Why Choose **Acronis**?

Businesses need more than prevention. They need the certainty that when something goes wrong, they can recover fast, stay compliant and keep operating — without complexity or compromise.

Six reasons why Acronis has got you covered...

1 AI-powered recovery: Clean, verified and malware-free

Acronis uses AI-powered behavioral detection to identify and stop threats in real time, including zero-day attacks. When recovery is needed, AI-assisted scanning validates every restore point is malware-free before it reaches production. This prevents reinfection and ensures you restore to a trusted, clean state every time, not back into an active attack.

2 Disaster recovery that activates in minutes

Traditional backup can leave your business offline for hours or days while systems are rebuilt. With Acronis Disaster Recovery, critical workloads failover to the Acronis Cloud in minutes, keeping your teams productive while your primary site is restored in the background. The DR infrastructure and orchestration platform are fully managed by Acronis, while you retain full control over initiating and managing failover via the management console.

3 One agent for backup and active security: no bolt-ons needed

Unlike vendors that pair a backup tool with a separate security product, Acronis runs a single lightweight agent on every endpoint that performs backup, anti-malware scanning, URL filtering, patch management and endpoint detection and response together. There is no second agent to deploy, no separate console to manage and no gaps between protection layers. Security is built into the backup, not added on top of it.

4 Protect any environment by failing over to the Acronis cloud

Whether your infrastructure runs on physical servers, VMware, Hyper-V, Nutanix or Proxmox, or in public clouds, Acronis protects it all from one platform. In the event of an outage, workloads failover to the Acronis Cloud, a fully managed environment with free hot storage included where you can run test failovers at no additional cost.

5 Immutable backups that support compliance and withstand attacks

Ransomware increasingly targets backup archives to block recovery. Acronis backups are immutable — once written, they cannot be altered, encrypted or deleted. Combined with a 3-2-1 approach, your recovery options stay intact, no matter what. These same capabilities support compliance with GDPR, HIPAA, DORA and NIS 2, giving your legal and compliance teams auditable evidence of data integrity, with built-in reporting to simplify audit preparation.

6 Predictable, scalable disaster recovery licensing

Acronis DR is available as a subscription add-on to any active Acronis Cyber Protect base license, across one-, three- and five-year terms. Capacity is defined by compute point packages (for example, 2,000 points covers approximately two weeks of failover per server) with storage options from 250GB to 5TB. Free hot storage is included with every DR subscription, enabling you to run test and production failovers for critical workloads at no extra cost.

"Acronis' mission is to protect, manage and automate all small and medium IT deployments."

750,000+
business customers

1,800+
employees in 60+ countries

26
languages in products

21,000+
service providers in 150 countries

50+
data centers in 35 countries

15
scenarios in one platform

What cyber resilience looks like with Acronis

Anticipate	Withstand	Recover	Adapt
Before the attack, Acronis has already assessed vulnerabilities, applied patches and mapped every protected workload. Immutable backups are running on schedule, quietly, automatically.	At 2 a.m., Acronis' AI engine detects anomalous encryption behavior and halts the attack. Affected endpoints are isolated. The backup archives remain untouched in governance mode and the attacker cannot reach them.	By 2:15 a.m., critical servers have failed over to the Acronis Cloud. Staff arriving in the morning find systems running normally. Restore points have already been scanned and confirmed as malware free before going live.	Post-incident, forensic data collected during the attack is used to close the vulnerability. Protection policies are updated. The business is better prepared for the next attempt than it was before this one.

Ready to see Acronis in action?

Talk to an Acronis expert or start a complimentary 30-day trial of Acronis Cyber Protect today.

LEARN MORE

Acronis

Learn more at
acronis.com