Acronis

WHITEPAPER

Building a solid BCDR program: a must in the compliance ecosystem

Introduction

Organizations want to avoid downtime in the case of an unexpected business disruption. An IT business continuity plan, which should be an important part of a company's overall risk management strategy, aims to reestablish business-wcritical activities as quickly as possible. In the best of all worlds, customers, partners and employees don't feel the disruption at all, and no data is lost or corrupted.

There are many types of events that can disrupt business continuity – from a local power outage, to a specific hardware failure, or an admin who inadvertently takes down a key service. Disaster recovery is the subset of business continuity that focuses on more dramatic and systemic disruptions such as natural or man-made disasters or a massive cybersecurity incident.

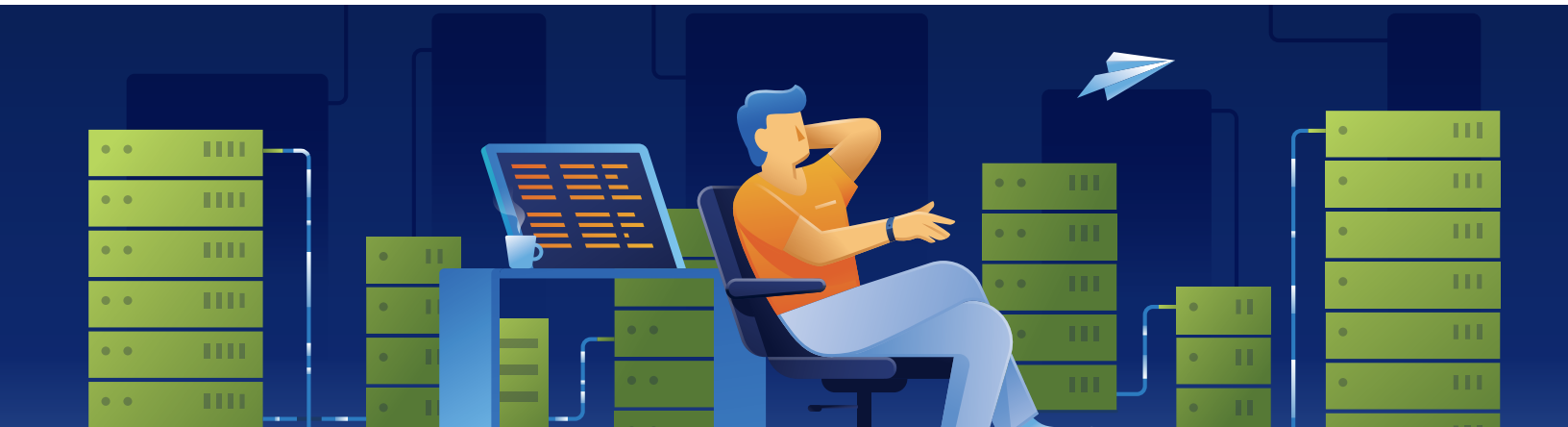
A resilient business continuity/disaster recovery (BCDR) program is essential for gaining the trust of end users, preventing loss of revenues and maintaining a company's competitive profile. But aside from all the good business reasons, today there are also governmental and industry regulatory frameworks that mandate BCDR activities as part of maintaining a robust security posture in general, and protecting sensitive data assets in particular.

The global compliance ecosystem is highly complex:

- National and state data protection laws (all of which reference BCDR) such as those of the E.U. (GDPR), U.K., Australia, Canada and California (CCPA), to name but a few.
- Data privacy laws that cover specific domains such as HIPAA/HITECH for the U.S. healthcare industry, the Gramm-Leach-Bliley Act (GLBA) for U.S. financial institutions, and the Sarbanes-Oxley (SOX) Act for public companies traded on U.S. exchanges.
- Industry-specific, self-regulating frameworks such as the global Payment Card Industry Data Security Standard (PCI DSS) or the Basel Accords of the worldwide Basel Committee on Banking Supervision.
- Government agencies that develop and enforce compliance standards and best practices, such as FedRAMP and NIST Cybersecurity Framework in the U.S. or FINTRAC in Canada.
- Global IT communities such as the Center for Internet Security (CIS), whose benchmarks and best practices carry great weight in the compliance world.

Understanding regulatory compliance isn't easy; there is a lot to navigate. This white paper describes the BCDR requirements of a specific set of regulatory frameworks: HIPAA, PCI-DSS, and SOX, and sets out BCDR best practices that promote compliance.

NOTE: This document and any other related documentation on compliance produced by Acronis does not offer legal advice. Customers are solely responsible for evaluating and fulfilling their own legal and compliance obligations.



An overview of regulatory frameworks

This section provides snapshots of the three regulatory frameworks – Health Insurance Portability and Accountability Act (HIPAA); Sarbanes-Oxley Act (SOX); and PCI-DSS – with an emphasis on their key BCDR-relevant requirements. The sanctions for noncompliance are discussed in a separate section below.

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) was enacted on August 21, 1996 to improve the portability, security and privacy of electronic Protected Health Information (ePHI). It applies to Covered Entities and their Business Associates, in which a Covered Entity includes health plans (health insurance companies, health maintenance organizations [HMOs], and so on); clearinghouses that process nonstandard health information; and providers (such as doctors, clinics, nursing homes, and pharmacies) who submit electronic HIPAA claims. The Act came into force on April 20, 2005, and as of July 27, 2009, the Health and Human Services (HHS) Office for Civil Rights (OCR) became responsible for enforcement.

The HIPAA regulations are organized under three major rules: Privacy, Security, and Breach Notification. The issues related to BCDR fall within the Security Rule, which refers to administrative, technical and physical safeguards designed to:

- Uphold the confidentiality, integrity and availability of all ePHI received, maintained or transmitted
- Reasonably protect against anticipated threats to ePHI security or integrity
- Implement guardrails against unauthorized use or disclosure of ePHI

HIPAA takes a flexible approach, with a relatively small subset of rules being mandatory ("Required") and the others being recommendations ("Addressable"). Here is a summary of the mandatory safeguards and implementations that have an impact on BCDR activities:

- **Administrative requirements:**
  - Conduct a thorough and accurate risk analysis
  - Implement ongoing risk management
  - Make it clear who is responsible for HIPAA security compliance
  - Have sanctions in place for workforce noncompliance
  - Regularly review information system activity
- **Security implementations:**
  - A data backup plan, with processes to create and maintain retrievable and exact copies of ePHI
  - A disaster recovery plan, with procedures to restore any lost data
  - An emergency mode operation plan, including procedures to make sure that ePHI security activities continue uninterrupted

Sarbanes-Oxley (SOX)

This Act was passed in 2002 to counteract fraud in the wake of accounting scandals that undermined investor trust at Enron, WorldCom and other major corporations. The SOX controls apply primarily to publicly traded companies or companies considering an initial public offering (IPO). SOX is enforced by the Securities and Exchange Commission (SEC).

Although many of the SOX provisions are related to financial and accounting practices, appropriate management of corporate data is core to compliance. In general, data must be accurate, kept safe from internal and external threats, and available in near-real time to auditors and investors. More specifically, the source data used to generate financial reports must be traceable and any revisions to source data must be documented. Similarly, if you revise your financial or accounting software, you must fully document these changes.

The key rules related to BCDR and compliance are:

- Permissions to access electronic data should be strictly on an as-needed basis, and access should be tracked and verifiable
- Back up financial records at an offsite location.
- Implement demonstrable safeguards for protecting data against breaches
- Detected data breaches or other security control failures must be disclosed
- CEOs and CFOs are personally responsible for the integrity of financial reports and the internal controls that are put in place (and regularly audited) to meet the various SOX requirements.
- Formal, written data security strategy and data security policies enforced consistently
- Record and document compliance activities

PCI-DSS

This standard was put in place to protect the security of credit/debit card transactions and cardholder data. It applies to all organizations involved in card transactions such as banks, merchants, clearinghouses, and other service providers. PCI-DSS 1.0 was introduced in December 2004 and compliance is enforced by the major card brands who established the Payment Card Industry Security Standards Council (PCI SSC): American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.

Note: PA (Payment Application) DSS extends the PCI DSS requirements to new digital payment platforms and adds core requirements for solutions vendors.

PCI DSS Requirement 12 focuses on establishing, publishing, maintaining and deploying an information security policy, including establishing and implementing a risk-assessment process. Section 12.10 mandates the creation and implementation of an incident response plan that ensures a quick and unified response to a data breach. The incident response plan must include the establishment of business recovery and continuity procedures as well as data backup processes. The incident response plan should be reviewed and tested at least once a year.

Best practices to keep you in line with BCDR obligations

This section outlines organizational and technical best practices that will keep your organization aligned with BCDR regulatory requirements.

Organizational

As with any strategic initiative, BCDR starts with a comprehensive plan that aligns an organization's business continuity program with their goals and environment. It's important to conduct analyses that identify clearly which business activities are most critical to continuity and what the risk level is of each of those activities. Aside from the essential insights that the business impact and risk analyses provide for setting focused BCDR objectives, the process of conducting them puts business continuity squarely on the corporate agenda. An effective business continuity program must have buy-in across the organization.

An organization may have a single unified business continuity plan, or it may develop separate plans for different business units and functions. However, in either case, there must be a clear framework for BCDR governance. Who is overall accountable for business continuity management? Have they been given appropriate authority to enforce compliance within the organization? What resources – both budgetary and personnel – have been allocated to design, implement and manage the business continuity plan?

Organizations that are subject to regulatory frameworks such as HIPAA, SOX, and PCI-DSS will have to undergo external audits from time to time to ascertain compliance. It is important that these organizations regularly conduct their own internal audits and reviews to test and assess the effectiveness of their BCDR policies, procedures and controls. Any weaknesses revealed by these internal audits should be immediately addressed and the plan updated accordingly.

Backups and restores

HIPAA, SOX, and PCI-DSS all address the need to safely back up data assets in order to be able to recover from data loss, corruption or inaccessibility scenarios. There are a number of best practices that contribute to backup compliance:

- **Frequency and retention:** Regulatory frameworks generally take a risk-based approach, which means that the appropriate cadence of data backups and how long they must be retained are determined by the data assets' criticality and risk profile. Real-time data in the production environment needs to be backed up continuously, while data sets used in staging or test environments can be backed up far less frequently
- **Snapshots:** For active data that ought to be backed up in real time, consider deploying snapshot technology that maintains metadata about where each block of data is stored. The snapshot updates incrementally whenever a data block is changed, deleted or added. Snapshots promote granular versioning and have small storage and bandwidth footprints compared to full backups.
  Tip: Using snapshots does not exempt the organization from conducting full backups on a regular basis
- **Location:** All of the regulatory frameworks require that data backups be stored in an accessible but separate location from the primary data assets. There are numerous options for meeting this requirement – from storing backups on removable media in an offsite physical facility to automatically mirroring on-premises or primary cloud data stores in a secondary public cloud environment
  Tip: Consider leveraging the automated, compliant and durable backup/restore services offered by the leading public cloud providers for their storage-compute-network resources, such as AWS Backup, Azure Backup or GCP's Actifio GO.
- **Security:** Data backups must be encrypted both in transit and at rest. In addition, all corporate security policies and threat protection controls should be applied to data backups, including access permissions and privileges (which should be based on a minimalist, zero-trust approach)
- **Data integrity checks:** Don't just assume that your data backups or replicas are faithful reflections of the primary data to be protected. Data can be lost or corrupted during the backup procedure. Put measures in place for spot checking the integrity of backup files as they are created, as well as periodic data integrity checks that validate backups by simulating restore procedures
- **Restores:** The organization should have clear and documented workflows that describe when a restore procedure should be initiated and who is authorized to do so. From a compliance point of view, it is important that the restore be conducted securely, including encryption of data in transit and a destination that meets the frameworks' security and privacy requirements. And don't forget that the restore procedure must include steps for verifying that the restore was successful, without loss of data integrity

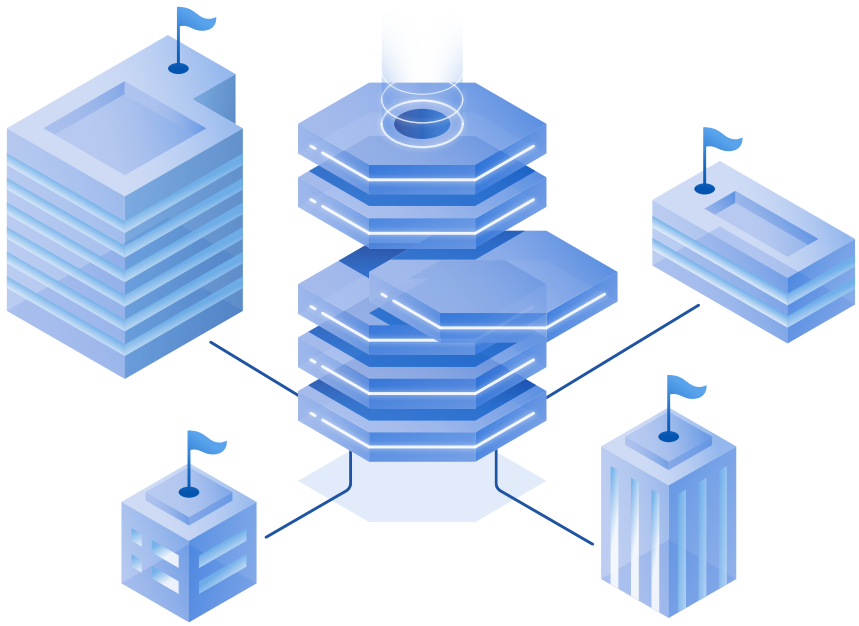
Note: In addition to data backups, the organization should also maintain up-to-date and accessible repositories of critical software as well as their configuration settings, such as OSes, applications, databases, and more.

Disaster recovery

A good disaster recovery (DR) plan lets the organization maintain resilience in the face of a full-fledged disaster and can be considered the true test of a business continuity program. DR plans are organized around Recovery Point/Recovery Time Objectives, where RPO is the maximum acceptable data loss and RTO maximum acceptable downtime before business continuity is compromised.

The regulatory frameworks expect mission-critical applications and data to have zero (or near-zero) RPO/RTO. Here are some best practices that can help your company achieve these ambitious metrics:

- **Fully documented plan:** The plan, which should be continuously maintained and accessible to all stakeholders, must outline all the roles and responsibilities, full contact information for personnel and facilities, what triggers the plan and what criteria determine that procedures can return to normal.
- **Data mirroring:** You must implement a high-availability data-synchronization/mirroring solution, which is typically based on snapshots as described above.
- **Full working replica of the production environment:** It's not just data that has to be mirrored; it's the whole infrastructure. A DR site should be ready to kick in as a production environment at a moment's notice so you have to maintain it on an ongoing basis, including software licenses, patching, upgrades and so on.
- **Choosing the DR remote colocation/location:** On the one hand, the DR site should not be hosted too close to the primary facility in order for it to be safe from the local disaster conditions that make it necessary. On the other hand, it should be feasible for IT personnel to access the facility physically, in addition to being able to activate it remotely.
- **Testing:** The last thing you want to happen when handling a disaster is to find out that the DR plan doesn't work. The DR plan must include a system for periodically testing all functionality (such as data recovery, failover and failback, access to remote data, stress testing and more), with clear success criteria (including RTO and RPO).



The perils of noncompliance

Noncompliance with these regulatory frameworks can result in penalties and fines of varying severity.

HIPAA sanctions

HIPAA violations can result in both civil and criminal penalties that are tiered based on the level of negligence or malicious intent. Tier 1 civil violations are those that the Covered Entity, despite reasonable due diligence, is not aware of and are subject to a fine of $100 to $50,000 per violation, with an annual maximum of $25,000. Tier 4 civil violations, on the other hand, are the result of willful neglect with no corrective effort after discovery and are subject to a fine of $50,000 per violation to a maximum of $1.5 million per year.

Knowingly obtaining or using ePHI for reasons not permitted by the HIPAA Privacy Rule can result in criminal penalties. The highest tier of criminal violation (Tier 3, in which ePHI is obtained for personal gain or with malicious intent) can result in a fine and a jail sentence of up to 10 years.

Some examples of recent HIPAA settlements:

- January 2021: A health insurer paid $5.1 million to the OCR to settle a data breach that affected ~9.3 million people
- September 2020: A HIPAA Business Associate paid a $2.3 million fine and submitted a corrective action plan for a breach that affected more than 6 million people and for systematic noncompliance with the HIPAA Security Rule
- September 2020: A health insurer paid a $6.85 million fine for a data breach that affected over 10.4 million people
- July 2020: An institutional health provider paid $1.04 million to settle a breach involving an unencrypted stolen laptop

SOX penalties

Sarbanes-Oxley noncompliance can result in corporate fines of millions of dollars and other penalties, including being delisted from public stock exchanges. And there doesn't even have to be an outright violation. Failing to correct disclosed noncompliant internal controls over financial reporting has also resulted in SEC charges and settlements.

SOX Section 906 holds corporate officers directly liable for violations. For example, a CEO/CFO who knowingly approves a noncompliant financial report faces a fine of up to $5 million or a prison term of up to 20 years. But even an individual who mistakenly violates the Act can be sent to jail for up to 10 years and subject to a fine of $1 million.

Although rarely enforced, SOX can also require a noncompliant corporate officer to give back incentive-based compensation under what's known as the clawback clause.

Last but not least, SOX protects employees who report violations ("whistleblowers") from retaliation, such as termination of employment. The courts have awarded generous compensation to whistleblowers who have shown that their employers violated the SOX provisions in this matter.

PCI-DSS violations

PCI SSC can fine an acquiring bank $5,000 to $100,000 per month for PCI-DSS compliance violations. The payment processor will seek to pass the fine along to the merchant, sometimes indirectly via increased transaction fees. Fines are evaluated each month, and if the merchant's status remains non compliant, the fee will be increased. An SMB that fails to comply with PCI-DSS and faces, for example, a $100,000 per month penalty for a period of three months, could well go out of business.

In addition, an actual data breach experienced by a noncompliant merchant could result in a $50 to $90 fine per affected consumer, up to $500,000 per incident. Affected consumers must also be notified, which can be a costly process as well.

Aside from fines, one of the worst consequences can be freezing a merchant account or adding a merchant to the Terminated Merchant List. Banks will refuse to do business for extended periods of time (usually at least five years) with merchants on this list. And while this sanction is typically reserved for perpetrators of fraud and other serious violations, persistent noncompliance can also be a cause for being added to this list.

It should be noted that, as a self-regulating body, the PCI SSC is under no obligation to publicize fines and sanctions. This inherent lack of transparency can make it difficult for merchants to contest imposed penalties.

Conclusion

Being able to respond resiliently to IT disruptions has become a business-critical KPI. Whether the disruption is localized and short-lived or extensive and highly impactful, customers, employees, partners, and, in many cases, regulators expect a business to be able to restore normal IT operations in near real time and with near-zero data loss. Regulatory frameworks such as HIPAA, PCI-DSS, and SOX set out business continuity and disaster recovery (BCDR) expectations, mandatory requirements and recommended best practices. It is up to each company to understand which regulations apply to its activities and to stay compliant with those regulations.

The direct costs of noncompliance in the form of penalties, fines, and sanctions are very significant. And there are also indirect costs, such as loss of revenue, damaged reputation and loss of trust. Companies, therefore, are highly motivated to be and stay compliant with their BCDR obligations.

BCDR compliance best practices include:

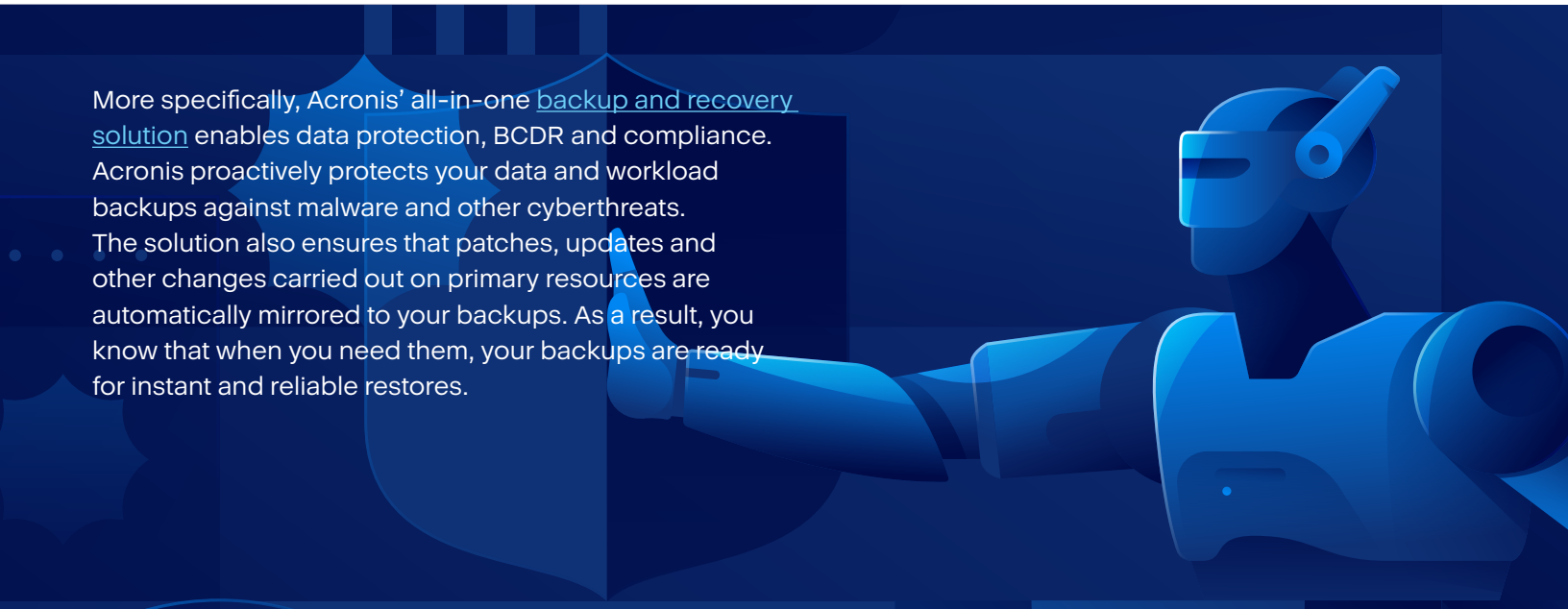
- Organizational activities such as strategic planning, getting cross-organization buy-in, and clear governance guidelines
- Frequent backups of data and critical software to secure offsite locations, regular data integrity checks, and tested restore procedures
- Maintaining a synchronized mirror failover site that takes over if the primary site goes down as part of a fully-documented and tested disaster recovery plan

How Acronis can support your BCDR program

Headquartered in Switzerland and Singapore, Acronis is a global company that for close to two decades has provided best-in-class, unified data protection and cybersecurity solutions to home offices, businesses of all sizes and service providers. Although you can choose to deploy Acronis' backup, security, disaster recovery and enterprise file sync and share solutions on premises, our commitment to keeping BCDR programs compliant starts with how Acronis manages cloud data centers for Acronis Cyber Cloud:

- Geographic distribution: With data centers in the U.S, U.K., Canada, Japan, Singapore and various locations in Europe and other regions, customers can choose a location that suits their compliance requirements. This geographic distribution also allows Acronis to maintain high-availability DR replica sites
- Physical security: Strict access management and controls ensure that only authorized personnel have physical access to data centers. Acronis' data centers are under constant CCTV surveillance. A minimum of two independent power sources ensures an uninterrupted 24/7 power supply
- Certifications and regulatory requirements: Acronis' information security policies and processes are certified per international security standards such as ISO/IEC 27001//9001, and are inline with industry best practices and requirements like NIST, GDPR and HIPAA
- Infrastructure and network security: High-availability, redundant hardware-layer infrastructure eliminates single points of failure and supports interruption-free scheduled maintenance
- Acronis implements advanced cybersecurity solutions and best practices to monitor for and prevent unauthorized access and cyberattacks. In addition, data at-rest and in-transit, as well as cryptographic keys, are encrypted
- Secure multi-tenant data storage environment: Physical and logical isolation ensures complete separation of each customer's data, with strict access controls based on Need to Know and Least Privileges principles. Immutable logs track all access attempts for auditing purposes. Acronis' proprietary software-defined storage solution – including API integrations with trusted business associates – provides high levels of data protection at scale – including efficient self-healing capabilities

More specifically, Acronis' all-in-one backup and recovery solution enables data protection, BCDR and compliance. Acronis proactively protects your data and workload backups against malware and other cyberthreats. The solution also ensures that patches, updates and other changes carried out on primary resources are automatically mirrored to your backups. As a result, you know that when you need them, your backups are ready for instant and reliable restores.



Acronis

Learn more at
www.acronis.com