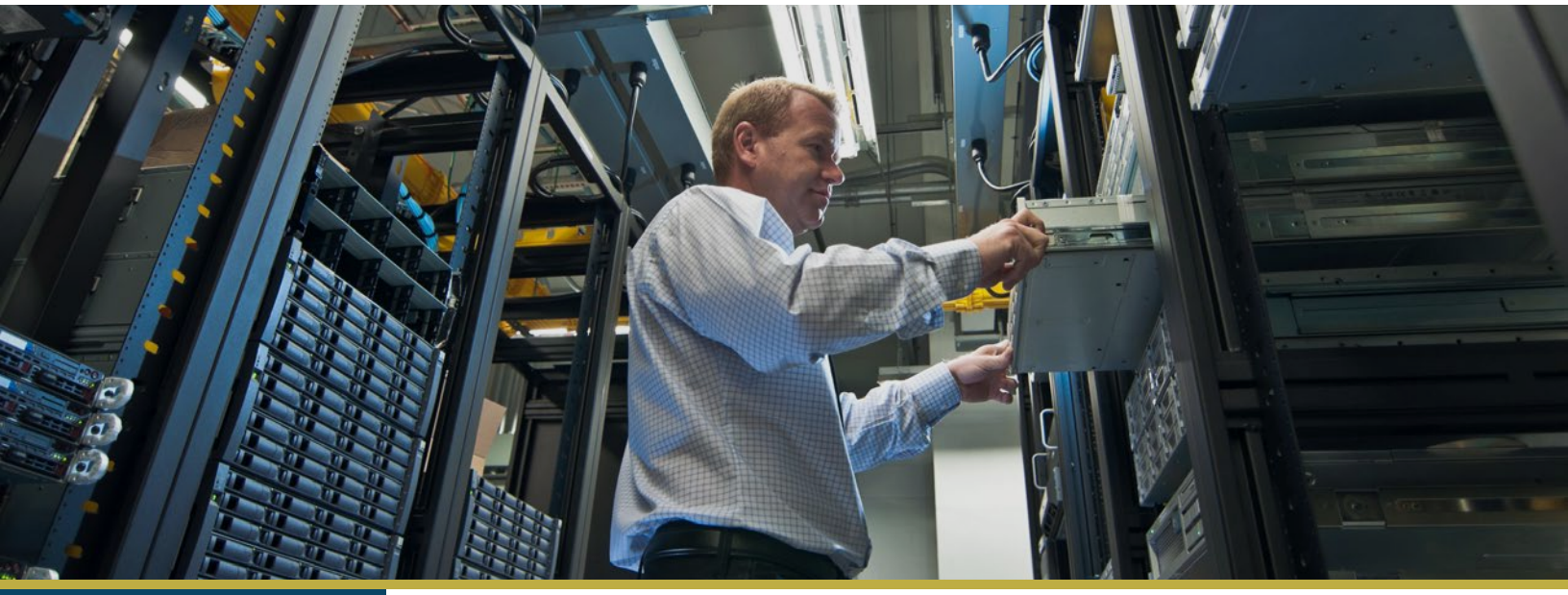
Petri IT Knowledgebase Resource
A BWW Media Group Brand



Protecting and Securing Your Critical Data with Acronis Backup

Security is the first and foremost consideration for effective data protection and business continuity in today's IT environment. While security might not seem to be a necessary component of data protection, an effective security strategy is absolutely necessary to truly protect your organization's critical data. Backup is the underpinning of every business's data protection strategy, but data protection is not an isolated activity.

To truly enable data protection security, you must deeply integrate it into backup and data protection processes. Businesses today are faced with far more invasive and potentially damaging threats than at any time in the past. Your organization's IT security is the first line of defense against incidents that can cause business interruption and data corruption.

Despite increasing attention to security, backup procedures are often neglected in overall security policies. Like the old adage says, an ounce of prevention is worth a pound of cure: stopping threats before they can cause irreversible data corruption can save your business the cost and effort of data restoration. In some cases, it can make the difference in your company's survival.

Sponsored by
Acronis

It's important to recognize that your backups contain all of your private and potentially sensitive company data. Unauthorized access or hacking into backups can result in the theft of intellectual property as well as the exposure of information that could potentially damage your business.

Securing backups is essential. Considering that many businesses today are taking advantage of the cloud to externally store backups, it's equally important to be sure those backups have multiple layers of protection.

The most critical feature of any backup solution is its ability to meet low recovery time objectives and recovery point objectives (RTOs and RPOs). These enable you to proactively avoid downtime caused by malware. RTO defines how long you can go without access to your data; RPO defines how much data loss your organization can tolerate. Today's threats go beyond simple data loss and recovery from failures. Backup solutions also require tightly integrated security features to enable better business continuity and protect critical data from threats like external hackers, insider attacks, and a broad array of malware, including ransomware.

In this whitepaper, you'll learn about the challenges of protecting and securing your business' private data. You'll also see how Acronis Backup provides a unique and highly secure approach to protect your critical data, increase your recovery speed and avoid downtime caused by today's malware threats, especially ransomware, the fastest-growing and most destructive, recent malware strain.

The Growing Dangers of Ransomware

Today's data protection plans need to include protection from ransomware attacks. These attacks are becoming far more frequent and can result in serious downtime and data corruption. Malware is hostile or intrusive software that invades servers, PCs, laptops, tablets and mobile devices for malicious purposes, such as stealing, altering or destroying data. Ransomware is a particular virulent new form of malware that encrypts the data on an infected system and illicitly tries to extort a payment from the target in exchange for the decryption keys needed to unlock the data.

Eric O'Neill, former FBI counter-terrorism and counterintelligence operative, explains that "businesses today are up against a rising tide of threats. Cybersecurity threats and data espionage are more prevalent than at any other point in our history – contributing to an anticipated $2 billion loss due to ransomware this year. What is scarier is malicious attacks are no longer limited to hackers; Ransomware-as-a-Service kits can be purchased for a mere $39 by anyone with low moral standards and a desire to generate a few dollars."

Security researchers and law enforcement agencies are forecasting that the threats posed by ransomware will continue to rise, making the ability to secure and recover your data from such attacks more important than ever. The damage caused by ransomware isn't just restricted to your production systems. It can also attack and destroy replication targets and backups.

The Value of Data and the Costs of Downtime

There's no doubt that downtime is very expensive. According to Gartner, the average cost of downtime for all types of businesses is $5,600 per minute, which equates to roughly $300,000 per hour. Information Technology Intelligence Consulting (ITIC) conducted a more granular study, showing that for 98% of businesses, a single hour of downtime costs more than $100,000. For 81% of business that hour of downtime costs more than $300,000 and for 33% of larger businesses an hour of downtime costs $1 million to over $5 million. The average cost of unplanned downtime has risen by 25% to 30% since ITIC first began tracking downtime in 2018.

Downtime has more than just financial consequences as well. It can also have a major impact on the

business itself. The U.S. National Archives & Records Administration reported that 93% of companies that lost their data center for 10 days or more during a disaster filed for bankruptcy within one year of the disaster. According to the University of Texas 43% of companies that suffer catastrophic data loss never reopen and 51% close within two years. Similarly, Boston Computing Network's, data loss statistics showed that 30% of all businesses that have a major fire go out of business within a year and 70% fail within five years.

Threats to Your Critical Data Backups

Today, simply producing backups isn't enough to ensure the safety of your business-critical data. The threats to your data have rapidly evolved in recent years, so the traditional backup approach (just copying data) is not enough to truly protect and secure it. In fact, traditional backup solutions may create a false sense of security, letting you believe that your data and backups are protected until a future restoral attempt renders them useless due to malware infection or data corruption. Some of the biggest threats to your critical data include:

Modern threats that can bypass traditional signature-based antiviruses.

- Malware strains that intentionally search for and destroy backup files.
- Threats that corrupt backup software executables
- Obsolete backup applications that are not designed with security in mind, offering weak or no encryption, or using an outdated architecture with multiple points of vulnerability and failure.
- Backup applications from vendors that only produce software and do not have end-to-end experience.

The threats to your company's data are continually evolving. It's not enough anymore to just make a backup copy of your critical data. A new generation of threats target your backups as well as your data. For instance, the ransomware Zenis encrypts your files and purposely deletes backups. Likewise, Locky and Crypto ransomware are known to destroy data shadow copies as well as data restore points.

To ensure a truly secure backup, you need security-rich protection for your entire IT infrastructure and data, including physical systems, virtual systems, cloud services, and mobile devices, plus the corresponding

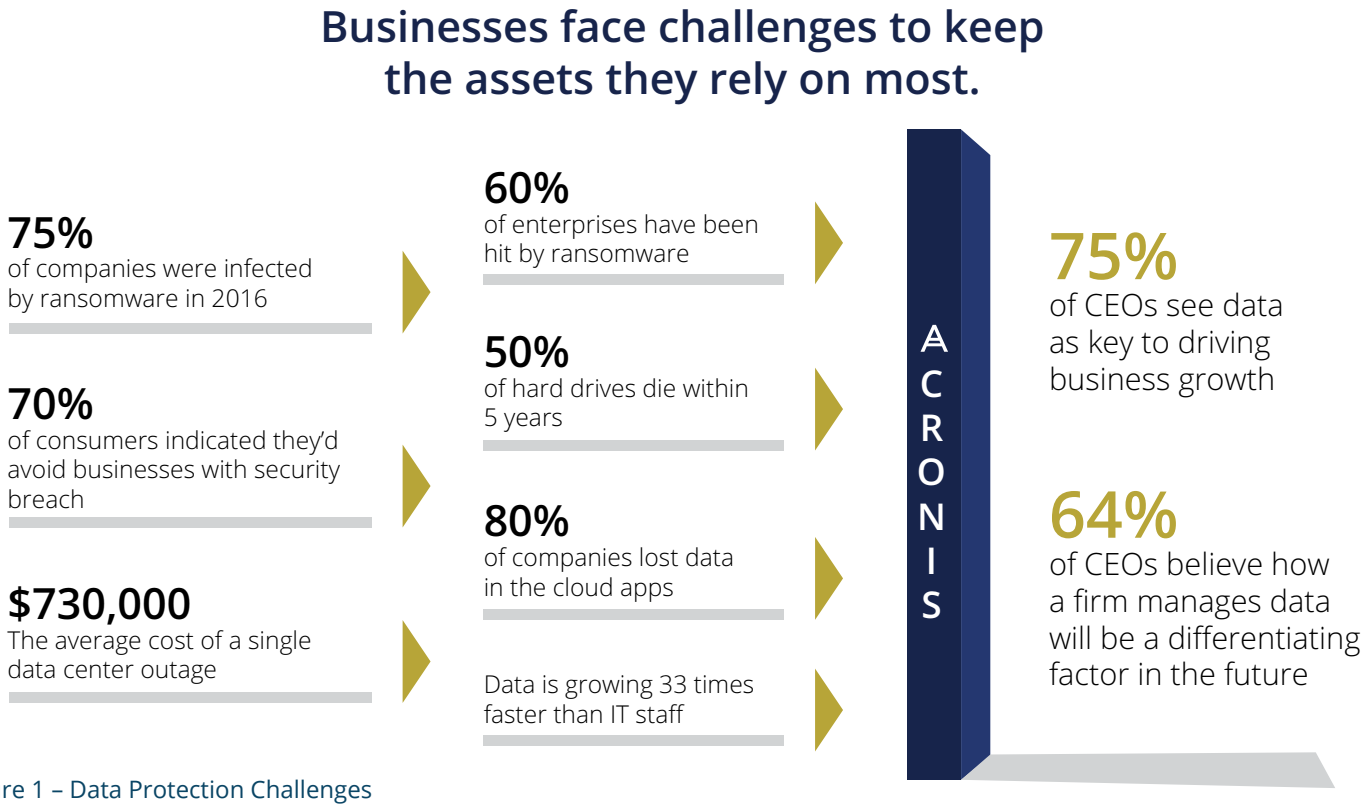


Figure 1 – Data Protection Challenges

backups for these devices. Today's businesses need to add a layer of security on top of their backups to both proactively prevent data downtime and data exposure as well as automatically detect and correct data corruption.

Sid Deshpande, principal research analyst at Gartner explains, "The shift to detection and response approaches spans people, process and technology elements and will drive a majority of security market growth over the next five years. While this does not mean that prevention is unimportant or that chief information security officers (CISOs) are giving up on preventing security incidents, it sends a clear message that prevention is futile unless it is tied into a detection and response capability."

You need to ensure that you can restore your backup by securing your backup process at every stage, taking care to securely store your backup files. You need to be able to select multiple different points in time to restore. Your data protection solution needs to protect you from downtime by proactively preventing attacks and automatically restoring data in case of an attack.

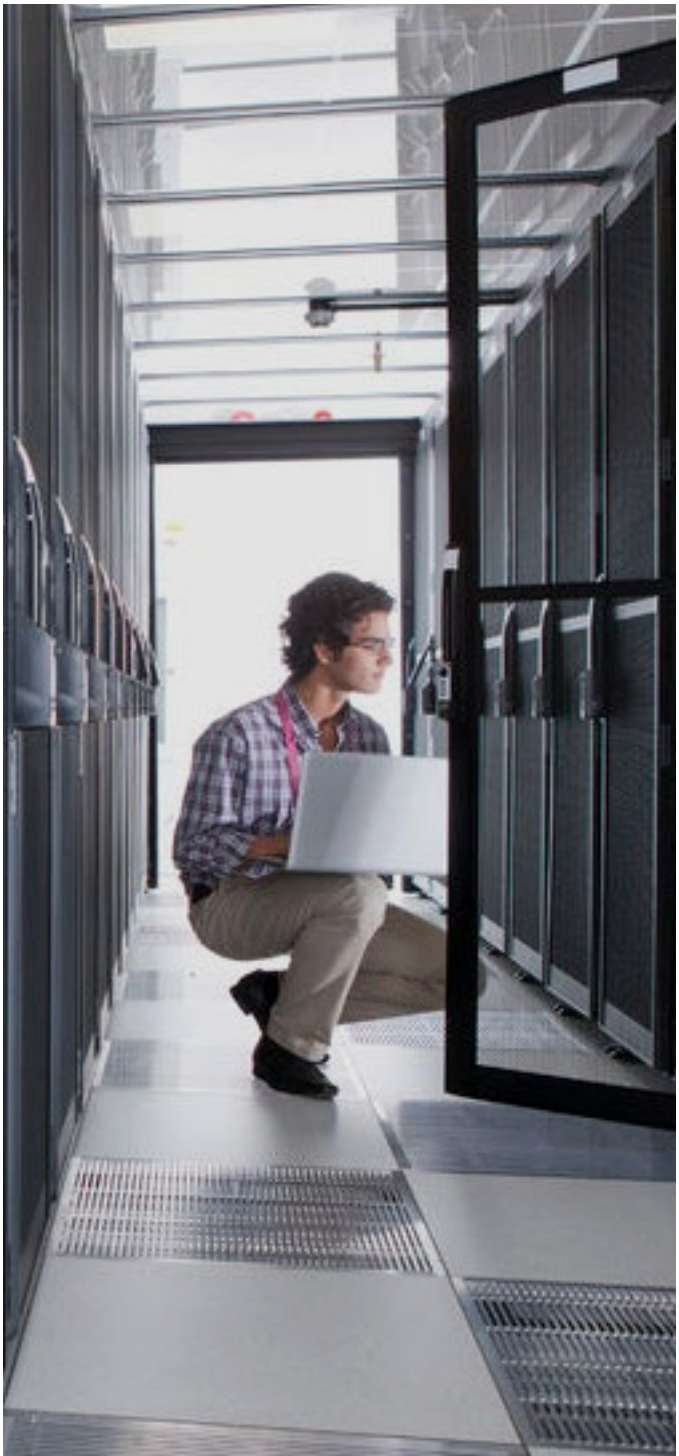
Let's look at the core backup and recovery features built-in to Acronis data protection products. Then we'll dive into their advanced security capabilities.

Advanced Data Protection Capabilities in Acronis Backup

Acronis Backup addresses today's modern data protection threats. It provides a complete data protection solution for hybrid IT environments that can back up and recover physical, virtual, cloud and mobile device data as well as proactively prevent and defend against malware and ransomware attacks.

Acronis Backup supports 21 of today's popular platforms, including Windows Server 2016 back to Windows Server 2003 and Windows 10 back to Windows XP SP3. It supports all of the current Linux distributions, including Red Hat Enterprise Linux 4.x — 7.4, Ubuntu 9.10 — 17.04, Fedora 11 — 24, SUSE Linux Enterprise Server 10 — 12, Debian 4 — 9.2, and CentOS 5.x — 7.4. It also supports Apple OS X 10.11 and later versions, macOS 10.13, iOS 8 and later versions, and Android 4.1 and later versions. Acronis Backup also supports all of the most popular hypervisors, including VMware vSphere, Microsoft Hyper-V, and Citrix XenServer.

Indeed, Acronis Backup provides a number of advanced data protection and recovery features that enable you to secure your backups as well as lower your RTOs and RPOs.



Acronis Instant Restore reduces RTOs by running VMs directly from backups

Acronis Instant Restore enables you to vastly reduce your recovery times by using your backup to immediately start a Windows or Linux virtual machine directly from storage. As no data is being moved, you can start your backup VM and get it up and running in seconds. To make this happen, the Acronis agent on the host creates a virtual datastore that allows the host to read directly from the backup and start the VM. Changes to the VM are written to a temporary file on the host – all in a manner that is completely transparent to the virtualization host.

Remote and bare-metal recovery reduce RTOs with direct restore capabilities

Bare-metal restore enables you to accelerate your recovery by restoring a full system backup on a computer that has an empty system drive. This allows you to avoid a lengthy OS installation before running your restore processes. There's no need to reinstall backup or other applications. You can immediately restore from a complete system image. Built-in smart-boot technology automatically detects the system's startup requirements. If your computer has been infected by a virus or ransomware then recovery from the bare-metal image eliminates any malware that may have been present. You can also perform remote recoveries by connecting to the Linux-based Acronis Bootable Agent from a networked system using the Acronis Management Console.

Acronis Universal Restore enables backups to be restored to dissimilar systems

Sometimes when you try to use an entire disk image to recover to a new system with hardware that is not identical to the original machine, the recovery can fail because the system failed to boot. This can often be attributed to boot drivers in the backup image that do not match the new hardware requirements. Acronis Universal Restore solves this problem by reconfiguring the target operating system before booting, first by analyzing the target system, then changing any relevant OS settings and injecting any new drivers required to successfully boot the system. Universal Restore can also be used to perform migration between physical and virtual machines.

Granular recovery of individual files and emails

One of the most common user requests is to restore single items that have been accidentally deleted. Acronis Backup enables granular recovery by powering searches for specific documents, like files and emails, then restoring them individually without having to recover the entire backup. This significantly reduces RTOs and operational efforts.

Rapid vSphere restores with vmFlashback

Acronis vmFlashback enables fast VMware vSphere VM recovery by selectively restoring only the virtual hard disk data blocks that have been changed since the last backup, foregoing the need to restore the entire VM. Acronis vmFlashback uses VMware's Changed Block Tracking (CBT) technology to track and save only blocks of information in a VM backup that have changed since it was created. CBT identifies the disk sectors that have been changed by comparing special change set IDs. When a restore is required, CBT provides a list of changed disk blocks by comparing the disk IDs from the backup to the current virtual disk set IDs, then restoring only the changed disk blocks.

Acronis Provides a Secure and Technologically Unique Backup Solution

Acronis Backup provides a unique backup security solution that goes beyond simple protection of your backup files. A completely new generation of data protection technologies have been built into the

fundamental core of the Acronis Backup application by a team of security experts with experience at leading global security vendors.

Acronis has rebuilt its core backup application, incorporating the newest approaches to data security. Acronis Backup now utilizes microservices, the Go programming language, and new engineering practices in the product's development lifecycle. Using a team of ten dedicated security experts, Acronis has implemented a Secure Development Life Cycle (SDLC) that utilizes security-focused code and design review processes. Each version of Acronis Backup is built in our lab in Schaffhausen, Switzerland, and signed as it is released. Acronis Backup is fully TAA compliant and features more than 100 patents in data protection and security. Acronis Backup provides a number of tightly integrated security features that enhance enterprise data protection capabilities.

Acronis Active Protection protects executables and data from ransomware

Unlike most other backup software solutions, Acronis Backup is built on a secure architecture called Active Protection that prevents it from becoming compromised by malware and ransomware. Acronis installs a special protected driver on the system that monitors systems files, executables and data. Active Protection detects unexpected malware activity and prevents any possible corruption of the Acronis Backup executable programs. Acronis can detect and halt a ransomware attack, and any data that was corrupted by the attack can be recovered and restored from a protected Acronis backup archive.

Backup encryption prevents unauthorized access

To provide better protection from brute-force attacks, Acronis has strengthened its backup encryption and traffic encryption. Acronis Backup supports industrial-grade AES-128, AES-192, AES-256 and GOST encryption algorithms, and uses machine-based encryption with a different key for each individual machine. Backup users can select the algorithm and set the password used for encryption. The Acronis agent handles key creation. Users also have the option to avoid storing encryption keys in the Acronis Management Server (AMS) or the cloud. The password you assign to the backup is not stored as a part of the backup and cannot be retrieved. This provides an extra level of protection from targeted malware attacks by ensuring that passwords cannot be found in the Acronis agent, program files or backups. This protects your critical backup data and prevents it from being compromised even if a hacker somehow gains unauthorized access to it.

Secure modern storage format and Acronis Notary blockchain authentication

In addition, Acronis Backup uses the new and improved Archive 3 storage format to strengthen backup storage security. Archive 3 is a modern format designed for both block and file level environments. It supports up to a billion files, 100,000 slices and a 50 TB archive size. The Archive 3 format supports asynchronous data access, fast browsing and paging. It also provides built-in block-level deduplication and adaptive compression using the ZSTD/LZ4 algorithms.

Data encryption support separates encryption keys and passwords enabling you to change passwords without requiring re-encryption. Secure storage provides a first line of defense for your critical backup data. Acronis Backup storage is European Union (EU) General Data Protection Regulation (GDPR), ISO 27-001, and HIPAA compliant. Acronis Backup replication can be used to copy your backups to a secondary location.

Acronis has also pioneered the use of blockchain for data protection. The Acronis Notary features uses blockchain to provide notarization and electronic signatures of backup files. Blockchain enables the integrity of your backup files to be verified, ensuring that they have not been altered. To verify and protect data backups, Acronis Notary computes a cryptographic hash that is unique for each file. The algorithm that creates this hash will always produce the same output for a given input file, enabling it to verify the file's authenticity.

This ensures archived backups have not been altered or corrupted by malware and that they can be used to restore your critical data.

Role-based access provides administrative delegation and remote access

To provide flexible administrative functionality, Acronis Backup uses a role-based access model. This feature lets you easily manage data protection for your remote offices, branch offices, and individual departments by establishing different roles for multiple administrators and delegating different backup tasks to local personnel.

Acronis uses two types of roles:

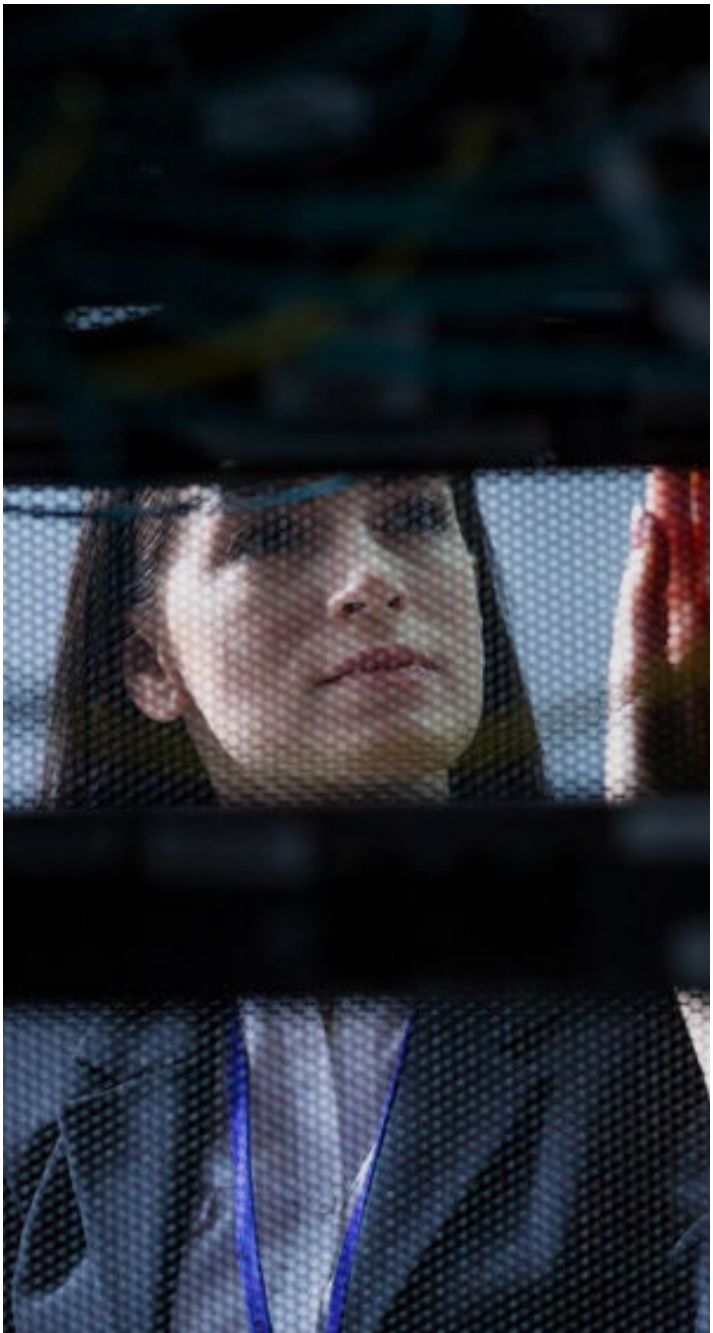
- Regular users – Regular users can perform file-level backup and recovery of any files for which have permissions. They can create and manage backup plans and tasks, and view backup plans and tasks created by other users.
- Administrative users -- Administrative users can perform file-level backup and recovery of all data on a system and can back up and recover the entire machine. They can create and manage backup plans and tasks for different users.

Acronis Backup provides centralized and remote management of backups to make it easier to protect data that resides in remote locations, private clouds, public clouds and mobile devices. Remote backup administration can help reduce the RTOs of remote systems by accessing bootable media and restoring bare-metal servers remotely across remote Internet connections.

Secure cloud data protection

Acronis Backup includes 5 GB of free cloud storage, enabling all active customers to start storing their most critical data in the cloud. Acronis Cloud Storage is fully integrated into Acronis Backup. Users have the option to store encrypted data on the Acronis Cloud. The purpose-built, highly reliable and secure Acronis Cloud Storage uses the scalable and secure Archive 3 data storage format.

By leveraging the cloud, you can create hybrid cloud backup plans that implement the 3-2-1 data protection strategy, i.e., keeping at least three copies of your data on at least two different media with at least one off-site storage location. The Acronis Cloud can be used to store an additional backup copy on cloud storage media in an off-site location. Acronis Backup can also replicate archives to Amazon Web Services (AWS), Microsoft Azure, or another remote data center for added backup data protection.



Acronis Backup Integrates with Popular Endpoint Security Solutions

Malware variants like ransomware can disrupt business operations, destroy critical data, reduce cash flow, dilute customer and partner trust, and reduce profit margins, as when frightened customers and partners begin returning products or asking for discounts. Acronis Backup is designed to integrate with other endpoint security solutions, increasing the overall scope of protection for an organization. To provide protection from malware strains like ransomware, Acronis Backup is integrated with most anti-virus solutions, providing deep kernel-level protection for all major computing platforms.

Acronis' security strategy focuses on leveraging and integrating with existing protection technologies -- not replacing them. It uses a single agent that shares low-level interceptions for both backup self-protection and defense against malware attacks.

Acronis Active Protection proactively detects attacks before they occur and provides an active defense of endpoints and backups to terminate attacks in progress. Acronis Backup can restore all files after an attack. This unique, proactive technology prevents system downtime caused by 99.99 percent of ransomware attacks. Any files impacted by an attack are quickly, automatically restored.

Acronis combines its expertise in malware protection, backup, artificial intelligence (AI) and machine learning (ML) to provide total control of the executable lifecycle on protected systems. Acronis has been thoroughly proven and tested in many real-world production environments, achieving a record of successfully defeating over 200,000 ransomware attacks, and protecting over 5000 petabytes (PBs) of customer data at more than 500,000 customers. In the past 12 months, Acronis Active Protection also stopped 200,000 attacks against 180,000 consumer devices.

Johnson Electric Blocks Ransomware Attacks with Acronis Backup

Johnson Electric, one of the world's largest providers of motors, solenoids, micro-switches, flexible printed circuits and micro-electronics adopted Acronis Backup to better protect their critical data and to block ransomware attacks.

Before implementing Acronis, Johnson's Ohio office suffered a series of four ransomware attacks that their existing antivirus protection failed to detect. The total downtime was more than 30 hours. After the attacks, Johnson Electric adopted Acronis because it was the only backup solution that could address both data protection as well as data security.

Since adopting Acronis Backup Johnson Electric has not suffered any further ransomware attacks. Johnson Electric network administrator Joel Stuart said, "ransomware was a major point of concern for us. With the innovative features such as Acronis Active Protection against ransomware, we are implementing the strongest defense on the market today. And the Acronis Notary technology available in 12.5 is strategically important to us for the future."

Acronis Joins AMTSO Strengthening its Malware Protection

In April 2018, Acronis joined the Anti-Malware Testing Standards Organization (AMTSO) to make its data protection solutions even more secure. The AMTSO is an international non-profit association focused on addressing the global need for improvement in the objectivity, quality and relevance of anti-malware testing methodologies.

As a part of the AMTSO, Acronis adheres to evaluation standards for data protection products and takes part in establishing protocols and procedures for future technologies, thereby improving security testing practices within the industry. The new partnership enables Acronis to leverage objective and statistically significant testing methodologies to provide comprehensive and secure data protection, as well as tapping into the AMTSO's Real Time Threat List (RTTL) database.

Acronis Backup Provides Modern Secure Data Protection and Recovery for Your Business

Acronis Backup provides a unique, comprehensive and secure data protection platform for your business-critical data and backups. It offers a number of fast recovery options that will lower your RTOs and RPOs. In addition, it provides many advanced and unique security capabilities to protect your critical data from unauthorized access, insider attack, and malware variants including ransomware.

Acronis Backup uses strong encryption and built-in Active Protection anti-malware technology with deep kernel-level support of all major computing platforms that makes them highly resistant to ransomware. Its unique integration with leading anti-virus products adds an extra level of defense against fast-growing security threats like ransomware. The secure data protection capabilities in Acronis Backup are specifically designed to defend your organization's critical data from these fast-growing and potentially lethal threats.

Acronis Backup comes in both Standard and Advanced Editions. Designed for small and medium businesses, the Standard Edition provides essential advanced data recovery capabilities and integrated malware protection. The Advanced Edition is designed for mid-market businesses and enterprises, offering extended functionality to support larger organizations, including centralized storage with deduplication, role-based administration, blockchain-based data protection, Acronis Instant Restore, and automated bare-metal recovery. Learn more about Acronis Backup at Acronis Backup Key Features.

Acronis