Acronis Cyber Compliance



Continuous compliance built for MSPs

Cyber Compliance helps MSPs deploy, measure, and continuously monitor security controls across customer environments. Rather than treating compliance as a point-in-time assessment, it enables a continuous compliance approach where evidence remains current and security controls are continuously assessed. Built into the Acronis Cyber Platform, Cyber Compliance translates platform telemetry into control evidence. This helps MSPs understand which safeguards are implemented, identify gaps, prioritize remediation and track security improvements over time.

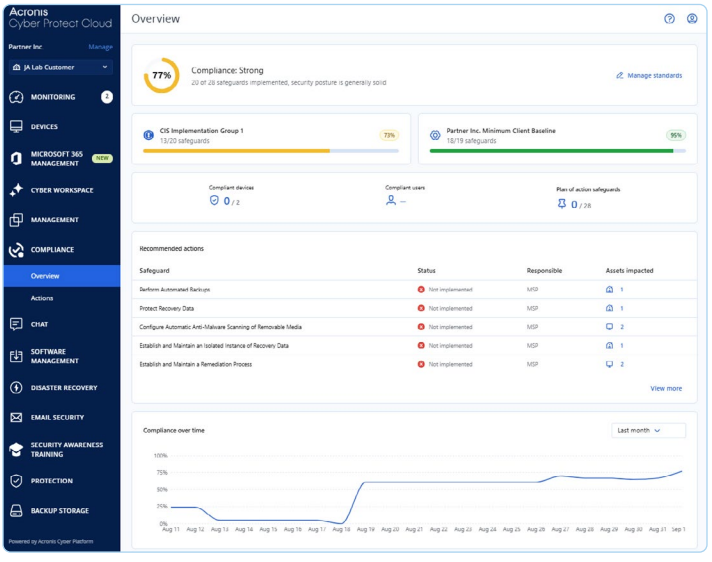
The challenge

MSPs face growing pressure to help clients meet an expanding range of compliance requirements, including security frameworks, industry standards, regulatory mandates and cyber insurance obligations. However, traditional assessments provide only a snapshot in time and do not offer the continuous visibility MSPs need to understand whether controls remain implemented across changing client environments. At the same time, fragmented tools, manual processes and inconsistent configurations make it difficult to standardize compliance services, maintain current evidence and demonstrate adherence. MSPs need a scalable way to continuously measure security controls, track remediation and prove ongoing compliance across their client base.

The solution

Acronis Cyber Compliance gives MSPs a structured way to turn recognized security best practices into measurable security outcomes. It brings together platform telemetry, control status, ownership, remediation activities and compliance trends within a single platform.

MSPs can continuously demonstrate which controls are implemented, where gaps exist and what actions are needed to strengthen each customer's security posture.



Copyright © 2003-2026 Acronis International GmbH.

Features and capabilities

Compliance status



- Calculate compliance implementation status based on CIS Controls v8.1 and mapped to widely adopted regulatory and industry frameworks.
- Reflects actual implementation from Acronis product usage and partner integrations.[1]
- Available at tenant and device level.

Central compliance visibility



- Dedicated compliance section in the Acronis console.
- Dashboards showing overall status, trends and clients requiring attention.
- MSP-level and client-level views.

Compliance reporting



- High-level and detailed compliance reports.
- Compliance trends over time.
- Visibility into safeguard status and responsibility.

Frameworks and standards



- Supports CIS IG1, IG2, and IG3.
- Default baseline of IG1 for new customers.
- Popular frameworks supported e.g. NIST CSF 2.0.[1]

Custom standards



- Use predefined CIS standards or clone and customize.
- Exclude nonapplicable safeguards.
- Assign responsibility per safeguard.

Actionable safeguard insights



- Safeguard status: Implemented, partially implemented, planned or not applicable.
- Clear ownership (MSP vs. client).
- “How to fix” guidance explains which Acronis capabilities and integrations can help.

[1] Indicates capability on the roadmap for phase two.

Start your free trial of Acronis Cyber Platform LEARN MORE

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. 2026-10