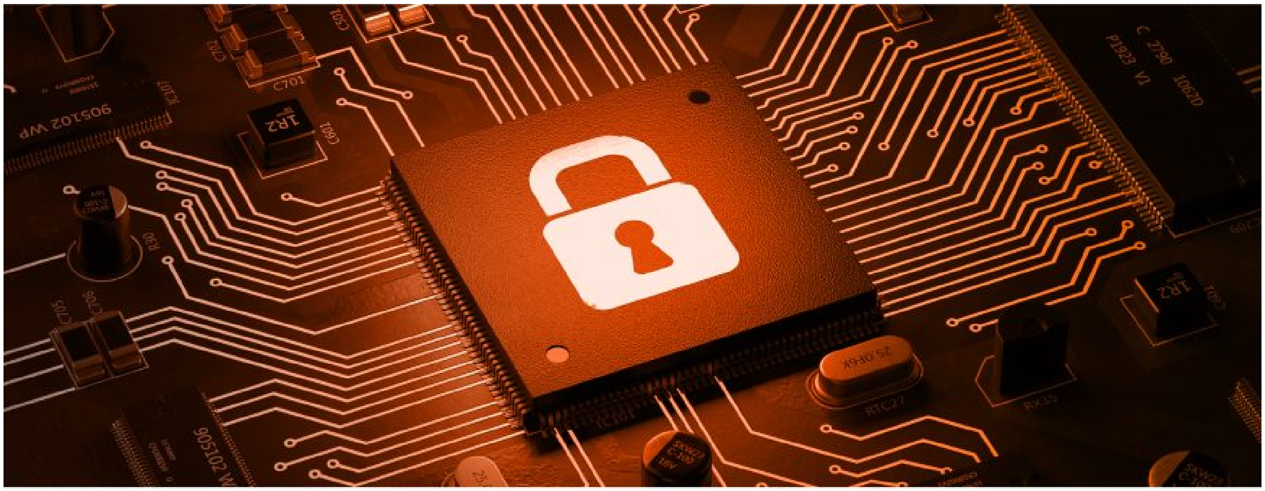
GUIDE

The Definitive Guide to Data Protection



As the total amount of data created, stored, and shared continues to grow at exponential rates, so too does the importance of protecting your data from loss, corruption, and exposure.

What is data protection?

Data protection is the process of protecting data against loss, corruption, or the disruption of services through the use of backups and data resilient architecture. From backups to recovery (https://www.purestorage.com/fr/solutions/data-protection/data-backup.html) and data reuse, it covers all technologies and techniques an organization may use to keep data secure and highly available for its products, services, and operations.

In this guide, we'll dive into the various technologies and techniques at a system administrator's disposal for keeping data safe.

Related Articles

BLOG

5 Ways to Address Security Gaps Before an Attack

(https://blog.purestorage.com/perspectives/5-ways-to-address-data-security-gaps-before-an-attack/)

BLOG Avec son SLA, Pure propose une garantie de rendement énergétique avec le stockage le plus écologique au monde (https://blog.p... →

FR / FR

PURESTORAGE(https://www.purestorage.com/fr/)

Main Menu

Produits

Solutions

Services et support

Ressources

Société

Partenaires

FERMER

BLOG

Who Are Ransomware Attackers and What Are They After?

(https://blog.purestorage.com/perspectives/who-are-ransomware-attackers-and-what-are-they-after/)

BLOG

5 Questions to Ask Your CISO Today

(https://blog.purestorage.com/perspectives/5-questions-to-ask-your-security-team/)

Data security vs. data privacy vs. data protection

While the term data protection is often used interchangeably with data security and data privacy, there are subtle differences between the three terms:

- **Data protection** is often used as an umbrella term that includes data security and data privacy. In the industry, however, it often refers more specifically to the prevention of data loss or corruption through resiliency, redundancy, and recovery.
- **Data security** is more specific, relating to the prevention of unauthorized access, manipulation, or corruption of data by internal and external parties through firewalls, encryption, and other technologies.
- **Data privacy** focuses on controlling access to data to prevent the exposure of sensitive data and information. It includes security training, authentication strategies, and compliance with information security regulations such as the GDPR.

You'll want to invest in all three if you want to ensure your organization's data is fully protected. For this guide, we'll focus primarily on data protection, although some overlap naturally exists between the three domains.

Elements of a disaster recovery strategy

The philosophy behind data protection in the server room or data center has long been one of redundancy. You can't afford to have your data lost, corrupted, or compromised, so always have a backup.

Of course, in practice, backing up your data is the bare minimum. Data protection is really an exercise in managing your recovery point objectives (RPOs) and recovery time objectives (RTOs) for the most critical services in your operational technology stack. In other words, it's how quickly you can back up and restore your data to prevent the disruption of critical business operations.

So what exactly are RTO and RPO?

- **RTO**: The maximum time your business can afford to lose access to the data that powers your apps and operations. It determines how quickly you need your system to recover.

- **RPO**: Refers to the maximum amount of data you can afford to lose. Use this to determine the frequency of your backups.

RTO and RPO are the key performance indicators (KPIs) you'll want to be aware of when building your disaster recovery strategy.

Learn why With Ransomware, Restore Is the New Backup (https://blog.purestorage.com/perspectives/with-ransomware-restore-is-the-new-backup/)

Backup and restore

Also known as backup and disaster recovery, backup and restore refers to the practice of backing up your data so that you can restore business services and operations in the event of a disaster. Disasters can include everything from natural disasters and blackouts to human errors (https://blog.purestorage.com/perspectives/what-are-insider-threats-and-how-can-you-combat-them/) and cyberattacks (https://blog.purestorage.com/perspectives/what-is-cyber-espionage-and-what-can-you-do-about-it/).

Data backup planning

Depending on the technologies and resources available to your organization, you may need to employ one or more of these backup techniques as part of a larger data center disaster recovery strategy:

- **Full image backup**: You back up the full image of your data to create a restore point you can instantly roll back to. Because you're performing a full backup, this technique takes the longest to store.
- **Differential backup**: Backs up all changes since the last full image backup. Restoration only requires two files: the last full image backup, followed by the most recent differential backup.
- **Incremental backup**: You incrementally back up changes since the last full image restore point. After a set number of incremental backups, the cycle completes with a full image backup. Restoration starts with the last full image backup, followed by incremental backups to the target RPO.
- **Real-time backup**: Also called a continuous backup, this method involves instantly copying every change to your data to a separate storage device. It provides the most granular and comprehensive backup.
- **Instant recovery**: A continuously updated backup virtual machine (VM) is maintained for a production VM. When the production VM fails, the backup instantly takes over, yielding zero RTO and zero RPO.

Learn about tiered backups and data bunkers for long-term, highly available backup solutions (https://blog.purestorage.com/perspectives/bounce-back-faster-with-tiered-backups-and-bunkers/)

Data center disaster recovery

Implementing a solid backup plan is only one part of the data protection equation. The second part involves hitting your RTOs. In other words, how do you get your business systems back up and running in the wake of a disaster? A typical disaster recovery plan will include:

- **Disaster recovery team**: Designate a group of directly responsible individuals (DRIs) for implementing the disaster recovery plan.
- **Risk analysis**: It pays to be prepared and aware of what could go wrong within your organization. Identify risks and plans of action in the event of unplanned downtime or a disaster.
- **Compliance**: Just because you're the victim of an attack doesn't mean you get a break from data compliance regulations (https://blog.purestorage.com/perspectives/how-to-improve-data-compliance-with-smarter-storage/). A compliance officer can ensure your organization is following retention and deletion policies and not backing up sensitive data previously slated for deletion for compliance reasons.
- **Business impact analysis**: In the wake of a disaster, you need someone to assess the potential impact to business services. It may be possible to get the most critical services back up and running earlier. Identifying and documenting which systems, applications, data, and assets are most critical for business continuity can help your disaster recovery team take the most efficient steps needed to recover.
- **Data backup**: Depending on which backup strategies and technologies you're using, you can resume business operations by rolling back to the most recent backup. RTOs and RPOs will vary depending on the backup and services affected.

It's all about continuous data protection

In an increasingly digital world, customers expect businesses to be able to deliver their services 24/7, without downtime or disruption. Continuous data protection (CDP), also known as a continuous backup, is the practice of backing up the continuous stream of data needed to support modern business operations. It gives organizations the ability to restore a system to any previous point in time. The goal of CDP is ultimately to minimize RTOs and RPOs in the event of a disaster. By leveraging continuous real-time backups and implementing a solid disaster recovery strategy, it's possible to maintain business continuity through CDP.

Ransomware protection

Thus far, we've covered the things you can generally do to protect your data and maintain business continuity in the face of a disaster. But there's one type of disaster that is on the rise and worth addressing on its own: ransomware.

Cybercriminals have always been a threat, but while the hacktivists of yesteryear were motivated by political, cultural, and religious beliefs, today's cybercriminals are largely motivated by financial gains. Ransomware, in which a hacker locks you out of your data via encryption until you pay a ransom, is now a multimillion-dollar industry. And in a world where downtime directly translates to lost revenue, it's never been more tempting to just pay that ransom.

In the following sections, we'll cover the things you can do to mitigate a ransomware attack.

Preventing a ransomware attack

The best way to fight ransomware is to prevent it from occurring in the first place. It's about obtaining system-wide visibility, practicing good data hygiene, and having a plan in place to deal with a threat once you've identified it.

BLOG Avec son SLA, Pure propose une garantie de rendement énergétique avec le stockage le plus écologique au monde (https://blog.p... → FR / FR

PURE STORAGE (https://www.purestorage.com/fr/)

Main Menu

Produits

Solutions

Services et support

Ressources

Société

Partenaires

FERMER ✕

- **Logging and monitoring**: Logging and system monitoring tools can give you a bird's-eye view of your systems and help you understand what your IT infrastructure looks like when everything is running smoothly. Speedy real-time analytics can help you spot anomalies (e.g., a spike in traffic from a suspicious IP address) and other activity that can tip you off to a potential attack.
- **Data hygiene**: When hackers plant malware, they're looking for security vulnerabilities such as unpatched operating systems, poorly secured third-party tools, and messy data management. Data hygiene means implementing good patch management, system configuration, and data sanitization practices. Not only do these things make your organization run smoother, but they also greatly reduce the attack surface of a potential hack.
- **Operational security**: Humans are an often overlooked vulnerability when it comes to cybersecurity. Implementing multi-factor authentication, administrative controls, and data tiering can ensure data is only available to the authorized individuals that need it. Security awareness training covering the techniques of hackers and phishing attacks can help prepare your organization for spotting real attempts in the wild.

What to do during a ransomware attack

Cyber attacks aren't as obvious in real life as they are to the protagonists of movies. The attack itself may last only 30-40 minutes as they access your files and move laterally through your networks, encrypting files and deleting backups. On the flip side, an attacker might lurk on your network long after gaining access, monitoring your responses to anomalies as they plan out an actual attack. Either way, by the time you receive a ransom note for your data, the attack has already been completed.

The only way to catch a ransomware attack while it's still happening is to take notice of foiled phishing attempts as they happen (by training your employees) or catch suspicious activity on your network through SEIMs and logs. Provided you've taken these proactive steps and have the necessary tooling, it pays to have a cyber incident response (CIR) plan to deal with the anomalous activity when you discover it. Document everything and notify the relevant IT personnel to isolate affected systems and mitigate damage. You'll need those records to meet compliance requirements and help law enforcement with investigations should that activity prove to be a real ransomware attack. We'll cover the details of creating a CIR plan later in this article.

Post-ransomware attack disaster recovery

So your files have been encrypted and you've just received a ransomware note. What are your options?

One option is to just pay the ransom, but doing so could risk exposing your organization to further extortion down the line.

A better option, provided you followed the proactive ransomware mitigation steps outlined in earlier sections, is to purge, restore, and respond:

- **Purge** your systems of the vulnerabilities that allowed the attackers to access your data. Compromised hardware and software should be isolated and disconnected from the network immediately. A system and network audit should be conducted to ensure no backdoors or other malware remain. It's important to sanitize your systems before you restore data from your backups and go live.
- **Restore** data by leveraging your backup and recovery plan. Hopefully, you have some snapshots and disaster recovery infrastructure in place to allow you to pick things up right before the cyber incident occurred. Your defense team should perform a forensic analysis of your backup data within a sanitized virtual environment to ensure the attackers didn't leave anything behind. You're looking for an untampered recovery point you can roll your systems back to.
- **Respond** to the attack appropriately by taking measures to review records, audit systems, and document the nature of the attack. In order to comply with regulations, you may need to notify customers of a data breach and you'll want your logs to demonstrate that your organization did everything it could to respond to the attack. Information gained from the attack can be leveraged to help law enforcement track down the perpetrators, as well as help secure your own systems against future attacks.

Learn more: Hacker's Guide to Ransomware Mitigation and Recovery (https://www.purestorage.com/fr/resources/type-a/hackers-guide-to-ransomware-mitigation-and-recovery.html)

Elements of a cyber incident response plan

A cyber incident response plan is a formal document that outlines the details personnel should follow in the event of a cyberattack. It's also a Payment Card Industry Data Security Standard (PCI DSS) requirement. Cyber incident response plans are generally composed of six distinct phases:

1. Preparation

This phase outlines the steps, roles, and procedures that should be followed in the event of a cyber incident. Prepare a team of individuals with clearly defined roles and responsibilities for responding to a cyber incident. It also covers testing these roles and procedures via employee training with drill scenarios such as mock data breaches.

2. Identification

This phase involves detection and forensic analysis of anomalous cyber events to determine whether a breach has occurred and the severity of the incident.

- What data was exposed?
- How was it discovered?
- Who discovered the incident?
- Who does it affect?

The scope and severity of the incident needs to be documented and analyzed before it can be effectively addressed. System and network logs can be the key to responding immediately to a breach and determining the critical details of a security incident after it has occurred.

Learn more: You've Been Hit by Ransomware. Now What? (https://blog.purestorage.com/perspectives/youve-been-hit-by-ransomware-now-what/)

3. Containment

In the event of a cyber incident, the containment phase specifies actions taken to prevent further damage and mitigate risks. Containment typically involves steps for disconnecting and deactivating affected devices from the internet.

4. Eradication

Once a threat has been contained, it can be analyzed by a security professional to determine the root cause of the incident and eliminate any threats. Malware removal, security patches, and other measures should be outlined in the eradication phase.

5. Recovery

The recovery phase (https://blog.purestorage.com/perspectives/5-ransomware-recovery-steps-to-take-after-a-breach/) involves steps and procedures for restoring the affected systems and devices back to production. Redundant backups, snapshots, and a disaster recovery plan may be implemented to restore mission-critical services (https://blog.purestorage.com/perspectives/bounce-back-faster-with-tiered-backups-and-bunkers/) in the event of a breach. You should also have a staged recovery environment that can give you a "prebuilt" way to get back online right after an event.

6. Lessons learned

Cybersecurity is a continuous process. It's important to collect information gathered and lessons learned from a cyber incident and apply them to enhancing security protocols and the incident response plan itself.

Get a detailed 6-Point Plan for the "During" of a Data Breach (https://blog.purestorage.com/perspectives/a-6-point-plan-for-the-during-of-a-data-breach/)

Safeguard your data with modern data protection solutions from Pure Storage

In this guide, we looked at the various tools, strategies, and technologies available for protecting your data and maintaining business continuity in the event of a disaster. At the end of the day, your data is only as secure as the infrastructure you use to manage it.

That's why Pure Storage® products are designed from the bottom up with modern data protection in mind. Examples of modern data protection solutions developed by Pure include:

- **FlashBlade® Rapid Restore**: Delivers 270TB/hr of data recovery performance (https://www.purestorage.com/fr/docs.html?item=/type/pdf/subtype/doc/path/content/dam/pdf/en/solution-briefs/sb-flashblade-rapid-restore.pdf/context/knowledge/definitive-guide-to-data-protection.html) to production and test/dev environments.
- **ActiveDR™**: Built into Purity, ActiveDR gives you near-zero RPO (https://www.codyhosterman.com/2020/06/pure-storage-data-protection-part-i-replication-fundamentals/) via robust asynchronous replication that covers both new writes and their associated snapshots and protection schedules.
- **Purity ActiveCluster™**: Synchronous replication for RPO zero meets transparent failover for RTO zero in this true bidirectional active-active metro stretch cluster.
- **SafeMode™ snapshots**: SafeMode snapshots (https://blog.purestorage.com/products/protect-your-data-from-ransomware-with-safemode-snapshots/) are a ransomware protection solution built into FlashArray™ and FlashBlade. The snapshots are immutable, allowing your team to recover data in the event of a ransomware attack.

Modern data threats require modern data protection solutions. Storing your data with Pure Storage is the best way to ensure performance, reliability, and security for your organization.

We Also Recommend...

Check Out Our Resource Center → (https://www.purestorage.com/fr/resources.html)

11/2020

PRÉSENTATION 3 PAGES →

(https://www.purestorage.com/fr/docs.html?item=/type/pdf/subtype/doc/path/content/dam/pdf/en/solution-briefs/sb-modernize-vmware-hybrid-

05/2022

The Rise of Data Storage as a Service

Why Agility and Flexibility Are Critical to How Organizations Use and Analyze Data

RAPPORT D'ANALYSTE →

05/2018

Guide Le datacenter 100 % flash pour les nuls

Accédez gratuitement au guide Le datacenter 100 % flash pour les nuls. Ce guide fournit des informations précieuses sur le coût de possession,

E-BOOK 52 PAGES →

cloud.pdf/context/knowledge/definitive-guide-to-data-protection.html) (https://www.purestorage.com/resources/type/a/rise-data-storage-as-a-service.html) (https://www.purestorage.com/fr/resources/type/a/flash-for-dummies.html)

BLOG Avec son SLA, Pure propose une garantie de rendement énergétique avec le stockage le plus écologique au monde (https://blog.p... → FR / FR

PURESTORAGE (https://www.purestorage.com/fr/)

Main Menu

Découvrir Pure

- Produits
- Solutions
- Services et support
- Ressources
- Société
- Partenaires

Webinars (https://www.purestorage.com/fr/resources/we →

Blog (https://blog.purestorage.com/) →

FERMER ✕

Centre d... (https://www.purestorage.com/fr/resources. →

À propos (https://www.purestorage.com/fr/company.html)

Pourquoi Pure Storage (https://www.purestorage.com/fr/why-pure.html)

Relations investisseurs (https://investor.purestorage.com/investor-home/default.aspx)

Équipe de direction (https://www.purestorage.com/fr/company/leadership.html)

Newsroom (https://www.purestorage.com/fr/company/newsroom.html)

Offres d'emploi (https://www.purestorage.com/fr/company/careers.html)

Quelques chiffres (https://www.purestorage.com/fr/docs.html?item=/type/pdf/subtype/doc/path/content/dam/pdf/en/infographics/ig-pure-storage-fast-facts.pdf)

Produits (https://www.purestorage.com/fr/products.html)

Ressources (https://www.purestorage.com/fr/resources.html)

Connaissances (https://www.purestorage.com/fr/knowledge.html)

Blog (https://blog.purestorage.com/)

Podcasts (https://www.purestorage.com/fr/resources/the-pure-report.html)

Webinaires (https://www.purestorage.com/fr/events.html)

Événements (https://www.purestorage.com/fr/events.html)

Travailler en partenariat avec Pure (https://www.purestorage.com/fr/partners/request-access.html)

Portail partenaires (https://purestorage.force.com/partners/s/login1/?language=en_US)

Alliances technologiques (https://www.purestorage.com/fr/partners/technology-alliance-partners.html)

Certifications (https://www.purestorage.com/fr/resources/certifications.html)

Validated Designs (https://www.purestorage.com/fr/resources/validated-designs.html)

Contactez-nous (https://www.purestorage.com/fr/contact.html)

Communauté de clients (https://www.purestorage.com/fr/company/customer-community.html)

Sélectionnez Votre Région

(https://www.linkedin.com/company/pure-storage)

Vie privée (https://www.purestorage.com/fr/privacy.html)

BLOG Avec son SLA, Pure propose une garantie de rendement énergétique avec le stockage le plus écologique au monde (https://blog.p... → FR / FR

Conditions d'utilisation du site Web (https://www.purestorage.com/fr/terms.html)

Informations juridiques (https://www.purestorage.com/legal/productenduserinfo.html)

PURESTORAGE (https://www.purestorage.com/fr/)

Paramétrage des cookies

Main Menu

Produits

Solutions

Services et support

Ressources

Société

Partenaires

FERMER ⊗