

Acronis

Cyber Compliance



The challenge

MSPs are expected to deliver secure, consistent IT environments while protecting margins and scaling operations.

Fragmented tools and inconsistent configurations across clients make it difficult to standardize service delivery and achieve predictable cybersecurity outcomes.

At the same time, clients and cyber insurers demand proof of compliance with recognized security best practices.

The challenge is not tools, but creating a repeatable approach to baseline environments, enforce standards, and continuously improve security maturity and compliance at scale.

The solution: Cyber Compliance

Cyber Compliance gives MSPs a structured way to baseline, standardize, and continuously improve client environments using proven compliance and security best practice frameworks.

Built into Acronis Cyber Protect Cloud, it maps compliance controls to real Acronis capabilities and integrations, helping MSPs see what is in place, identify gaps, and prioritize action.

The result: stronger security outcomes, clear evidence for cyber insurance and regulatory requirements, improved operational efficiency, reduced churn risk, and scalable long term growth.

WHY MSPS CHOOSE CYBER COMPLIANCE

Understand what's actually implemented

Helps you and your clients understand which security safeguards are implemented, where gaps exist and how to improve over time.

Built for long-term success

Support continuous compliance across customers, assets and security tools with increasing levels of automation and ecosystem integration.

Native platform integration

- Built into the Acronis platform.
- No solution sprawl.

Features and capabilities



Compliance scoring

- Calculate compliance implementation scores based on CIS Controls v8.1 and mapped to widely adopted regulatory and industry frameworks.
- 153 safeguards supported.¹
- Reflects actual implementation from Acronis product usage and partner integrations.²
- Available at tenant and device level.



Central compliance visibility

- Dedicated compliance section in the Acronis console.
- Dashboards showing overall scores, trends and customers requiring attention.
- MSP-level and customer-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.
- Multiple standards can be assigned per customer.
- Popular frameworks supported e.g. NIST CSF 2.0.²



Custom standards

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

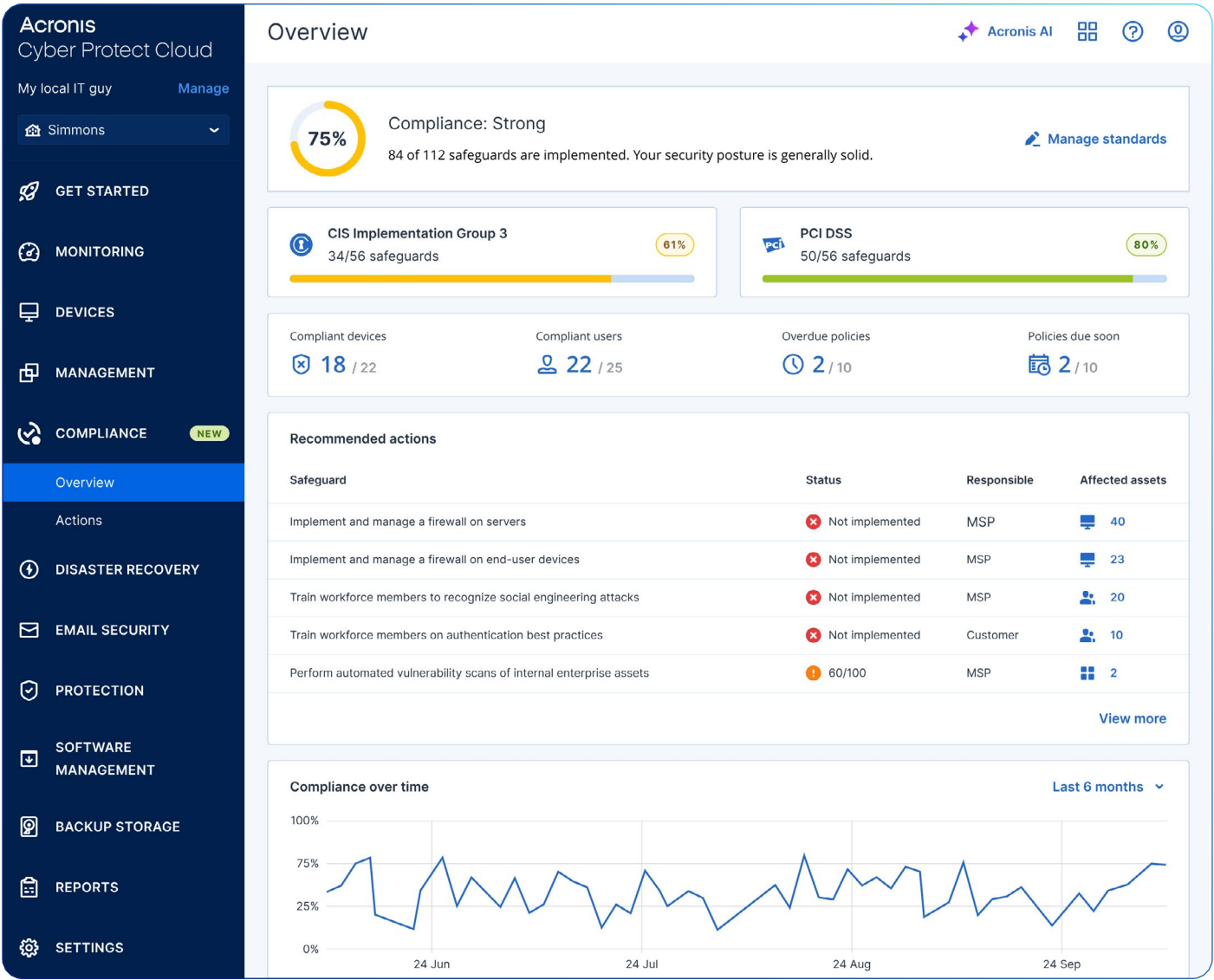


Actionable safeguard insights

- Safeguard status: Implemented, partially implemented, planned or not applicable.
- Clear ownership (MSP vs. client).
- "How to fix" guidance explaining: What the safeguard requires. How scoring works. Which Acronis capabilities and partner integrations² can help.

¹ Only Safeguards implemented by using Acronis products will be supported in phase one.

² Indicates capability on the roadmap for phase two.



Learn more about compliance frameworks

New to Acronis or evaluating compliance alignment? Compliance Navigator provides a high-level overview of selected major frameworks, example control mappings, and educational resources to help you understand what can be implemented.

Acronis Cybersecurity Compliance operationalizes Compliance Navigator by turning those insights into measurable, actionable controls.

EXPLORE ACRONIS COMPLIANCE NAVIGATOR



Forward-looking statement disclaimer

Commercial in confidence — Contains forward-looking information subject to change. Not for distribution. This presentation includes forward-looking information about product features in development. Future capabilities, timelines and functionality are subject to change and are not commitments or guarantees. Please do not rely on these statements for purchasing or planning decisions.