

# Protect your data from cyber attacks with Cyber Resilience

AI-driven cyber threats, increased exposure of IT infrastructures and new regulations are pushing companies toward advanced solutions for data protection and operational resilience.

In large organizations operating in highly regulated, data-intensive sectors, it's crucial to implement strategies that protect critical data, secure applications, and ensure cyber recovery. **But what's the most effective, sustainable, and compliant way to build Cyber Resilience? And how can organizations stay ahead of threats while minimizing the economic and operational impact of cyber incidents?**

## Key Trends

+11%

Annual growth rate of cybercrime costs (2024–2029)

59%

of global businesses were targeted by ransomware in 2024

56%

of companies report business disruption following a data breach

Source: Statista

A solid Cyber Resilience strategy protects critical data and ensures compliance with Italian, European (GDPR, NIS2, ACN), and industry-specific regulations (such as DORA and EMA).



**We offer tailored solutions for every type of infrastructure, requirement and market context.**

## Key Benefits

- Operational resilience** and rapid recovery post-ransomware
- Increased reliability** and reputation with customers
- Compliance with data** security and regulatory requirements

## Protect your most strategic data

- 01 PERSONAL AND LEGAL DATA**

  - Information about clients, users, and employees
  - Data subject to retention obligations
  - Data related to national or corporate security
- 02 HEALTH AND PHARMACOLOGICAL DATA**

  - Personal and sensitive clinical data
  - Research data for drug testing and development
- 03 OPERATIONAL AND INDUSTRIAL DATA**

  - Production, monitoring and logistics data
  - Distribution and billing data
  - Network detection and tracking data
- 04 FINANCIAL DATA**

  - Data on transactions and financial services
  - Critical banking and insurance information

We support clients in achieving Cyber Resilience with an end-to-end offering that includes managed services integrated with our SOC and cloud, on-premises, and hybrid deployment models.

### Analysis and Planning

In-depth analysis of risks and business impact, compliance audits and identification of critical infrastructure and data, and design of failover solutions to ensure continuity and security.

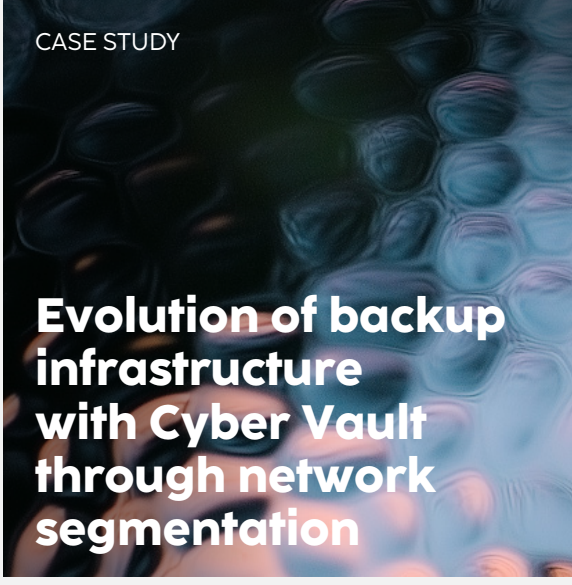
### Isolated Protection and Recovery

The Cyber Resilience plan integrates threat detection tools, Cyber Vault, and Isolated Recovery Environment to ensure secure failover and verified infrastructure recovery.

### Proactive Monitoring, Compliance, and Recovery Testing

We ensure resilience through continuous and proactive threat detection, testing and regular compliance checks, keeping customer systems secure, up-to-date and ready to respond to evolving threats.

## Our Toolbox



## Our Approach

A comprehensive approach to **Cyber Resilience** that combines the expertise of our Security, Cloud and Infrastructure teams with best-of-breed partner solutions. We offer customized systems to reduce risks and ensure cyber resilience.

- 800+**

CLOUD AND IT INFRASTRUCTURE PROFESSIONALS
- 300+**

CYBERSECURITY PROFESSIONALS
- 3**

CERTIFIED DATA CENTERS