



Acronis

DATA SHEET

Acronis Cyber Protect

for Scale Computing Platform



The most secure backup and fastest recovery for Scale Computing environments

Acronis Cyber Protect delivers the most secure backup and fastest recovery for Scale Computing HyperCore environments. It provides robust cyber resilience against a broad range of threats, protecting the most challenging environments — including industrial computing environments where Scale Computing virtual machines (VMs) are used to control and configure operational technology (OT) and industrial control systems (ICS) — as well edge computing environments outside of centralized data centers.

Designed for ease of use and maximum efficiency, Acronis Cyber Protect for Scale Computing environments enables swift, user-driven recovery of any computer, regardless of age or function, reducing local dependence on remote IT support and minimizing costly downtime associated with a broad range of cyberthreats.

Acronis Cyber Protect eliminates the complexity of traditional, piecemeal approaches to data protection, protecting over 20 SaaS, on-premises and cloud workloads, including Scale Computing environments.

Scale Computing customers can also store backups in Acronis Cloud data centers, which employ AI-driven proactive defenses to stop ransomware and other malware attacks, and actively scan for and remediate malware and known vulnerabilities from backups to ensure clean recoveries.

Protect Scale Computing environments with agentless backup.

- Deploy full virtual machine backup and fast recovery of all workloads on SC//HyperCore clusters without “in guest” backup agents.
- Back up and restore data directly from SC//HyperCore clusters to Acronis backup storage locations, including cloud storage.
- Protect local and remote workloads through a single pane of glass.

Maximize availability, minimize downtime.

- Achieve RPOs and RTOs of less than 15 minutes, enable best-in-class production practices, test failover speeds, and implement flexible backup frequency policies.
- Cut recovery time in half with complete system images that are instantly ready to reinstall, automatically detect boot requirements, and restore any full system to a physical computer or virtual machine with an empty “bare metal” disk drive.

Get AI-enabled protection of backups stored in Acronis Cloud data centers.

- Secure all backups stored in Acronis Cloud data centers against ransomware and other malware.
- Take advantage of proactive malware and vulnerability scanning and remediation to ensure clean recovery operations.

Most secure backup, fastest recovery

Strengthen enterprise cyber resilience with the most secure backup and fastest recovery of SC//HyperCore environments, including immutable storage.

AI-based cyberthreat protection of Scale Computing backups stored in Acronis data centers

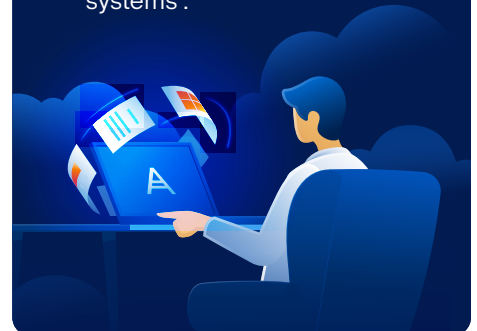
Proactively protect Scale Computing backups stored in Acronis data centers from advanced cyberthreats, including ransomware and other malware attacks.

Disaster recovery in a box




Convert backups of other machines running anywhere else into SC//Hypercore virtual machines to enable fast, local disaster recovery by leveraging Scale Computing Hypercore compute and storage resources. The SC//Hypercore cluster effectively serves as a fully functional Disaster Recovery site in a box.

Best ROI and TCO

- Save 10x on storage space with deduplication.
- Retain 20% of work hours with simplified, automated administration.
- Avoid upfront costs and easily switch from legacy systems .



Three layers of protection

 <p>Proactive</p> <p>Vulnerability assessments, patch management and removal of malware from backups.</p>	 <p>Active</p> <p>Continuous, AI-based cyberthreat protection of Scale Computing backups stored in Acronis Cloud data centers.</p>	 <p>Reactive</p> <p>Rapid recovery of data, integrated disaster recovery and user-initiated, one-click recovery, including bare-metal recovery.</p>
---	--	---

Features

Acronis Cyber Protect for Scale Computing environments

Advanced backup features

- Protection of all supported VM operating systems on SC//HyperCore, including Windows, Linux, UNIX and desktop systems.
- Agentless protection of SC//HyperCore clusters with flexible backup storage options, including Acronis native cloud storage, local SC//Hypercore cluster storage, local SMB shares, local NFS shares and public cloud storage on Azure, Amazon and Wasabi. (Note that cloud deployment of the Acronis console is required to use Azure, Amazon and Wasabi cloud storage.)
- Immutable backup storage to protect against accidental or malicious deletion of Scale Computing backups stored in Acronis Cloud data centers.
- One-click recovery, enabling non-IT staff to restore failed computers quickly, simply and reliably in remote locations, including home offices and highly automated industrial settings.



Advanced anti-malware and security management features for Scale Computing backups stored in Acronis Cloud data centers






- Proactive scanning for and remediation of malware and known vulnerabilities in backups to ensure clean recoveries.



Storage flexibility and low-cost, long-term retention for regulated industries

- Flexibility to store backups in hot, warm, and cold storage to meet a range of cost and retrieval speed needs: SC//HyperCore virtual disk storage, NAS, SAN, tape, disk, Acronis Cloud data centers, private cloud and public cloud (e.g., Azure, AWS, Google).
- Support for compliance with regulations that require long-term data recovery (e.g., to meet data retention requirements extending over periods of years).



Identify 	Protect 	Detect 	Respond 	Recover 
<ul style="list-style-type: none"> • Auto-discovery of new devices. • Vulnerability assessments. • Data protection map. 	<ul style="list-style-type: none"> • Remote agent installation. • Backup and data protection. • Unified protection policies management. 	<ul style="list-style-type: none"> • Detect zero-day and advanced threats. • Defend against malware and exploits. • Hard drive health control. 	<ul style="list-style-type: none"> • Investigation via forensic backups and remote connections. 	<ul style="list-style-type: none"> • Pre-integrated backup and disaster recovery. • One-click mass recovery.

Complete multisite and industrial IT protection

Empower recovery

Remove IT bottlenecks, cut downtime and save resources by enabling user-led recovery processes.

Cyberthreat protection

Use AI and backup storage immutability to guard data, applications, systems and backups against advanced cyberthreats, including ransomware and zero-day attacks.

Reduce TCO

Support over 20 workload types across platforms and OS versions for backup vendor consolidation and unified protection.

Rapid industrial recovery

Rapidly restore computers used to control OT and ICS in highly automated industrial settings.

Simplify management

Unify views of backup and recovery operations with centralized control and integration with third-party tools.

Universal computer recovery

Ensure quick, reliable recovery of any computer (including legacy systems) with optional bare-metal restoration.

Data sovereignty

Store backups using in-house storage and / or any of 50+ cloud locations, including Acronis Cloud data centers, Google Cloud and Microsoft Azure.

Remote worker protection

Enable self-service recovery for remote workers, enabling fast post-outage recovery without direct IT intervention.