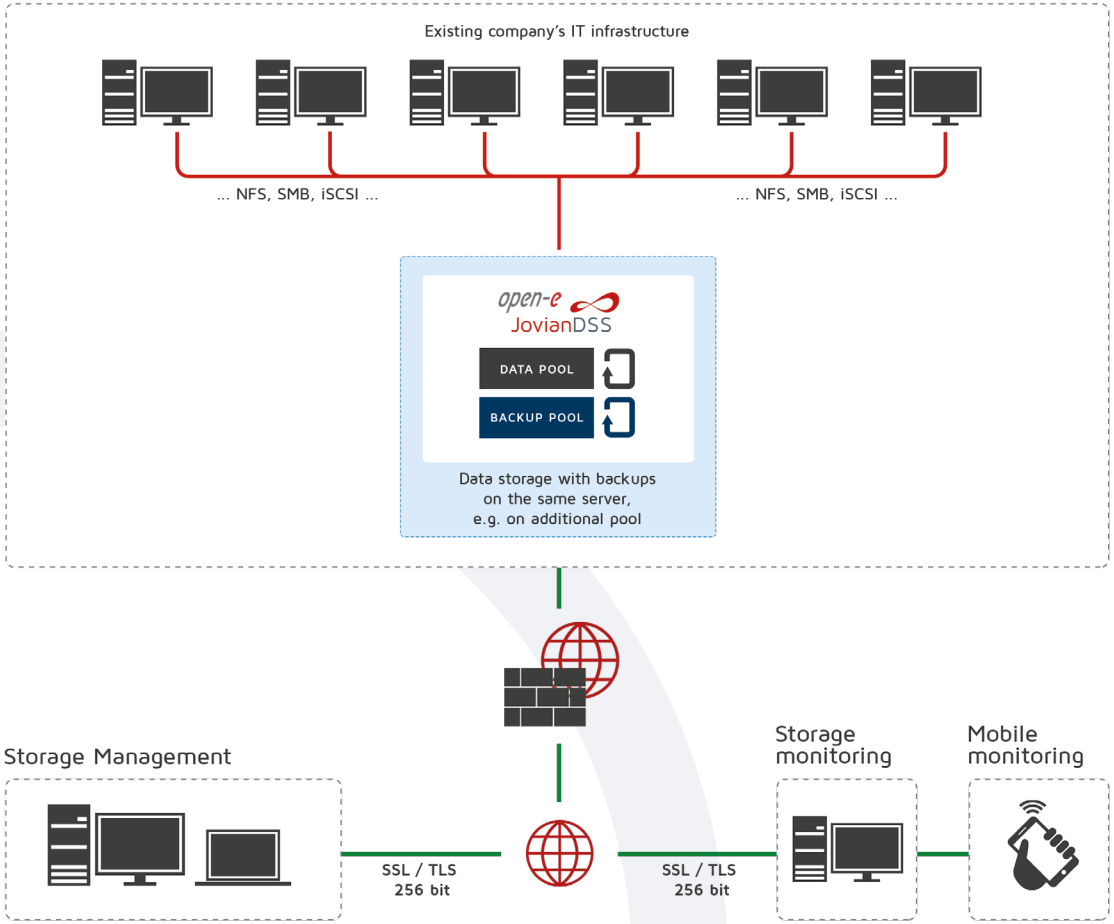
Data Protection with Basic Data Redundancy

If you run a **small business** that **focuses on minimizing the total cost of data infrastructure** and your transaction systems are not business-critical, **it can be enough to have a data storage system that provides the basic data redundancy to protect against:**

✓ **Data drive(s) failure**

How to achieve that? The elemental data protection that uses **the production server with the pool built of chosen RAID level** seems sufficient in this case. Securing data **against the consequences of a ransomware attack** with **snapshots, self-healing, protecting from the silent corruption** still works, but this way you can achieve much more! RAID protects you against losing one or more drives, depending on how your array is built. The possibility of building your data pool with RAIDs allows for data redundancy, so in case of losing some information from the drive or the drive itself, you can always rely on the parity data to restore it.

Using a higher RAID level (i.e., Raid 5 or Raid 6) protects you against losing more drives from the pool. It's up to you to decide how important these data are and how much you wish to spend on additional drives. Once establishing it, you can decide on choosing a particular RAID build.



+ protects with snapshots (access to previously saved data)
+ gives you the possibility to choose snapshot frequency
+ self-healing
+ disk failure (RAID)
+ RAID rebuild
+ fast snapshot rollback
+ low costs
– doesn't save you from natural disasters
– doesn't save you against on-site storage unit (and backup pool) failure
– doesn't prevent downtime

WARNING: Bear in mind that there's no protection against system failure or location issues protection (power outages, disasters, and human action or errors that affect the disk array as a whole). So if you lose your array - you lose your data and a chance to retrieve it. This security level is still not sufficient for most real-life business purposes. **It is not an actual backup, and no Disaster Recovery is provided.**

High Availability Cluster

What if your business process also requires protection against the failure of more drives that your RAID level supports?

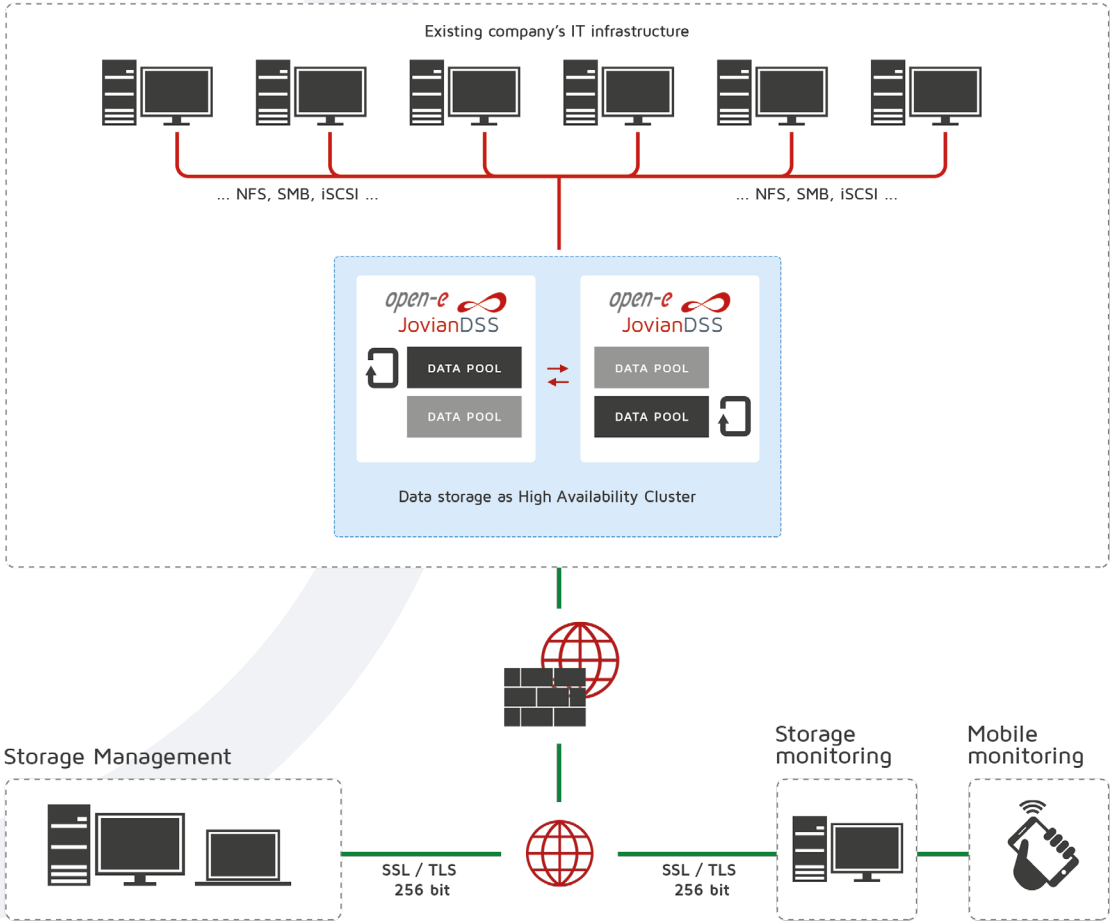
If something wrong happens to your server built with one node, you will lose all your data kept there. Well, there's a higher level of data security, which is a **high availability cluster that protects you against:**

✓ **RAID failure (on production node)**

It is built with at least **two nodes connected locally or remotely,** using the shared- or non-shared data storage architecture. **Retail, hospitality,** or just **small- and medium-sized businesses** that apply this to their data security infrastructure ensure Business Continuity by providing uninterrupted access to data even during hardware failure and maximizing the hardware and network resources utilization.

Note that **this is still not an actual backup** because you don't keep the data elsewhere. Moreover, **losing the cluster is going to cause irreversible data loss.** The hardware is also **exposed to disasters or harmful and intentional human actions** (i.e., theft) that may cause the whole cluster unavailability because of its location at your place of business.

However, there is a **solution Open-E JovianDSS gives** you to work it around - **non-shared storage stretched cluster.** It requires an additional node placed elsewhere at a maximum distance of 50 miles (80 km) from the main node (in case of point-to-point fiber optic connection) to mirror the data between each other. Actually, it can be even more when using an additional switch between nodes if provided network latency will not exceed 5 ms. So because the second node is located somewhere else, **you don't need to worry about your data availability, even in the case of a fire or flood.**



+ protects with snapshots (access to previously saved data)
+ gives you the possibility to choose snapshot frequency
+ self-healing
+ disk failure (RAID)
+ RAID rebuild
+ fast snapshot rollback
+ system failover
+ may prevent downtime
− doesn't protect you against natural disasters
− doesn't protect you against on-site storage unit failure

WARNING: Implementing this to your data security allows managing the production server functions available by the additional node while restoring the first one in the background. It's possible because data is shared between both nodes constantly, hence, the higher level of protection. It's the first step to provide the maximum data security. However, it needs to be implemented with on- or off-site data protection to equip your infrastructure with proper backup. **Remember that no matter if a non-shared storage stretched cluster is used it's still not an actual backup. Also, Disaster Recovery is not provided, but no worries - we're getting close to that.**

Business Continuity vs. Disaster Recovery

In the previous part, we focused on the **Business Continuity** procedures for your data storage infrastructure that relate to the threats you can face and aspects you need to evaluate once you choose different data storage protection features. But even the best data security methods can't make you 100% sure that disaster or another unfortunate event won't happen.

That may lead you to a situation where **Disaster Recovery** must be applied so the business can continue all its processes as fast as possible. So, how to ensure that you're appropriately prepared to recover from a disaster? Let's focus on that now.

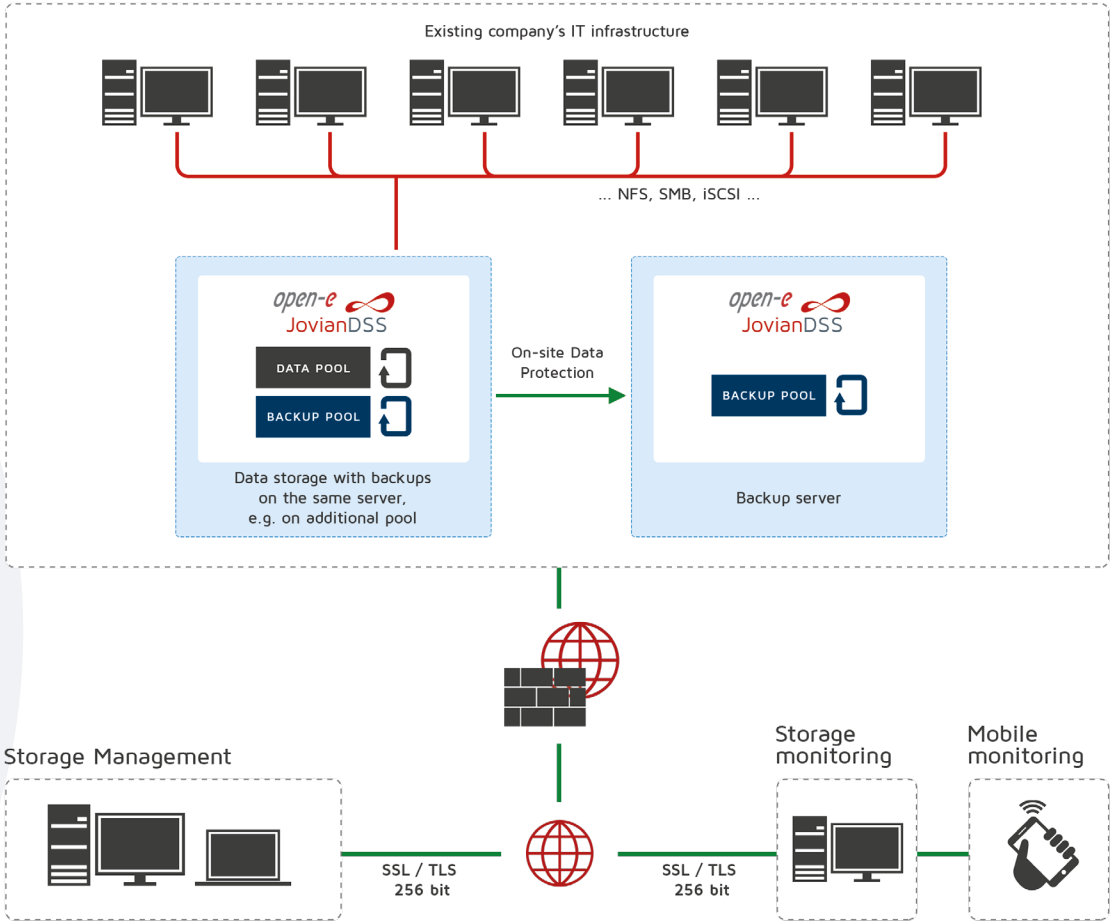
On-site Data Protection with Backup Pool

You may wonder how to protect your company against the consequences of your High Availability cluster system failure. It can be one of the component issues or unintentional human error that causes unavailability. If the whole unit is down, you won't be able to provide your business processes and manage the data properly. So the one-in-two answer and resolution is **On-site Data Protection** that **secures you against:**

- ✓ **Cluster failure**

On-site data protection allows for keeping backups at your emplacement on an additional local Open-E JovianDSS--based system. Hence, what you can count on to store your data is a production server unit, the backup on the local pool, and extra backup on the second local server.

Who can benefit from it? **Healthcare organizations** to protect patient information, **financial services** to protect customer information, **government institutions** to protect sensitive information and comply with regulations, and **manufacturing and logistics** to protect operational information and customer data. Plus, all of them will comply with regulatory requirements.



+ protects with snapshots (access to previously saved data)
+ gives you the possibility to choose snapshot frequency
+ self-healing
+ disk failure (RAIDs)
+ RAID rebuild
+ fast rollback
+ system failover
− doesn't protect you from natural disasters
− doesn't protect you from on-site storage unit failure
− doesn't prevent downtime

WARNING: Due to extra drives or the second server on your location, data restore is usually easier and faster than an off-site backup if the main production server is down. Therefore, it is a perfect solution for hot data backup that can be restored from the backup copy. Note that this doesn't protect against natural disasters, on-site storage units failure, and downtime. **It is only a local backup, but Disaster Recovery in case of the cluster failure is provided.**

Off-Site Data Protection

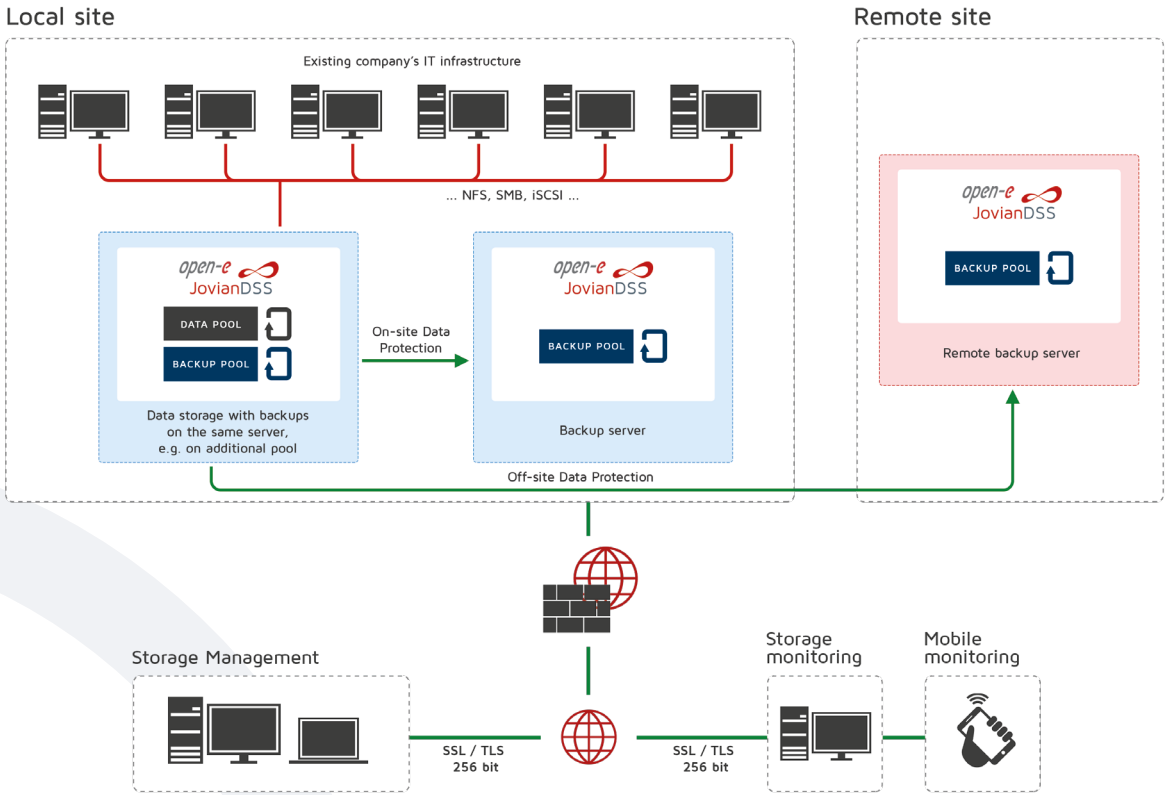
As we're all aware, there is an eternal conflict that also reflects on businesses - **man vs. nature**. In some extreme cases we tend to lose, and so do our businesses. **Flood, fire, earthquakes**, etc., don't mind how important our data is, so if something like this happens, it **may lead to total bankruptcy**, as you lose the whole equipment and everything stored there. Is there anything more punishing? We doubt it. Especially if your business relies on archiving and keeping long-term backups. If that's what concerns you, there's **Off-site Data Protection**, a solution that ensures:

- **Protection against natural disasters**
- **Great archiving opportunities with long-term backups**

Besides covering all previously mentioned features with snapshots, RAIDs, High Availability, and on-site backup servers, it uses an **additional remote server**, allowing you to benefit from all advantages of external data backup. These are: **protecting from natural disasters as well as harmful and intentional human actions** (i.e., theft), causing both - the production system and the on-site backup server - failure or destruction.

It is a remarkable solution for **large enterprises managing critical applications and core-business data**. It finds a lot of usability in **defense and national security** departments managing classified information. **Technology, software, energy, and utility companies** can rely on it too.

It has some disadvantages. It **won't fully prevent you from downtime**, so Business Continuity depends on the time it can fully recover and the connection throughput. Sometimes, depending on the amount of data you keep and manage, the recovery can take a long time, and **the costs are much higher** in such a case because you need another independent backup unit.



+ protects with snapshots (access to previously saved data)
+ gives you the possibility to choose snapshot frequency
+ self-healing
+ disk failure (RAIDs)
+ RAID rebuild
+ fast rollback
+ system failover
+ protects against natural disasters
+ protects against on-site storage unit failure with a backup server
+ allows converting backup server to production server
+ no need to use a third-party backup system
− doesn't prevent downtime
− high costs
− long recovery time (in case of failure of the rest of the safety)

WARNING: Off-site data protection makes it possible to back up all your data on a remote server at a different location. Hence, once the data from the production server is lost, you can retrieve it from the remote backup unit. It may take some time, depending on the number and size of these files. Companies that manage archives and rely on long-term backups that don't require instant access may also benefit from using a remote server and transferring or restoring data to the main location once needed. **It is an actual backup, and Disaster Recovery is provided.**

Maximum Data Security

If your main goal is to ensure the **highest data security level**, money is not the problem, but the downtime is something you can't afford - you can maximize the data security by combining all of the previously mentioned methods and managing it by Open-E JovianDSS. The **On- and Off-site data backup with an additional high availability cluster** allows for **full Business Continuity with zero downtime**.

The costs may be considered a disadvantage, but try to compare them to the costs of data loss. Nobody can afford to lose data. Moreover, you don't need to rely on the most expensive hardware and still, the additional components will do the job when it comes to keeping your data safe.

This solution is mainly popular in the **software, technology, or finance markets** as well as **the national defense departments**. If one decides to choose this option, it means that no downtime is allowed, as **full Business Continuity** is crucial. It's also capable of managing huge amounts of **sensitive, secured, and high-value information**, hence **the recovery time may be longer if you perform a restore from a remote location and all other safety methods fail.**

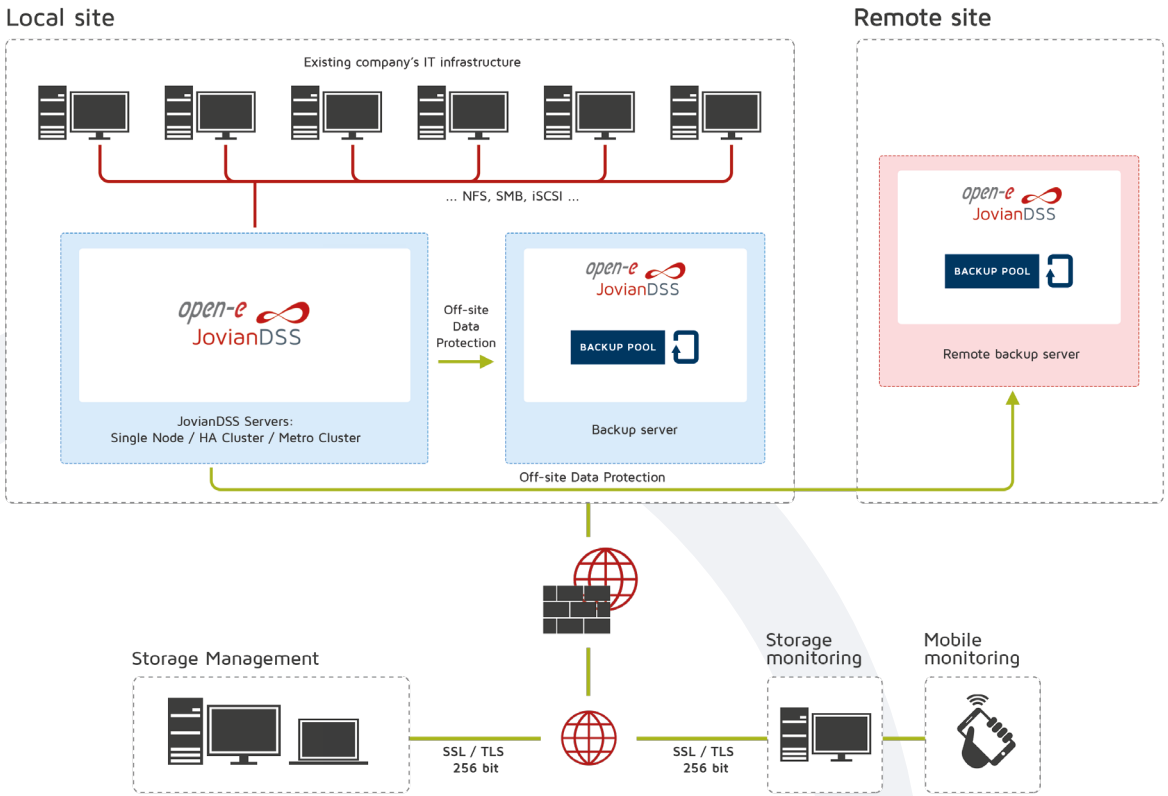
High Availability

+

On- & Off-site Data Protection

=

Maximum Data Protection



+ **protects with snapshots (access to previously saved data)**
+ **gives you the possibility to choose snapshot frequency**
+ **self-healing**
+ **disk failure (RAIDs)**
+ **RAID rebuild**
+ **fast rollback**
+ **system failover**
+ **protects against natural disasters**
+ **protects against on-site storage unit (backup pool) failure with a backup server (pool)**
+ **allows to converting a backup server to production server**
+ **no downtime while recovery**
+ **full Disaster Recovery (HA)**
− **high costs**
− **long recovery time (in case of failure of the rest of the safety)**

WARNING: This model covers any possible scenario that may act against your business processes. Archives and long-term storage will be safe if kept on the **remote backup, the on-site backup** server will contain the hot data needed to be restored instantly, **and RAIDs and snapshots** will protect you with parity and self-healing. This can all be managed by **Open-E JovianDSS** providing full and quick accessibility and efficiency. **It is an actual backup, and Disaster Recovery is provided.**

Check the Latest Open-E Brochures

TIME IS MONEY, AND SO IS THE DATA: Business Continuity & Disaster Recovery

As we already established, your business safety should focus on ensuring its continuity and (in case of any unfortunate event that eventually happens) recovering from the disaster. Why?
To provide the business back on track as fast as it's possible.

Let's get back to three crucial questions specified earlier to make sure which path of data protection you should choose:

- **Which data is critical for your company operations and keeps your business up and running?**
- **Which data is not so important but still necessary to maintain long-term operability?**
- **Which data is irrelevant, meaning you can get rid of it or reduce its costs as much as possible?**

If you answered them honestly and already picked the most suitable method for your company's safety, we have some advice and tips for you! It will be profitable to make your business continue its operations with minimized interruption and set the appropriate indicators of a **Disaster Recovery** plan to shorten the downtime to a minimum. Disaster Recovery is a part of **Business Continuity**, with all processes that should and can be included to provide the best possible method to shorten the downtime and bring back the fully operational business status. The proper **retention plan** with its two main **objectives - period and interval** - can help to determine a smart backup process tailored to your possibilities and needs.

Remember - **TIME IS MONEY, AND SO IS THE DATA!**

Business Continuity

Business Continuity is a kind of plan in the risk management field that helps you understand the essential organizational functions, the reasons for controlling them, and how to recover your data in any scenario. The basic functions **prevent you from losing data** because of silent data corruption or protecting your company data with proper redundancy by keeping the parity data in your data storage array. It includes a **High Availability cluster** with the additional production and backup pool, used once the primary one fails. Finally, **the Open-E JovianDSS On- and Off-Site Data Protection** deployed for keeping backups prevent you from losing hot data stored on-site or the cold data, i.e., archives kept off-site. These are also the first steps to enable the **Disaster Recovery** procedures, which we will cover later. Such a plan gives you a complete picture of any possible emergency so that you can prepare to operate at least on a basic level during potential disruptions.

Knowing what **Business Continuity** is, we can now focus on the crucial factors and tips that help to apply it most efficiently.

Place resilience at the top of your priority list. It helps to reveal the weak spots in the business system and prepare for any disaster that may take place. In this strategy, you should analyze the organizational environment to prioritize further actions. It requires the evaluation of all possible data storage backup options, including local and remote ones.

Here are the key tips to help ensure Business Continuity:

- Determine which functions are essential to the operation of your business and prioritize their continuity in the event of a disruption.
- Implement backup systems and redundancies to reassure that critical infrastructure and technology can be recovered in case of a disruption.
- Make sure that employees are trained and familiar with the Business Continuity Plan and continuity procedures.
  Remember that humans are still the leading cause of data loss.
- Use off-site locations to ensure that critical data can be accessed and recovered in case of a disruption.
- Develop a crisis communication plan and ensure that all employees are familiar with it to ensure effective communication during a disruption.
- Implement redundant power supply and backup generators to ensure that critical infrastructure can be powered in case of a disruption.
- Establish protocols for communication with employees, customers, partners, and other stakeholders during a disruption.

BOOST

YOUR DATA STORAGE SOLUTION

with Open-E JovianDSS Setup!

Enjoy the unlimited possibilities in data storage solution implementations with **Open-E JovianDSS:** a ZFS- & Linux-based hardware-agnostic **Data Storage Software** that can be used in a wide range of advanced solutions for:

- **Business Continuity & Disaster Recovery.**
- **Data Storage.**
- **Backup.**

Learn more information on our website:
www.open-e.com/r/qvfn

DISASTER RECOVERY

Let's agree that having no backup equals taking too much risk regarding successful business management. No one would like to face the consequences of losing their own or their customers' data. Reputation decline, legal penalties, or costs can be much harder to cope with than investing in appropriate **Disaster Recovery** solutions. **As stated before - time is money, and so is the data!** A proper backup tailored to the business model makes you safe and more confident on the market. It is a great advantage over your competitors, ensuring smart Disaster Recovery, so you won't get lost behind them if something wrong happens.

Here are the most important tips for ensuring Disaster Recovery:

- Make sure to regularly back up all critical data to a secure location.
- Store backups in a secure offsite location to prevent data loss in the event of a physical disaster and be able to restore the most recent data.
- Use virtualization technologies to enable fast and flexible Disaster Recovery.
- Use multiple network paths to ensure network availability.
- Determine which systems and data are essential to the organization's operations and prioritize the backup and recovery.
- Establish procedures for communicating with stakeholders during a disaster.

Two main indicators to be followed will provide you with the best way to recover your system and prevent you from losing data, time, and - as a consequence - money: **recovery point objective** and **recovery time objective**. You can treat them as the key performance indicators of system availability.

Recovery Point Objective (RPO)

RPO defines how much data a company can afford to lose in the worst-case scenario and helps determine the frequency and type of backups required to meet the desired RPO.

- **Evaluate your infrastructure** - assess the hardware, software, and network components involved in your data backup and recovery process to identify all potential bottlenecks or limitations.
- **Use multiple backup methods** - implement a multi-tier backup strategy that includes a combination of on-site, off-site, and cloud backups.
- **Automate backup and recovery processes** - ensure that backups are consistent and frequent to reduce the risk of human error.
- **Regularly test backup and recovery processes** - testing helps ensure that the backup and recovery process works as intended and that data can be recovered quickly and effectively.

Recovery Time Objective (RTO)

RTO is a metric used in Disaster Recovery and Business Continuity planning that indicates the maximum acceptable time to recover a critical business function after a disaster. It sets a target for the time to recover from a disaster. It is a critical factor when it comes to determining the resources and strategies needed for a Disaster Recovery plan.

- **Conduct a risk assessment** - identify the critical business functions and the potential impact of a disaster on those functions.
- **Create a Disaster Recovery plan** based on the risk assessment and develop a detailed plan for recovering critical business functions in the event of a disaster.
- Based on the Disaster Recovery plan, **choose the technologies that best support the RTO**, including backup and recovery software, hardware, and cloud services.
- **Implement the Disaster Recovery plan**, including the creation of procedures and protocols.

Place Resilience at the Top of Your Priority List

The response appears to be an essential part of Business Continuity as it gives an emergency plan of how each department should act if any kind of unexpected event happens. This strategy should also include instructions on how to behave in case of regular maintenance of the IT infrastructure:

- **Code of conduct for all the employees showing how they should react in case of data loss and emergencies**
- **Up-to-date contact details with the employees/third parties responsible for response in case of data loss**
- **Channels of communication defined and established in case of data loss**
- **RPO and RTO precisely defined in SLA**
- **“Safety drills” for both Business Continuity and Disaster Recovery Plans**

Recovery, on the other hand, helps build a proper plan or a scenario for returning to the 100% operational workflow level after any disaster or unexpected event which can arise. The recovery strategy can be divided into several options depending on the type and the size of a business organization:

- **Utilizing backup infrastructure, appliances, or facilities**
- **Restoring regular work with internal or external resources**

Just Technology GROUP

Just Technology Group Data Storage Services

Just Technology Group is a managed Service provider that supports hundreds of clients. With Open-E JovianDSS, we can create, manage, and restore virtual machines that suit a wide range of customers’ needs. As a 5-year partner with Open-E, we have onboarded multiple clients with their products to create remote backups and Disaster Recovery plans. It makes it possible to run quick restores with a rollback feature and cloning tool to recover lost data and restore infrastructure within a few minutes preventing further downtime. Snapshots taken every 5 minutes provide quick infrastructure rollbacks to any previous system state in case of any issues or security incidents.

Just Technology Group
United Kingdom

To sum up, these are the key factors for ensuring Business Continuity and data protection. Below we listed some of the most important things to remember:

→ Backup and Disaster Recovery Plan:

One of the most important aspects of Disaster Recovery for data storage is to have a comprehensive backup and recovery strategy. It involves regular data backup, storing backups offsite, and testing the recovery process to ensure that data can be quickly restored in the event of a disaster according to your Disaster Recovery plan.

→ Redundancy:

Redundancy is a crucial aspect of Disaster Recovery the storage business, as it ensures that data and systems are available even if one component fails. It can include redundant storage arrays, backup generators, and redundant network connections.

→ Scalability:

Disaster Recovery plans must be scalable to meet the changing needs of the business as it grows. It includes ensuring there is sufficient storage capacity to accommodate future growth and that the Disaster Recovery plan can be easily updated to reflect changes in the business.

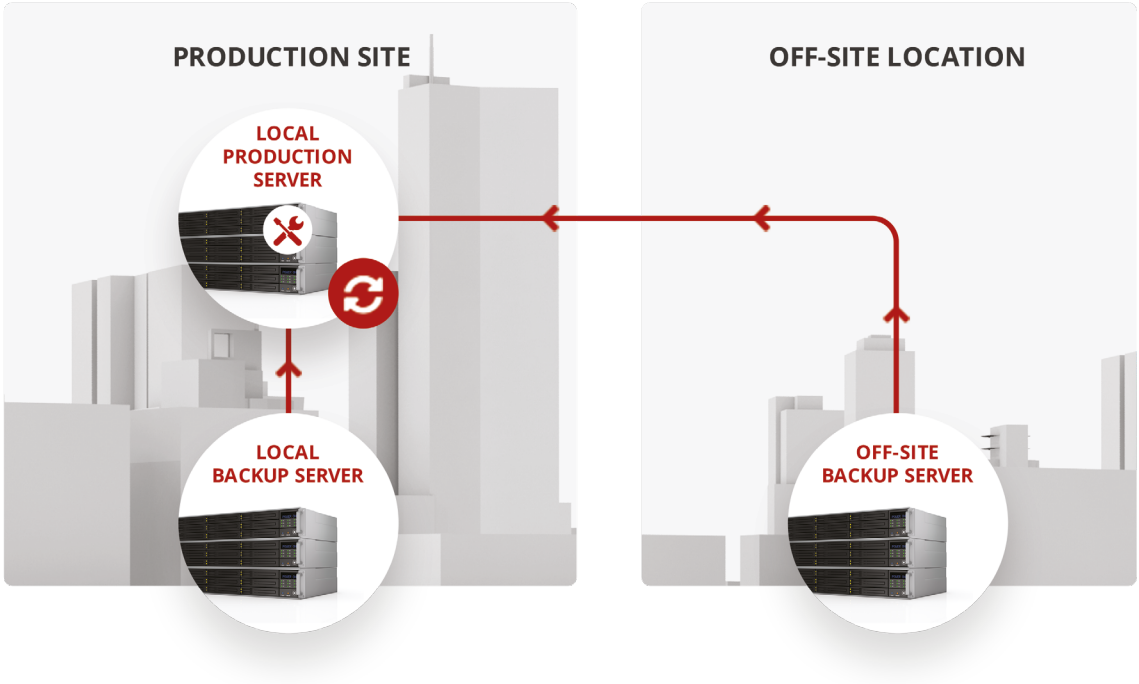
Once building a comprehensive Disaster Recovery plan and ensuring Business Continuity, remember it should incorporate backup, recovery, redundancy, and scalability essential for storage businesses. It will work on minimizing the impact of disasters on the company's operations and protect its valuable data.

ON- AND OFF-SITE DATA PROTECTION IN Disaster Recovery

with Open-E JovianDSS Data Storage Software

The On- and Off-site Data Protection feature in the Open-E JovianDSS Data Storage Software allows users to back up and restore crucial company data in case of an unexpected event due to a combination of several technologies. This feature enables the creation of consistent snapshots and asynchronous snapshot replication to local and/or remote destinations. The replication tasks can be set according to the specific requirements due to advanced retention plans.

The On- and Off-site Data Protection is very flexible, as it covers a wide range of Disaster Recovery plans without the need to use additional third-party tools. However, there is an important aspect that people tend to ignore in case of an off-site backup. The backup kept externally is much more reliable and safe to be used and applied in business-critical situations. On-site backup is an asset, of course, but it won't protect you entirely. Issues like unexpected events or others lead to total hardware failure.



Once this happens, you lose all your data and will need to face the consequences that might cost you much more than investing in an off-site backup. Evaluate this while reading more about **retention plans** that focus on **snapshot backups**.

Founded in 1998, Open-E is a well-established developer of IP-based storage management software. Our flagship product, Open-E JovianDSS, is a robust, comprehensive, and award-winning data storage application known for its excellent compatibility, ease of use, and stability. It's an undisputed leader in price-performance with over 41,000 installations worldwide. Building on this expertise, we've introduced Open-E JovianVHR, a software-defined data storage solution specifically designed to act as the immutable data storage target for a Hardened Repository from Veeam.

With a reputation for business reliability and a commitment to innovation, Open-E has become the technology partner of choice for industry-leading IT companies

+41000 software implementations

+100 countries worldwide

+27 years of experience

+800 certified engineers and sales professionals

Scan to learn more

Open-E, Inc. | +1 (678) 666 2880 (US) | +49 (89) 800777 0 (Europe) | info@open-e.com