Acronis Cyber Resilience

Natively integrated cyber resilience for servers and VMs

Building cyber resilience with Acronis

Cyber resilience goes beyond traditional cybersecurity. It is not only about preventing attacks but also about ensuring that businesses can continue to operate even when incidents occur. As NIST defines it: “Cyber resilience is the ability to anticipate, withstand, recover from and adapt to adverse conditions, stresses, attacks or compromises on systems.”

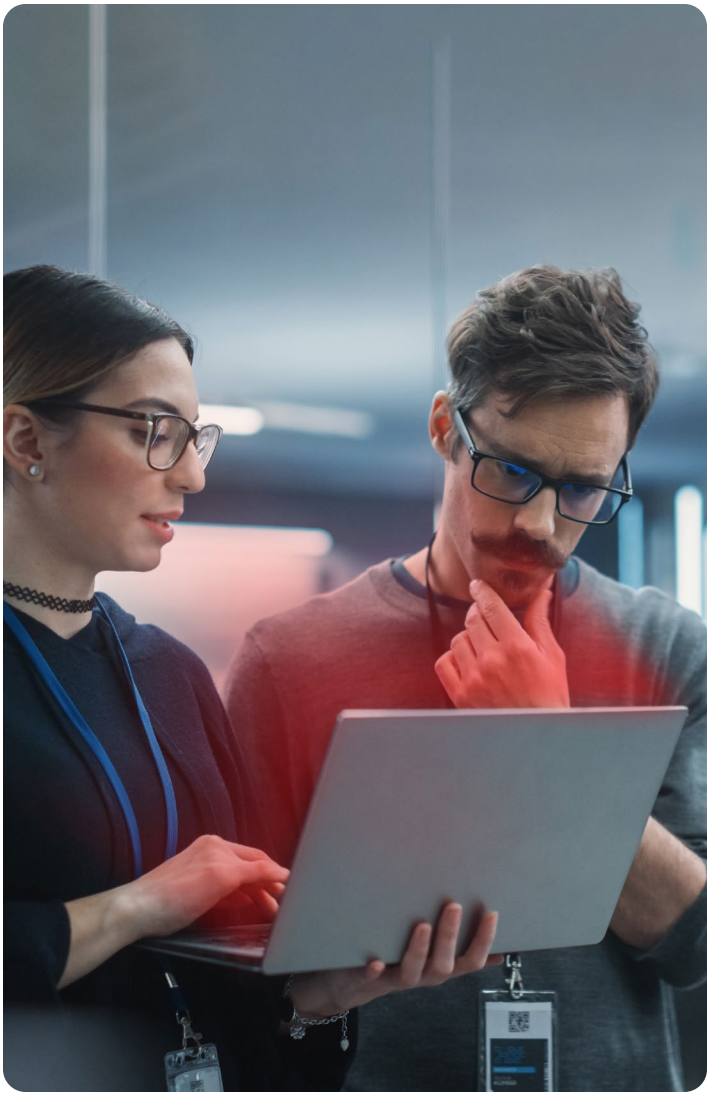
For both service providers and enterprises, the real question is: How fast can your business bounce back? Without clear incident response playbooks, tools and defined recovery time and recovery point objectives (RTOs and RPOs), every disruption risks causing lost revenue, diminished customer trust and lasting reputational damage.

Resilience pain points

Businesses of every size are finding that downtime costs far more than just lost data. Service providers face the added risk of churn as clients quickly move on if recurring outages erode confidence.

Enterprises, on the other hand, contend with growing compliance pressures and regulatory oversight. Any gaps in preparedness expose them to fines, penalties and reputational risk.

Managing incidents with fragmented tools also creates unnecessary complexity. Without a unified strategy, IT teams experience operational chaos, struggling to stitch together detection, response and recovery across multiple consoles and agents. These inefficiencies increase costs, slow response times and expand liability. Rising cyber insurance premiums add another layer of concern, and poor resilience can even mean coverage is denied altogether.



Technology barriers to resilience

As businesses accelerate digital transformation, achieving resilience has become more challenging. Hybrid IT environments stretch across on-premises systems, cloud platforms and remote endpoints, creating a constantly expanding attack surface. This results in more interdependencies and single points of failure. At the same time, threats have grown more sophisticated. Ransomware, supply chain compromises and insider risks are exploiting the cracks left by siloed solutions. Point tools may reduce specific risks, but they also create blind spots, manual processes, and gaps that attackers are quick to exploit.

The path to cyber resilience

Achieving true cyber resilience requires more than strong defenses. It is about ensuring continuity, no matter the disruption. Businesses can achieve resilience when adopting a structured approach that begins with anticipating risks through asset mapping, vulnerability assessment and patch management. They must then be able to withstand threats by detecting and containing them in real time with advanced capabilities such as endpoint detection and response (EDR), extended detection and response (XDR) and data loss prevention. These proactive measures are only effective when paired with a strong recovery strategy.

Recovery is the next critical step. Restoring data and systems quickly, reliably and free of malware keeps downtime to a minimum. In a severe outage, this is first and foremost about maintaining business continuity. With Acronis Cloud Disaster Recovery, businesses can immediately failover workloads directly to the Acronis Cloud or to Microsoft Azure. This immediate failover ensures continuity even during the most severe outages and serves as a secure fallback environment until the full restoration of primary systems can be completed.

Finally, resilience is not static. Organizations must adapt by learning from incidents, training their teams and refining defenses over time.

The spectrum of disaster recovery

Ultimately, these strategies are not just about recovering after a disaster — they are about the operational resilience to continue essential business functions under any adversity. The ability to recover services in minutes rather than days is the key to minimizing financial losses and maintaining customer trust.

Disaster recovery strategies are typically categorized by the RPOs and RTOs they can achieve. Two of the most adopted strategies are:

Warm DR

This approach provides a balance of cost and recovery speed. It uses prestaged systems that can be brought online quickly, aligning with the "recover" goal of minimizing downtime while still having a defined RPO and RTO.

Cold DR

Focused purely on reconstitution and data restoration, cold DR relies on full recovery from backups, resulting in longer recovery times but lower ongoing costs.

By unifying detection, protection and recovery, businesses gain the critical advantage of being able not only to survive a crisis but also to emerge stronger. With Acronis Cloud Disaster Recovery, organizations can select the right level of resilience for every workload — from warm-to-cold failover options that reconstitute services after an outage, to near-instant continuity with integrated hot DR. This flexibility strengthens defenses at every stage of the cyber resilience journey.

The Acronis Cyber Resilience solution

In addition to disaster recovery, Acronis provides a natively integrated platform that unifies backup, disaster recovery, endpoint security, risk assessment and data loss prevention. This approach eliminates silos, reduces tool sprawl and ensures resilience without added complexity. Built for both enterprises and service providers, the platform covers every stage of the resilience journey: anticipate, withstand, recover and adapt. With a single platform, a single agent and a single console, businesses can detect threats faster, recover operations without disruption and continuously adapt to evolving risks.

ANTICIPATE	WITHSTAND	RECOVER	ADAPT
• Device discovery • Data protection map • Asset inventory • Vulnerability assessment • Patch management	• Real-time threat detection • Endpoint detection and response (EDR) • Extended detection and response (XDR) • Data Loss Prevention (DLP) • Rapid containment of active threats	• Secure and automated data recovery • Cloud disaster recovery (CDR) • Immutable backups • Hypervisor mobility • Recover to malware free points	• Remote monitoring and management (RMM) • Security Awareness Training (SAT) • Managed detection and response (MDR) • Advisory incident response templates

Why businesses choose Acronis

For service providers, Acronis offers a path to accelerated recurring revenue. By adding high-margin cyber resilience services to their portfolio, MSPs not only expand their offerings but also stand out in a commoditized market. The unified platform simplifies operations by reducing tool sprawl, while a straightforward licensing model maximizes margins and scales seamlessly with customer growth.

For enterprises and SMBs, Acronis ensures continuity by enabling rapid, malware-free recovery that minimizes downtime and financial losses. Built-in reporting and compliance support make regulatory audits easier to navigate. Strong resilience capabilities also improve eligibility for cyber insurance, often reducing premiums. Just as importantly, demonstrating a robust resilience strategy builds trust with customers, partners and regulators alike.

Book a meeting with an Acronis expert

Your business continuity depends on more than protection. It requires resilience. See how Acronis can help you anticipate threats, withstand attacks, recover faster and adapt for the future.

CONTACT US

Acronis

Learn more at
www.acronis.com