

Complimentary resources

Acronis Solutions for Healthcare: HIPAA-compliant Cloud Backup and Disaster Recovery

acronis.com/industries/backup/healthcare/

Acronis Solutions for Biopharma acronis.com/biopharma-backup-solution/

Acronis Solutions for Manufacturing

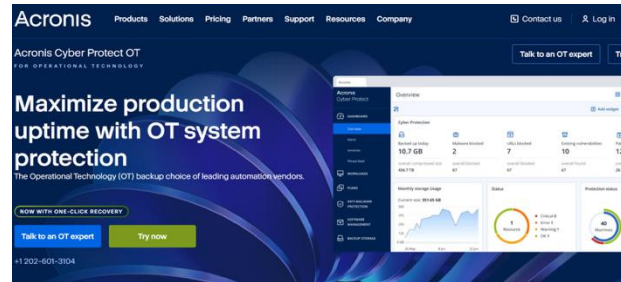
acronis.com/industries/backup/manufacturing/

Product page: Acronis Cyber Protect for OT

acronis.com/products/cyber-protect-ot/

Infographic: Maintaining OT uptime with One-Click Recovery

acronis.com/resource-center/resource-preserving-uptime-in-operational-technology-ot-environments/



Further reading

Solution brief: Preserving uptime in OT environments
acronis.com/resource-center/resource/preserving-uptime-in-operational-technology-ot-environments/

Acronis infographic: 5 steps to building cyber resilience in health care
acronis.com/resource-center/resource/5-steps-to-building-cyber-resilience-in-health-care/

Acronis solution brief: How Acronis Cyber Protect enables health care organizations to maintain HIPAA compliance
acronis.com/resource-center/resource/acronis-cyber-protect-enables-health-care-organizations-to-maintain-hipaa-requirements/

Acronis case study: BDR Pharmaceuticals reduces capex-by-30-and-opex-by-12-with-acronis-cyber-protect/
acronis.com/resource-center/resource/bdr-pharmaceuticals-reduces-capex-by-30-and-opex-by-12-with-acronis-cyber-protect/

Preserving uptime in operational technology (OT) environments

The high costs of OT system downtime

Operational technology (OT) systems are a critical link in maintaining production uptime and company profitability. When they fail, they can bring down assembly lines, pipelines, safety grids and supply chains with them. The costs of the resulting outages can run from tens to hundreds of thousands of dollars per hour. A survey by ASIS found that 61% of companies had recently experienced downtime caused per month, and outages cost businesses \$60,000 per hour. Other consequences of OT downtime include:

- Sales opportunity costs due to unfilled orders and longer lead times.
- Increased direct labor costs per quantity of goods produced.
- Customer relationship and brand reputation damage caused by slow or other deliveries.
- Shrinking market capitalization as investors lose confidence in the business's ability to maintain consistent production.
- Financial penalties for unmet service level agreements and other contractual obligations.
- Compliance fines and criminal penalties for failure to meet regulatory requirements for cyber resilience.

As a result, the stakes are high in defending OT systems against cyberattacks, natural disasters, hardware failures, software glitches and human errors — and getting them back online quickly when they fail.

5 steps to building cyber resilience in health care

The health care sector is a lucrative target of widespread cyberattacks, and the costs to recuperate are in the billions of dollars every year. Why are health care ecosystems are the impact and damage of attacks to resources to do more damage.

BDR Pharmaceuticals International reduces CapEx by 30% and OpEx by 12% by switching to Acronis Cyber Protect

Indian pharmaceutical company dramatically improves RPO and RTO metrics while reducing bandwidth requirements by 10% with Acronis

BACKGROUND

BDR Pharmaceuticals International (BDR Pharmaceuticals) is part of the BDR Group of companies, an internationally known player in manufacturing pharmaceutical APIs and new drug formulations (including critical care, genomics, and neurology) based in Mumbai, India. The company invests heavily in research and development to create new molecules — and ultimately, medicines. Given the critical sensitivity of the data being generated BDR Pharmaceuticals needs a highly secure and resilient infrastructure that is compliant with all regulatory agencies governing their activities such as the FDA. For backup and recovery, they had a NAS device Synology in place. The CIO Vaid Bhaner wanted to build out a new cloud-focused infrastructure that would support up to 25 critical systems and 7 TB of data.

THE CHALLENGES

With the existing NAS solution in place, Bhaner noted they were experiencing a "slow backup process that consumed a lot of bandwidth and a complex restoration process that required lots of time and effort." Ultimately, he lacked the necessary visibility into the infrastructure. "This meant that Bhaner's team was able to meet their RPO metrics only 50% of the time.

When considering a new cloud-focused infrastructure, Bhaner had several critical concerns: "Security is the most important factor — data must always be protected from leaks, malware, and ransom." He explained, "We must adhere to strict regulations such as data residency requirements from the FDA. We must improve our RPO and RTO metrics, and we will be more observant along with proper visibility into all of the infrastructure."

KEY CHALLENGES

- RPO metrics only achieved 50% of the time
- Complex backup and restoration processes
- High costs for storage and bandwidth
- Poor visibility into infrastructure

KEY REQUIREMENTS

- Reducing time from leaks, malware, and ransom
- Compliance with regulatory agencies
- Improving bandwidth efficiency

PROTECTED RESOURCES

- 25 critical systems
- 7 TB of data

KEY BENEFITS

- Reduced CapEx and OpEx
- Full audit trail required for backup and recovery
- Enabled near-perfect RPO metrics and improved RTO metrics

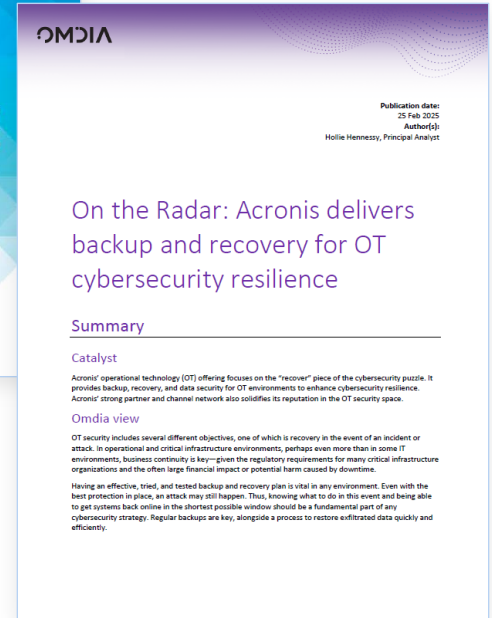
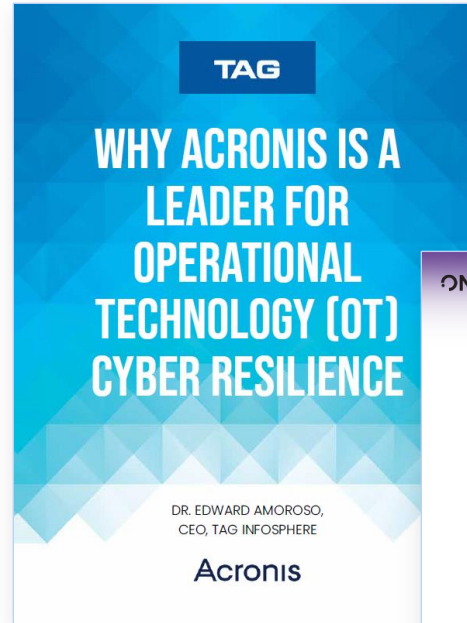
Analyst reports

TAG Infosphere report: Why Acronis Is a Leader for Operational Technology (OT) resilience

acronis.com/resource-center/resource/why-acronis-is-a-leader-for-operational-technology-ot-cyber-resilience/

Omdia report: One the Radar: Acronis delivers backup and recovery for OT cybersecurity resilience

acronis.com/resource-center/resource/acronis-delivers-backup-and-recovery-for-ot-cybersecurity-resilience/



Acronis

Schedule a private consultation with an Acronis SE

acronis.com/lp/healthcare-cyber-protect-request-demo/



Acronis

Defend your health care organization with Acronis Cyber Protect



Uptime and unimpeded access to health care data is critical to maintaining operations. While natural disasters and cyberattacks are the most common causes of data loss and downtime, aging infrastructure and hardware failures are equally common. And as the list of regulatory requirements grows, so too do the ramifications of failing to keep pace.

Acronis Cyber Protect

Protect your health care organization from devastating downtime and data loss and avoid costly compliance violations. With a single agent on every endpoint, HIPAA-compliant disaster recovery and continuous protection for even legacy infrastructure, Acronis Cyber Protect defends your health care organization from the most prevalent threats that keep you up at night.

Get a personalized demo

Schedule a 1:1 demo with an Acronis solution engineer to explore Acronis Cyber Protect in depth. They will present a live demo of the solution and answer any questions you might have.

Schedule a 1-on-1 call with an Acronis expert

Serbia
+381

Phone

Example: 060 1234567

Number of Employees
Select

Country/Region
Serbia

By continuing you agree to Acronis [Privacy Statement](#).

Submit

Protected by reCAPTCHA, [Google Privacy Policy](#) and [Terms of Service](#) apply.

Acronis Cyber Protect


Start your free 30-day trial
with Acronis expert support

Acronis

FOR BUSINESS





Acronis Cyber Protect

Includes all features of Acronis Cyber Backup



Discover cyber resilience that seamlessly integrates the most secure backup with cybersecurity to provide complete, streamlined protection.

- The most secure backup
- Rapid recovery
- Dramatically reduced TCO
- Comprehensive security capability
- Integrated remote endpoint monitoring and management

**Start your free 30-day trial with
Acronis expert support**
or log in if you have Acronis account

First Name Last Name

Enter first name

Email Password

Bulgaria Phone

Example: 043 032 345

Purpose of using the product

Country/Region

I agree to the Acronis [Terms of Service and Privacy Statement](#)

This site is protected by reCAPTCHA and the Google [Privacy Policy](#) and [Terms of Service](#) apply.

