Acronis

WHITE PAPER

Beyond cybersecurity: A practical blueprint for cyber resilience to evolve from prevention to continuity

Executive summary

Cybersecurity and cyber resilience are two sides of the same coin because both are essential to sustaining business operations against modern threats. While traditional cybersecurity focuses on prevention by keeping attackers out, cyber resilience represents a strategic shift toward adaptability and business continuity. It is defined not merely as a function of security operations but as the strategic capacity of an organization to anticipate, withstand, recover from and adapt to cyber disruptions.

Aspect	Cybersecurity	Cyber resilience
Scope	Keeping attackers out	Operating during and recovering from attacks
Primary focus	Preventing attacks / protecting data, infrastructure	Adaptability and business continuity
Core assumption	Stopping attacks is possible	Attacks are inevitable
Outcome	Avoiding breaches	Minimize disruption, ensure business continuity
Key activities	Firewalls, antivirus, intrusion detection / prevention	Incident response, business continuity, disaster recovery (DR)
Mindset	Fortress / perimeter	Agile / adaptive

This white paper presents a resilience blueprint that moves beyond legacy redundancy models to a unified, risk-driven approach powered by Acronis. This shift is driven by an increasingly hostile threat landscape where the average ransomware claim cost has surged to over $1.18 million in 2025.[1] Because reliance on prevention-only tactics is no longer financially sustainable, organizations are adopting the Acronis Cyber Protect platform to transition from fragmented tools to a consolidated framework. This ensures that they can protect the integrity of their critical assets and return to normal operations quickly after any disruption.

[1] Resilience Risk Operations Center. "Mid Year Cyber Risk Report." 2025. https://unlock.cyberresilience.com/hubfs/2025%20Cyber%20Risk%20Report.pdf

Copyright © 2003-2026 Acronis International GmbH.

The strategic imperative: Beyond redundancy

Historically, organizations relied on architectural redundancy to minimize downtime through methods such as dual power supplies, high-availability hardware pairs and redundant data centers. While these measures protect against physical hardware failure, they were engineered for accidental outages rather than intelligent adversaries.

In the context of modern ransomware, duplication-style resilience often fails. A redundant data center can replicate an infection from the primary site as an attack propagates across the network fabric. Furthermore, these fragmented approaches often lead to tool sprawl, where IT teams must manage disconnected consoles for backup, DR and security. This creates a 'Franken-stack' that kills productivity, increases the total cost of ownership and creates dangerous vulnerability blind spots.

The Acronis difference

True resilience requires a platform capability rather than a simple collection of tools. Acronis differentiates itself by delivering natively integrated cyber resilience that includes backup, security and DR within a single agent and a single management console. This eliminates the operational drag of switching between interfaces and ensures that recovery is not only rapid but also verified and trusted.

Step 1 Asset classification and prioritization

The foundation of any resilience strategy is the recognition that protection must be commensurate with asset value. Not all data requires the same level of resilience; therefore, the first step is asset classification.

Classify server criticality by business value and not server count

A common misconception in resilience planning is equating technical volume with business value. Organizations must understand that the requirement for cyber resilience is dictated by the criticality of the server, not the number of servers or their raw performance specifications.

As detailed in risk assessment methodologies, a single critical server hosting proprietary information or top-secret intellectual property is inherently more valuable than 100 servers hosting non-sensitive data.

Copyright © 2003-2026 Acronis International GmbH.

The loss of the single critical asset can lead to severe financial liability, regulatory penalties or severe reputational damage.

Consequently, resilience resources including near-zero recovery time objectives (RTOs) and high availability failover should not be assumed or applied uniformly across the entire estate. Instead, they must be concentrated on the specific workloads that underpin the organization's revenue and reputation.

Apply actionable asset labelling to automate protection policies

To make this concept operational, organizations must move from theoretical paper-based classification to digital tagging within their management consoles. Practical asset labelling involves assigning metadata tags to workloads that dictate their automated protection policies.

Common classification labels include:

Confidential or proprietary
The highest level. Compromise leads to severe business loss. These assets require Acronis Disaster Recovery with immediate failover capabilities.

Sensitive
Breach causes tangible damage to mission or reputation. These require frequent immutable backups and aggressive recovery point objectives (RPOs).

Private
Internal data such as personnel records. Standard backup schedules apply.

Public
Data permissible for disclosure. Lowest priority for recovery resources.

By tagging assets within the Acronis console, IT teams can automate the application of protection plans, ensuring that a confidential server automatically inherits an immutable backup policy and a standby cloud virtual machine, while a public server receives a standard daily backup.

Copyright © 2003-2026 Acronis International GmbH.

Step 2 Business impact analysis (BIA) and financial quantification

Once assets are classified, the BIA identifies critical operations and quantifies the consequencesof their disruption.

Core recovery metrics

The BIA establishes the essential metrics that the Acronis platform is configured to meet:

- **RTO**: The maximum tolerable elapsed time for restoration.
- **RPO**: The maximum tolerable data loss.
- **Maximum tolerable downtime (MTD)**: The absolute longest period a system can remain unavailable before causing irreversible damage. Exceeding MTD crosses the threshold from disruption to business failure.
- **Mean time to clean recovery (MTCR)**: The definitive modern metric for ransomware. It measures the time required to recover to a verified, malware-free state.

Acronis addresses MTCR by integrating security scanning into the recovery process, preventing the restoration of infected files.

Quantitative risk analysis

To justify the investment in resilience architecture, organizations should utilize quantitative risk analysis to calculate annual loss expectancy (ALE). This is calculated by multiplying the asset value, the exposure factor, and the annualized rate of occurrence. Acronis supports this economic model through flexible licensing, which allows organizations to align their spending directly with the asset values derived from their risk calculations.

ALE calculation:

Asset value (AV) ×

Exposure factor (EF) ×

Annualized rate of occurrence (ARO)

Step 3 Strategic risk response

Based on risk analysis, organizations must adopt a strategic response tailored to the criticality of their assets. For mission-critical systems where risk avoidance is not viable, the necessary strategy is risk mitigation. Acronis serves as the primary engine for this mitigation through two critical layers that aim to stop an attack before it can devastate the business.

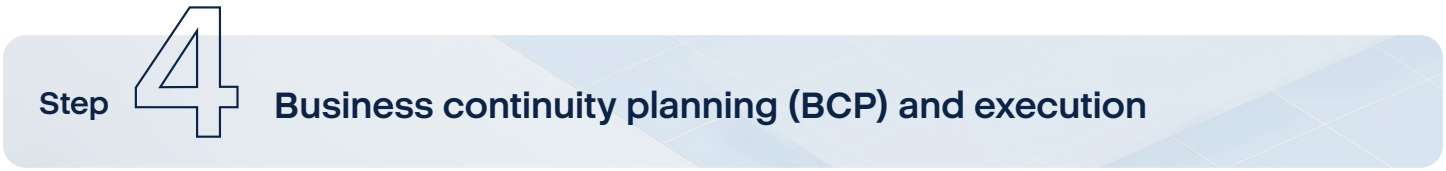
Copyright © 2003-2026 Acronis International GmbH.

Risk mitigation: Neutralizing the threat

Mitigation focuses on reducing the likelihood and impact of a breach. Acronis executes this through immutable storage and AI-assisted defense. Backups are stored in governance mode to ensure that even if an attacker gains administrative access, they cannot delete backup data. Simultaneously, AI-powered behavioral detection engines identify zero-day threats in real time by analyzing active processes and stopping attacks before damage is done.

Risk recovery: Ensuring continuity

When mitigation is bypassed, the strategy shifts to Risk Recovery to ensure the business stays standing. For mission-critical workloads, the Acronis Cloud provides a DR failover environment. This allows the organization to shift production to the cloud instantly, transitioning from crisis to continuity while the primary site is remediated.



The execution of the resilience strategy occurs through a continuous cycle of anticipating, withstanding, recovering and adapting. To replace legacy processes with modern efficiency, Acronis provides streamlined DR and layered cyber protection built for the corporate cloud environment.

The recover phase: Integrated DR

When a disruption occurs, the Recover phase becomes the primary focus. Acronis Disaster Recovery integrates with the base backup license to provide enterprise-grade recovery at a fraction of the cost of legacy, hardware-heavy sites.

- **Cloud-managed infrastructure:** The underlying cloud environment and orchestration platform are fully managed by Acronis. This reduces customer complexity by eliminating the need for off-site hardware maintenance.
- **Customer-controlled execution:** While the infrastructure is managed by Acronis, customers maintain total control over initiating, testing and managing failover and failback operations via the central console.
- **Failover strategy and risk-free testing:** The platform supports failover directly to the Acronis Cloud. To ensure this works when needed, subscriptions include free hot storage to allow organizations to run test failovers for critical workloads at no additional cost.
- **Clean recovery validation:** To prevent the restoration of malicious code, AI-assisted backup validation scans for threats and verifies that restore points are clean before they reach production.

Copyright © 2003-2026 Acronis International GmbH.

The withstand phase: Layered cyber protection

Ensuring a business can withstand an attack requires more than just recovery; it requires active protection of the data itself. This is achieved through immutable full-image and file-level backups stored in governance mode, combined with AI-based ransomware defense that detects and blocks behavioral encryption in real time.

The resilience scorecard and DREAD model

To maintain a high resilience posture, organizations should utilize a scorecard that benchmarks maturity. A key component of this is prioritizing threats using the DREAD model (Damage, Reproducibility, Exploitability, Affected Users, Discoverability).

Acronis strengthens each dimension of the DREAD score:

Damage potential
Rapid cloud failover preserves revenue and limits financial impact.

Reproducibility
Immutable backups stop reinfection loops and prevent attackers from repeating their success.

Exploitability
Automated vulnerability assessments close the gaps that attackers seek to exploit.

Affected users
Granular workload isolation and labelling minimize the blast radius, ensuring compromise does not cascade across the entire user base.

Discoverability
EDR analytics reduce attacker dwell time, making it harder for threats to remain hidden.

Copyright © 2003-2026 Acronis International GmbH.

Why Acronis?

In a landscape where prevention alone is no longer enough, Acronis bridges the gap between traditional security and total business continuity. By unifying AI-powered threat defense with rapid, cloud-orchestrated disaster recovery, Acronis ensures your critical data is not only protected from an attack, but also designed for rapid, reliable recovery.

Integrated DR and recovery assurance: Acronis Disaster Recovery is an add-on component that requires an active base backup license to operate. The solution provides enterprise-grade DR at a fraction of the cost of legacy hardware-heavy sites.

Cloud-managed DR infrastructure: The underlying cloud environment, orchestration platform and necessary infrastructure are fully managed by Acronis, reducing customer complexity.

Instant failover to Acronis Cloud with usage-based compute billing: Critical server workloads can be recovered into Acronis Cloud during an outage or attack, with compute billed only when failover is activated, eliminating ongoing standby cost.

Customer-controlled execution: While the infrastructure is managed by Acronis, customers maintain control over initiating, testing and managing failover and failback operations via the console.

Clean recovery validation: AI-assisted backup validation scans for threats and verifies that restore points are clean.

Risk-free testing: DR subscriptions include free hot storage to allow organizations to run test and production failovers for critical workloads at no additional cost.

Layered cyber protection: Immutable full-image and file-level backups stored in governance mode. AI-based ransomware defense detects behavioral encryption.

Conclusion: The unified path forward to ensure business continuity

The contemporary threat landscape, characterized by AI-driven attacks and high-velocity financial damage, demands a fundamental change in how we protect business operations. Organizations can no longer rely on the assumption that perimeter defenses will hold or on disjointed redundancy tools that fail to stop ransomware propagation.

The solution is a transition to the Acronis unified cyber resilience platform. By consolidating backup, DR, cybersecurity and endpoint management into a single solution, businesses eliminate the complexity of tool sprawl and gain the power of AI-driven protection.

Ultimately, resilience is an economic decision. By aligning protection to business value through rigorous asset classification and BIA, and by executing this strategy through Acronis's cloud-orchestrated and AI-validated recovery runbooks, organizations ensure they can survive the inevitable. With Acronis, businesses do not just recover; they bounce back higher, securing their future in an unpredictable digital world.

Acronis

Learn more at
acronis.com

Copyright © 2003-2026 Acronis International GmbH. All rights reserved. Acronis and the Acronis logo are trademarks of Acronis International GmbH in the United States and/or other countries. All other trademarks or registered trademarks are the property of their respective owners. Technical changes and Differences from the illustrations are reserved; errors are excepted. 2026-01