Acronis

Environmental, Social and Governance

Report 2025

As AI reshapes how organizations work, cybersecurity is becoming more complex.

Table of contents

Acronis enables AI with confidence by protecting, managing and automating all small and medium IT deployments with a single, natively integrated cyber protection platform.

Copyright © 2003–2026 Acronis International GmbH.

About this report

Scope and period

This ESG Report covers Acronis' material sustainability topics for the year ended December 31, 2025.

Report notes

References to "Acronis," "the Company," "we," "us" and "our" mean Acronis AG and its direct and indirect subsidiaries. Figures and tables represent an aggregated view of Acronis, including all entities, unless noted. Any limitations or exclusions are disclosed in the relevant sections.

Basis of preparation

This report has been prepared with reference to the Global Reporting Initiative (GRI) Sustainability Reporting Standards (2021). It is informed by Acronis' 2025 double materiality assessment and impacts, risks and opportunities analysis. Methodologies, topic boundaries and definitions are summarized in the double materiality assessment section.

Data notes

Data and figures may be rounded. Prior-year figures may be restated to reflect improvements in methodology or other factors; any restatements will be clearly indicated.

Forward-looking statements

This report includes forward-looking statements that involve risks and uncertainties. These statements are not a guarantee of future performance. Actual results may differ due to many factors, some of which are beyond our control. We undertake no obligation to update these statements except as required by law.

Availability and cadence

The ESG report is published annually. This document is available digitally, and accessibility accommodations can be provided upon request.

Contact

Some information that may be required for a full assessment of Acronis' sustainability performance may be omitted from this report. If you have questions or feedback, please email:

ESG@acronis.com

Message from the Acronis CEO

In cybersecurity, trust is built through discipline. Customers and partners rely on Acronis to keep businesses running, recover quickly when incidents occur and safeguard their data and workloads. Acronis is the trusted partner to protect, manage and automate small and medium IT deployments. That responsibility goes beyond our products. It is reflected in how we manage risk, govern technology and data, support our people and communities and address the environmental footprint of our activities.

I returned to Acronis as Chief Executive Officer in 2025 at a time when expectations across our industry are growing exponentially. Threats continue to evolve, regulatory scrutiny is increasing and customers are asking not only whether solutions perform, but whether they are governed responsibly. Generative AI has accelerated this shift by expanding both opportunity and risk. Our response is deliberate: We improve what we deliver, and we strengthen the controls, accountability and oversight that enable innovation to endure. Our mission is to protect, manage and automate all small and medium IT deployments.

Following EQT's acquisition of a majority stake in May 2025, Acronis entered a new ownership phase with a clear focus on governance maturity and long-term value creation. Against this backdrop, we completed our first double materiality assessment. This was a practical exercise. It sharpened our priorities and clarified where structure, ownership and consistent measurement are essential. As a result, we are concentrating our efforts on the responsible use of AI, data protection and privacy, corporate culture and value chain management, alongside our commitments to community impact and environmental performance.

Responsible innovation is central to our approach. We are expanding the use of AI to strengthen security outcomes and operational efficiency, while tightening guidance, controls and accountability for AI systems across the business. In a risk-based industry, governance is not a constraint on innovation; it's what makes innovation credible. Exercising discipline in how new technologies are deployed is essential to maintaining trust over time. We have reinforced this foundation through updated policies, targeted training and strengthened oversight across key areas of business conduct and integrity.

On environmental matters, we improved transparency around our greenhouse gas emissions and energy use, increased renewable electricity matching to cover 70% of our purchased electricity, and reduced our workplace footprint in several locations. These actions are expected to lower energy demand over time. Our focus now is on improving data quality and consistency so progress can be measured reliably, compared over time, and used to inform decision making as the business grows.

On the social side, we invested in our workforce, skills and culture, and expanded community engagement through the Acronis Cyber Foundation Program, supported by employee and partner volunteering. We strengthened learning and development through structured training and mentorship, and reinforced feedback through employee-led initiatives such as Foundation Ambassadors and Voice of Employees. In a cybersecurity company, people are part of the security perimeter, and sustaining a strong culture is integral to managing risk responsibly.

Looking ahead, our priorities are clear. We will continue to strengthen the foundations of trust — security, privacy and responsible technology governance — while further improving ESG data governance and engagement across our value chain. As AI capabilities evolve, we will refine oversight to ensure progress remains disciplined, transparent and aligned with stakeholder expectations. Our objective is long-term value built on credibility, not short-term claims.

Jan-Jaap Jager

Chief Executive Officer, Acronis

About Acronis

26
Languages

150
Countries

1,800+
Employees

21,000
Service providers

750,000+
Businesses

Acronis is a global cyber protection company that provides natively integrated cybersecurity, data protection and endpoint management for managed service providers (MSPs), small and medium businesses (SMBs) and enterprise IT departments. Acronis solutions are highly efficient and designed to identify, prevent, detect, respond to, remediate and recover from modern cyberthreats with minimal downtime, ensuring data integrity and business continuity.

Acronis enables AI with confidence by protecting data, systems and agentic actions on a single, natively integrated cyber protection platform.

A Swiss company founded in Singapore in 2003, Acronis has 15 offices worldwide and employees in 67 countries. Acronis Cyber Protect is available in 26 languages in 150 countries and is used by over 21,000 service providers to protect over 750,000 businesses.

As of December 31, 2025, Acronis employed more than 1,800 people worldwide.

Our stakeholders include employees, customers, partners / MSPs, suppliers, local communities and investors. We maintain regular, structured engagement with each group to inform priorities and actions.

Acronis APJ team during sales kickoff event.

2025 highlights

In a year of rapid change in cybersecurity and AI, Acronis continued to strengthen the trust foundations of our business — protecting data, applications and systems, investing in people, supporting communities and reducing our operational footprint. Below are selected highlights from across Environment, Social and Governance.

Environmental

- Reduced total greenhouse gas emissions by 40% year on year primarily driven by lower use-phase emissions from sold products and updated electricity emission factors.
- Matched 70% of electricity consumption with energy attribute certificates.
- Held 18 Environmental Days across 11 regions; collected 1,500 kg (3,300 lbs.) of waste and planted 1,780 trees.
- Extended equipment reuse by donating 90 monitors and 120 PCs for a second life.
- Migrated Frankfurt data center workloads to a facility with improved energy-efficiency characteristics (ISO 14001/ISO 50001), migrating 100+ PB of data while prioritizing hardware reuse and certified recycling.

Social

- More than 1,800 employees across 67 countries; voluntary attrition decreased to 7.51%.
- Expanded a Voice of Employees program providing a structured way for employees to submit ideas and feedback on workplace improvements and culture. Fifty percent of submitted ideas were implemented.
- Employee engagement strengthened: eNPS improved to 16 with 73.5% survey participation; 600+ employees engaged in 129 community projects, contributing 2,378 volunteer hours.
- Launched LinkedIn Learning globally (≈70% adoption) and expanded mentorship programs.
- Scaled community impact through the Acronis Cyber Foundation Program:
  Three school building projects (1,289 children), eight IT skills programs (550+ learners) and 40 cyber safety workshops (2,100 participants) delivered by 63 employees and supported by 33 Acronis partners.

Governance

- Completed our first double materiality assessment and defined five material topics and five emerging topics to guide strategy and reporting.
- Strengthened ESG oversight by appointing a Board Sustainability Champion (board member), reinforcing governance and accountability for ESG priorities.
- Launched “Compliance Navigator,” an interactive web tool that helps MSPs and end clients identify applicable requirements (e.g., NIS 2, DORA, HIPAA) and translates them into actionable steps, with guidance on security best practices and how Acronis capabilities can support compliance planning.
- Strengthened responsible technology and AI governance through an AI Use Policy, training and updated customer terms for AI features.
- Advanced responsible procurement by rolling out new procure-to-pay system.

ESG awards

In 2025, Acronis' ESG and community efforts received external recognition across multiple regions. In Serbia, PwC Serbia's "ESG Leaders" awards recognized Acronis in the "Stakeholders engagement" sub-category, highlighting our social, volunteering and diversity initiatives in Serbia.

Aleksandra Vucicevic, Senior Human Resource Generalist receiving PwC Serbia's "ESG leaders" award.

Slav Umlenov, Acronis Country Manager CEE receiving a b2b Media Award in the CSR initiative category.

In Bulgaria, Acronis received third place in the b2b Media Annual Awards 2025 in the "CSR initiative" category, reflecting our ongoing commitment to education, community empowerment and digital inclusion through the Acronis Cyber Foundation Program. This recognition also builds on acknowledgment of our educational and social initiatives in previous years. In Australia and New Zealand, Acronis received the GTIA Spotlight Award for "Advancing Diversity in Technology Leadership." In addition, the Acronis Cyber Foundation Program was named a 2025 TrustRadius Tech Cares Award winner, recognizing corporate social responsibility and community impact.

Acronis' PwC "ESG Leader"' award for stakeholder engagement in Serbia.

Double materiality assessment

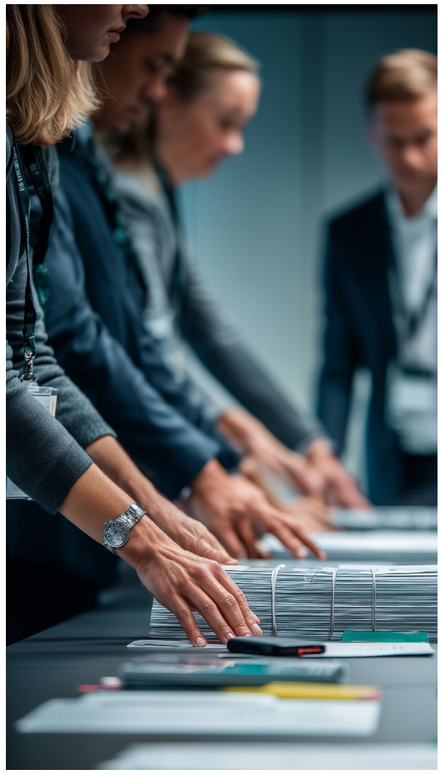
In 2025, Acronis conducted its first double materiality assessment (DMA) to identify the sustainability matters that are most important to our business and our stakeholders.

We applied the double materiality principle, assessing topics from two perspectives:

- **Impact materiality (inside out):** How Acronis' activities, products and business relationships can create positive or negative impacts on people and the environment.
- **Financial materiality (outside in):** How sustainability-related risks and opportunities could affect Acronis' financial performance, position, resilience and long-term value creation.

Methodology

The DMA was led by Acronis' cross-functional ESG committee, with representatives from Corporate Social Responsibility, Procurement, Finance, Government Relations, Data Center Operations, Communications and Marketing. The process and outcomes were reviewed with the Sustainability Champion from the Acronis leadership team and discussed with representatives of the EQT Sustainability Team.



Our approach combined stakeholder input with internal expertise and followed four core steps:

1. **Define scope and topic universe**

   We assessed sustainability matters relevant to Acronis as a global cyber protection company, considering our own operations and key value chain relationships (including suppliers, business partners and customers). The topic universe included common ESG matters as well as Acronis-specific considerations such as responsible technology and cybersecurity-related societal impacts.

2. **Stakeholder engagement and evidence gathering**

   We engaged key stakeholder groups including employees, customers (MSPs and distributors), suppliers, executive management, the board of directors and local communities (NGOs). The primary tool for stakeholder engagement was a set of online questionnaires tailored to each stakeholder group, complemented by internal discussions. Given Acronis' global footprint, we sought input across multiple geographies. We applied stakeholder weighting to reflect the relevance and influence of each group in the context of Acronis' impacts and business model.

3. **Scoring impact and financial materiality**

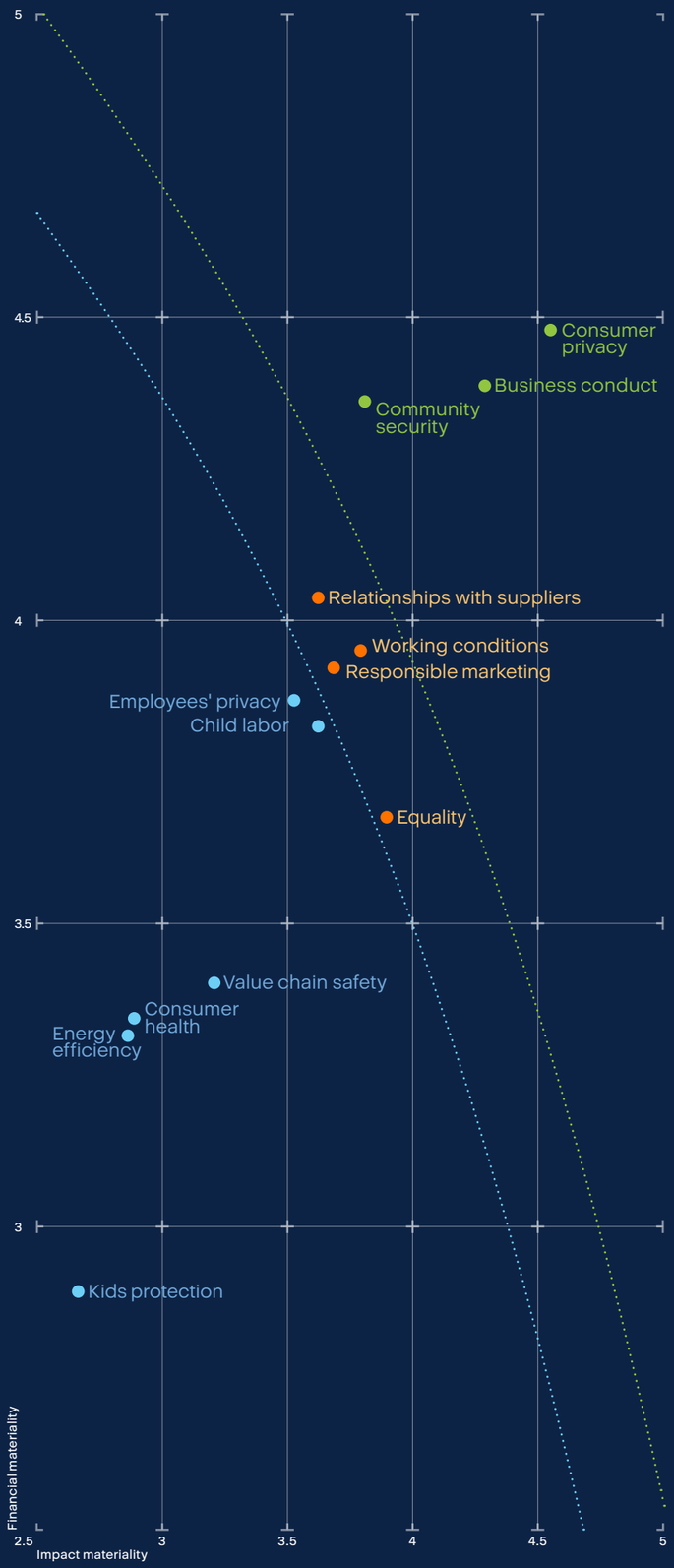
   For each sustainability matter, we assessed both:

   - Impact materiality, considering the severity of impacts (including scale, scope and remediability for negative impacts) and the likelihood of potential impacts.
   - Financial materiality, considering the magnitude and likelihood of sustainability-related risks and opportunities that could affect Acronis' business performance and resilience across relevant time horizons.

4. **Consolidation, validation and governance**

   We consolidated results across the two perspectives and validated the outcomes through expert review with the cross-functional ESG team and leadership oversight. The results are presented to the Acronis leadership team and board of directors as part of the annual ESG report review process. We expect the DMA to be reviewed periodically as our business evolves, stakeholder expectations shift and the maturity of our ESG data and processes increases.

Materiality matrix



Material topics

Based on the DMA outcomes and expert validation, Acronis identified the following material sustainability topics for this reporting period:

- **Protection** of consumer privacy.
- **Business conduct** (including corporate culture and prevention of bribery and corruption).
- **Security-related impacts** on communities.
- **Responsible use of AI** (added following expert review to reflect the growing importance of responsible technology governance and market expectations).
- **Climate change** (added following expert review to reflect the growing importance of climate-related risk management, stakeholder expectations for emissions transparency and evolving regulatory and market requirements).

These topics shape our reporting priorities and guide how we allocate resources and define sustainability initiatives across our operations and value chain.

Emerging material topics

In addition, we identified a set of emerging topics that are strategically important and monitored closely. These topics did not rank among our top material priorities in this assessment, but they may increase in significance over time due to changes in business scale, stakeholder expectations, regulations or operating context.

Our emerging topics are:

- **Working conditions** of our own workforce.
- **Equal treatment and opportunities** for our own workforce.
- **Management of relationships with suppliers.**
- **Responsible marketing** practices.
- **Energy use and efficiency** (added following expert review, reflecting relevance to our operational footprint and external expectations).

We will continue to strengthen data collection and management processes across these areas and integrate them more deeply into our reporting and sustainability roadmap as our ESG maturity develops.

Impacts, risks, opportunities

After determining the material sustainability topics, we assessed the related impacts, risks and opportunities (IROs) to better understand where Acronis affects people and the environment, and where sustainability matters could affect Acronis' business.

- Impacts include both positive and negative effects on people and the environment across our operations and value chain. We assessed impact materiality based on severity (including scale, scope and remediability for negative impacts) and the likelihood of potential impacts.
- Risks and opportunities capture sustainability-related factors that could affect Acronis financially, assessed through magnitude and likelihood.

The cross-functional ESG committee led the IRO analysis to ensure perspectives from across the business were reflected. The resulting IROs are summarized in the table below and are used to support ESG disclosures, prioritize actions and inform strategy and risk-management discussions.

Climate change adaptation	
Impacts	Strengthening climate resilience (e.g., business continuity planning and crisis response) can reduce disruption impacts on operations and service delivery.
Risks	Extreme weather events may disrupt suppliers and third-party data center operations, potentially affecting service availability, business continuity and financial performance. Heatwaves and poor air quality events can affect employee health and well-being and may disrupt commuting and office operations in affected locations.
Opportunities	Hybrid working arrangements can support operational continuity during extreme weather events or local emergencies. Cybersecurity, backup and disaster recovery capabilities can support customer resilience and continuity planning during disruption events.

Climate change mitigation	
Impacts	Our operations (including offices) and the electricity used across our digital infrastructure (including third-party data centers supporting our services) contribute to greenhouse gas (GHG) emissions. Improving operational efficiency (e.g., workplace energy management, travel and event optimization) can reduce emissions and support climate-related risk management over time. Local initiatives (e.g., tree planting and cleanup activities) can support community engagement and local environmental outcomes, while operational emissions reductions depend primarily on energy and efficiency measures.
Risks	Increasing climate-related regulation, disclosure expectations and stakeholder scrutiny may increase compliance costs and reputational risk if transparency and performance do not meet expectations. Physical climate impacts may indirectly affect access to energy and infrastructure reliability, influencing operational resilience and costs.
Opportunities	Improving product efficiency (e.g., reduced endpoint resource use) can support customer IT efficiency objectives and may be valued in procurement and partner requirements. Increasing renewable electricity coverage (e.g., through renewable electricity instruments where applicable) and prioritizing data center partners with higher renewable sourcing can support emissions reduction efforts over time. Climate-related initiatives can support employee engagement and partnerships in the communities where we operate.

Climate change, Energy	
Impacts	As our customer base and company grow, overall electricity consumption across offices and digital infrastructure may increase. By improving energy efficiency and increasing renewable electricity coverage (e.g., through renewable electricity instruments where applicable), we can reduce Scope 2 emissions and manage energy-related costs over time.
Risks	Increases in energy prices could lead to higher operational costs. New regulations may limit the use of nonrenewable energy sources, introduce additional reporting requirements, or increase costs for energy-intensive activities. Power outages or grid disruptions could affect operations in certain offices and third-party data centers, potentially impacting service availability.
Opportunities	Energy efficiency measures in offices and IT operations can reduce energy use and help manage operating costs.

Responsible use of AI

Impacts

Inappropriate or insufficiently controlled AI use may increase risks of sensitive data exposure, unintended data use or compliance breaches.

Biased or misleading AI outputs may lead to unfair outcomes, operational errors, legal exposure or reputational impacts.

Fast-evolving regulations and customer expectations may increase compliance complexity.

Risks

Increased use of AI (including third-party tools) can increase electricity consumption and place additional demand on digital infrastructure, depending on the type of use and scale of adoption.

AI can change job roles and skills needs across functions, creating both upskilling opportunities and transition challenges.

Use of AI (including third-party tools) can affect how personal data and sensitive information is handled if governance and controls are not applied consistently.

Opportunities

Well-governed AI use can improve productivity, quality and consistency in selected internal processes and customer support activities.

AI-enabled security capabilities may strengthen detection and response performance and support competitiveness, subject to appropriate controls and validation.

Clear AI governance (policies, training, vendor controls and oversight) can strengthen trust with customers, partners and regulators.

Security-related impacts on communities

Impacts

Our products and services can help organizations (including community organizations) reduce cyber risk and strengthen resilience.

Through technologies and education initiatives, we can contribute to improved cyber hygiene and reduced exposure to common threats.

Social initiatives delivered through the Acronis Cyber Foundation Program can support education and community resilience in locations where we operate.

Risks

Conflicts and crises in countries where we operate may affect employee safety and disrupt business continuity.

A significant cyber incident affecting customers or partners could contribute to wider harm and undermine trust.

Opportunities

Improved cyber resilience across local ecosystems can support continuity for SMEs and community organizations and contribute to broader economic stability over time.

Increasing regulatory requirements (e.g., NIS 2, GDPR, etc.) and growing cyberthreats are expanding the market for Acronis' backup, security and data protection solutions.

Protection of consumer privacy

Impacts

How we collect, process, store and transfer data can affect individuals' privacy and customers' compliance obligations.

Our products can support customers in protecting personal data and improving privacy outcomes.

Strengthening security and data handling practices across relevant business relationships and suppliers can support stronger privacy outcomes across the value chain.

Risks

A personal data breach may lead to regulatory exposure, litigation risk, financial costs and reputational impacts.

Rapidly changing data protection and AI-related regulations across jurisdictions may increase compliance efforts and complexity.

Opportunities

Strong privacy frameworks can support access to highly regulated customer segments and markets.

Privacy-by-design approaches can reduce rework and compliance risk across products and internal processes.

Impacts, risks, opportunities

Business conduct: Corporate culture, prevention of bribery and corruption

Impacts

Corporate culture and ethical standards influence decision making and behavior across the organization and in business relationships.

Given the central role of work in people's lives, workplace culture can positively or negatively influence employee experience and well-being.

Participation in bribery or corruption can undermine trust, fair competition and the rule of law in the markets where we operate.

Risks

Misconduct (including bribery and corruption) may result in legal penalties, financial losses, exclusion from business opportunities and reputational damage.

Inconsistent application of policies across geographies and third parties may increase compliance risk.

Cultural misunderstandings in distributed teams may reduce collaboration effectiveness.

Opportunities

Investment in culture, controls and speak-up mechanisms can support early issue detection and reduce incidents.

Transparent governance and effective third-party due diligence can strengthen stakeholder confidence and reduce transaction risk.

Our commitment to ESG

At Acronis, sustainability is part of how we build a resilient business and create long-term value. As a global cyber protection company, we protect data, applications and systems. We recognize that trust depends not only on security, but also on responsible environmental, social and ethical practices.

Our sustainability priorities are shaped by our double materiality assessment and ongoing stakeholder engagement, helping us focus on the topics that matter most across our operations and value chain.

We report progress transparently through our annual ESG report and continuously strengthen the quality of the data that underpins our disclosures.

Alona Geckler, SVP of Business Operations, Chief of Staff and Sustainability Champion at Acronis.

We organize our sustainability strategy around five pillars:

- **Environmental stewardship:** Improve GHG emissions accounting and management across Scopes 1–3, increase renewable electricity coverage, improve efficiency in offices and cloud operations and support circular practices such as hardware reuse and responsible e-waste management.
- **Cybersecurity, privacy and responsible use of technology:** Strengthen cyber resilience for customers and partners while protecting privacy, support responsible use of technology and uphold robust information security and ethical standards.
- **Responsible use of AI:** Acronis recognizes that AI can create new risks and opportunities for cybersecurity and business operations. We aim to use AI responsibly and in line with our existing security, privacy and ethical standards. As our AI capabilities and use cases evolve, we will continue to develop internal guidance and governance practices to help manage risks such as privacy impacts, security considerations and potential misuse.
- **People and communities:** Foster an inclusive and engaging workplace, support employee well-being and development, and contribute to communities through the Acronis Cyber Foundation and partner-led initiatives.
- **Strong governance:** Maintain strong governance, ethics and compliance functions, and respect human rights across our value chain.

In line with investor expectations, we plan to define a company-specific transformational KPI in 2026.

Environmental

Greenhouse gas emissions

Acronis' environmental footprint is primarily driven by electricity and fuel consumption across our offices and the third-party data centers supporting our cloud services, as well as value chain emissions from purchased goods and services, business travel and the use phase of our sold products (Acronis software). Our environmental program focuses on strengthening emissions transparency, increasing renewable electricity coverage, and reducing energy demand through efficiency improvements in our workplaces and cloud operations. Total emissions decreased by 40% from 2024 to 2025.

Emissions	2024 (tCO2e)	2025 (tCO2e)
Scope 1	78.81	1266.76
Scope 2 (location based)	868.85	730.71
Scope 2 (market based)	1071.09	807.08
Scope 3	178,805.49 *	105,527.38
Total scope 1, 2 and 3 (location based)	179,753.16	107,524.85

* Scope 3, Category 5 emissions for 2024 were recalculated after an error was identified in the initial. The correction has been applied to the 2024 baseline to improve accuracy and ensure consistency and comparability of year-on-year Scope 3 reporting.

Data reliability and emissions output

Acronis worked closely with its sustainability advisory partner to support the accuracy, consistency and reliability of our carbon footprint calculations. As data collection and analysis must be completed before the end of the financial year, actual data from January to October 2025 has been used for Scope 1, Scope 2 and Scope 3 Categories 3, 5, 7 and 8, with estimations applied for Q4. Conversely, Q4 Category 1, 2, 6 and 11 actuals were available to incorporate in our 2025 GHG footprint. We continuously strengthen data quality, documentation and controls to improve the robustness of year-on-year reporting.

Prior-year restatement

Following an external review by a sustainability advisory partner, we identified an error in the calculation of Scope 3, Category 5 (Waste generated in operations) in our 2024 inventory. The 2024 figure has changed from 206.04 tCO2e to 154.58 tCO2e. The 2024 Scope 3 and total emissions figures have been restated to improve accuracy and ensure comparability. Unless otherwise stated, all references to 2024 emissions in this report reflect the restated values.

Carbon footprint calculation methodology

The 2025 GHG inventory has been primarily calculated using a spend-based method, leveraging 2025 financial data combined with activity-based methods for some categories. Year-on-year movements may reflect both underlying changes in operational activity and value chain drivers, as well as improvements in data quality and methodological refinements.

Greenhouse gas emissions

	Scope 3 category	Share
1	Purchased goods and services	7.9%
2	Capital goods	0.6%
3	Fuel and energy-related activities	0.4%
5	Waste generated in operations	0.1%
6	Business travel	1.8%
7	Employee commuting	0.1%
8	Upstream leased assets	7.1%
11	Use of sold products	82.1%
12	End of life of sold products	0.004%

Scope 1 emissions

Scope 1 emissions primarily relate to stationary combustion (e.g., backup generators) and other direct fuel use where applicable. The increase in Scope 1 emissions in 2025 is mainly attributable to an updated estimation approach for stationary combustion. Where direct fuel consumption data was not available, we applied standardized assumptions to estimate generator fuel use based on office size.

Scope 2 emissions

In 2025, purchased electricity consumption totaled 1,500 MWh, representing the largest driver of Scope 2 emissions. We purchased energy attribute certificates (EACs) to match 70% of our electricity consumption with renewable electricity. The EAC portfolio includes Guarantees of Origin (GOs) in Europe, I-RECs in selected non-European markets, and Green-e Certified RECs in North America. These certificates represent the environmental attributes of renewable electricity generation and support market-based Scope 2 reporting; they do not change the physical electricity supplied to our sites.

Greenhouse gas emissions

Scope 3 emissions

In 2025, Scope 3 emissions accounted for 98% of total emissions, encompassing supply chain emissions, business travel, leased data centers, use of sold products and more.

2025 vs. 2024

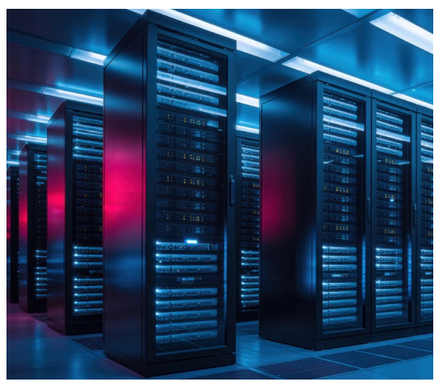
Primary drivers of changes in Scope 3 emissions in 2025 compared to 2024 base year are updated estimations of stationary combustions, changes in software volume, and improved data quality in several categories. Categories 4, 9, 10, 13, 14 and 15 are excluded from the calculations due to low materiality.

Key drivers of scope 3 emissions

- **Use of sold products** (Category 11 – 82.1%) remains the most material source of emissions. These emissions are associated with the electricity consumed during the operation of Acronis software by customers. In 2025, emissions in this category decreased by 41% compared to 2024, primarily due to changes in software volumes and the application of updated, less carbon-intensive electricity emission factors.
- **Purchased goods and services** (Category 1 – 7.9%) reflects emissions embedded in procured IT equipment, professional services and other operational expenditures. While smaller in relative share, this category is material from a supplier engagement and procurement strategy perspective.
- **Upstream leased assets** (Category 8 – 7.1%) is the third-largest contributor and relates primarily to energy consumption in third-party data centers. Emissions decreased year on year due to improved data completeness and reporting coverage. Data center electricity use and power usage effectiveness (PUE) are key determinants of this category's footprint.
- **Business travel** (Category 6 – 1.8%) contributes a modest share of total Scope 3 emissions, with air travel being the primary driver within the category.

	Scope 3 by categories	2024 (tCO_2e)	2025 (tCO_2e)
1	Purchased goods and services	7868.69	8310.12
2	Capital goods	703.26	684.01
3	Fuel and energy related activities	204.33	392.21
5	Waste generated in operations	154.59*	59.44
6	Business travel	2282.56	1878.18
7	Employee commuting	40.61	75.76
8	Upstream leased assets	9518.59	7488.68
11	Use of sold products	158,025.23	86,634.85
12	End of life of sold products	7.56	4.12

* Scope 3, Category 5 emissions for 2024 were recalculated after an error was identified in the initial. The correction has been applied to the 2024 baseline to improve accuracy and ensure consistency and comparability of year-on-year Scope 3 reporting.



Outlook

Given that Scope 3 emissions account for the vast majority of Acronis' GHG footprint, structured supplier engagement, software efficiency improvements and enhanced data quality will remain central to our approach to managing emissions. Continued improvements in data transparency, governance and methodological robustness will further strengthen the credibility and usefulness of our Scope 3 reporting.

Our offices

In 2025, we continued to reduce the environmental footprint of our workplaces by optimizing space and improving resource efficiency. We reduced occupied office space in Israel, Japan and Italy and closed our U.K. office, cutting our total office footprint by 2,376 m² which, over time, will lower energy use for heating, cooling and lighting. In 2026, we plan to continue optimizing office space across our footprint, balancing business needs with efficient, lower-impact operations.

Across our global locations, we provide recycling facilities and encourage proper waste sorting. In Bulgaria, we installed smart sorting bins in our Sofia office to improve waste separation. Based on data from February to December 2025 for an occupancy of around 50 people, the system identified that roughly 29% of waste is reducible, highlighted avoidable items such as disposable cups and food containers, and delivered an estimated CO_2 reduction equivalent to removing about 6.5 cars from the road per year, alongside approximately €1,788 in annual savings in municipal and office waste disposal costs. The office also uses water-saving tap aerators that typically reduce water consumption by around 30% compared with standard fittings.

Several of our offices are located in certified green buildings, including our LEED Gold–certified offices in Bulgaria and Germany and our Singapore office, which is located in a building with a Green Mark operational rating. Our team in Turkey is based in Technopark Istanbul, which the Ministry of Energy recognized in 2025 as the country's most energy-efficient commercial service building, reinforcing our aim to operate from efficient, lower-impact facilities.

Our focus on creating sustainable and people-centric workplaces also extends to how we design working arrangements. In 2025, Acronis won first place in the "Flexible Workplace" category at the b2b Media Employer Branding Awards in Bulgaria, recognizing our efforts to provide a work environment that supports flexibility, trust and a healthy balance between productivity and well-being.

As a next step, we plan to improve the consistency of data collection on waste, water and office space so we can more accurately track and manage our operational impact over time.

Acronis Serbia team in the office in Belgrade.

E-waste

To reduce potential e-waste and extend the useful life of our hardware, in 2025 we donated 90 monitors and 120 PCs for reuse by schools in Bulgaria and Niger, (the latter of which where Acronis opened a resource center in 2024), rather than sending them for disposal. Prioritizing reuse ahead of recycling supports a more circular approach to IT equipment, cuts the volume of electronic waste we generate and helps direct functioning devices to users who might otherwise lack access to up-to-date technology.

Environmental days

In 2025, Acronis employees continued to turn our environmental commitments into concrete action through a series of volunteer "environmental days" focused on local ecosystems, waste reduction and climate awareness. These activities not only reduced our footprint in the communities where we operate but also strengthened employee engagement around sustainability.

Cleanup events

Over the year, Acronis teams organized 18 cleanup events in 11 regions. Together, they collected a total of 1,500+ kg of litter (approx. 3,300 lbs.) from beaches, city parks, riverbanks and neighborhoods near our offices.

A highlight of the year was our participation in U.N. World Cleanup Day 2025, where eight Acronis offices joined a coordinated global challenge. As part of this initiative, eight cleanup events were organized, collecting 896 kg (1,975+ lbs.) of waste.

These efforts helped remove mixed municipal waste, plastics and packaging materials from local environments, while also raising awareness of responsible waste management among employees and their families.

In 2026, Acronis plans to build on these results by systematizing environmental days as recurring annual activities, expanding to additional offices.

18
clean ups

1,780
trees planted

1,500 kg
of waste collected

992
volunteer hours

~107 tCO_2
to be removed per year

Acronis "Cyber Leaders" Program participants planting trees.

Acronis Boston team during a cleanup event.

Acronis Singapore team during a cleanup event.

Tree-planting initiatives

In parallel to cleanup activities, Acronis organizes tree planting days to support local biodiversity and contribute to long-term carbon sequestration.

In 2025, hundreds of employees took part in tree-planting initiatives across three regions, resulting in 1,780 trees planted in city parks and schoolyard areas in Romania, Bulgaria and Serbia. Projects were designed together with local partners and municipalities to ensure that species selection and planting locations support local ecosystems and maximize survival potential. Activities often included short awareness sessions on urban heat islands, soil health and the role of trees in climate adaptation.

Based on a standard urban-tree sequestration factor (10-year average), these plantings are estimated to remove ~107 tCO_2 per year on average over the next decade (around ~1,068 tCO_2 cumulatively over 10 years). Actual sequestration will depend on tree survival and growth conditions and will be refined as local data becomes available.

Sustainable events

When running internal and external events, we aim to reduce waste and use resources more effectively by prioritizing reusable event materials and selecting merchandise with more responsible material choices. In 2025, this translated into scaling reusables across events such as reusable table covers and backdrops and shifting core giveaways toward recycled or certified material options and longer-lived products that attendees can keep using beyond the event.

Across 2025, we distributed merchandise at scale, including 459 rPET backpacks and 820 rPET umbrellas, supported by vendor-provided product footprint calculations (2.73 kg CO_2 per backpack and 2.00 kg CO_2 per umbrella, each benchmarked by the vendor against conventional alternatives). We also provided tote bags for event and community engagement, including 2,435 cotton totes and 500 organic cotton totes. To reduce single-use beverage waste, we introduced reusable drinkware at scale with ~5,000 stainless steel tumblers delivered in 2025 supporting an estimated ~5,000 single-use plastic water bottles avoided on a one-time substitution basis.

Acronis merchandise.

Note: Unit volumes are estimates where automated reporting was not available, and product carbon footprint values are vendor reported and may be updated over time as underlying datasets and methodologies evolve.

Environmental days

Responsible innovation

Our approach

As a cyber protection company, Acronis' impact centers on the security, privacy and reliability of our services. These pillars build customer trust and ensure the resilience of the digital environments we protect.

Our 2025 double-materiality assessment confirmed "Data privacy and security" and "security-related impact to communities" as priority topics, reflecting both our responsibility to safeguard our customers' data and our role in helping organizations worldwide meet rising regulatory and resilience expectations.

We manage these topics through our focus on cybersecurity, privacy and responsible use of technology. We embed security and privacy into both product development and operations through secure-by-design and privacy-by-design practices, a secure software development lifecycle and regular independent assurance.

This includes ISO/IEC 27001 certification, which confirms a structured information security management system, and SOC 2 Type 2 reporting for Acronis Cyber Cloud, which provides third-party assurance that key security and availability controls are operating effectively over time.

Oversight sits with our Chief Research and Development Officer, supported by cross-functional leaders in product, AI research, data center operations, security, compliance and ESG. Together, they set policies, review AI and data-related risks and monitor progress against key indicators such as product certifications, vulnerability and incident metrics, privacy complaints and the adoption of renewable and efficient infrastructure in our data centers.

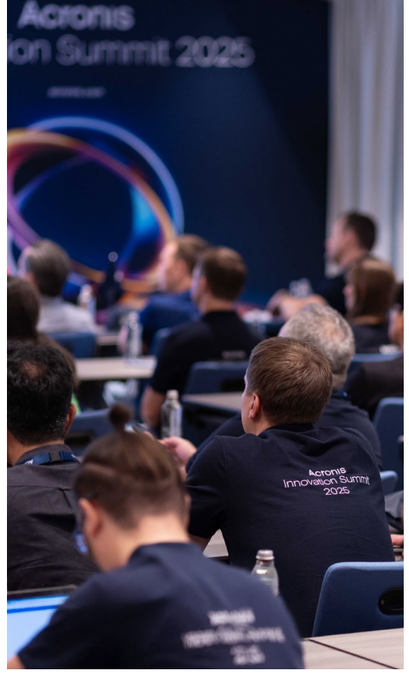
We evaluate the effectiveness of this approach through third-party security testing, participation in industry standards bodies, internal KPI reviews and feedback from customers and partners. Where gaps are identified — for example, emerging AI regulation or new cyberthreat patterns — we adjust our roadmap and controls accordingly.

Our product

Acronis provides an integrated cyber protection platform that unifies backup, disaster recovery, endpoint protection, EDR and management capabilities in a single solution, designed for managed service providers (MSPs), small and medium-sized businesses and enterprises. Our products help customers keep data available and recoverable, reduce the risk of cyberattacks and demonstrate compliance with evolving frameworks and regulations.

Security and privacy are embedded in our product design. We apply S-SDLC practices, conduct regular threat modeling and enforce rigorous code review and testing standards. Data is protected with strong encryption in transit and at rest. For data at rest, including in cloud storage, we use enterprise-grade AES-256 encryption. Our role as a CVE Numbering Authority (CNA) and our public Security Advisory Database further support transparency by providing customers with up-to-date information on vulnerabilities and patches across Acronis products.

By consolidating multiple tools into a single platform, we aim to help customers improve their cyber resilience while avoiding complexity, operational risk and resource overhead that can arise from fragmented point solutions.

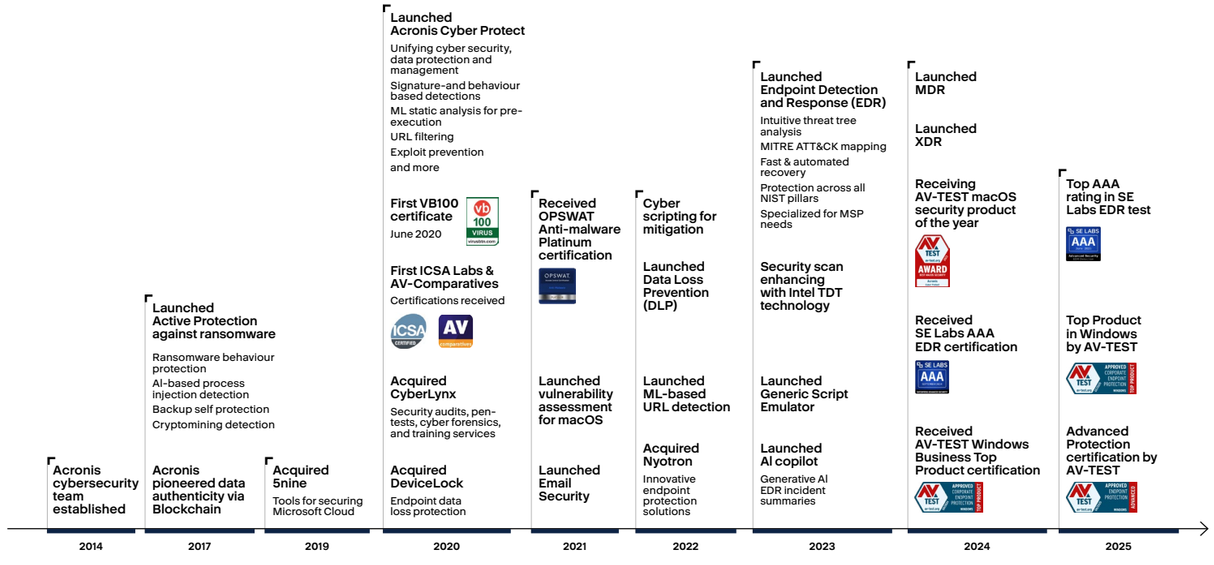


Acronis R&D team during "Innovation Summit."

Security technology evolution

Acronis has evolved from a backup vendor into a cyber protection platform that brings together data protection, cybersecurity and management in one architecture. This strategic shift is designed to help organizations reduce downtime and recover faster from cyber incidents by connecting prevention, detection, response and recovery in a single operational flow. In 2025, we continued strengthening this integrated model by improving how backup, endpoint detection and response (EDR), access controls and automated remediation work together — aiming to shorten detection-to-recovery time while keeping deployment and day-to-day use simple for IT teams and MSPs.

Our approach is built on three reinforcing layers. Prevention and detection combine signature-based, behavioral and AI-assisted techniques, informed by threat intelligence from the Acronis Threat Research Unit (TRU). Response and recovery connect EDR actions with backup and restore workflows to isolate threats, roll back harmful changes and restore systems quickly. Continuous hardening is supported through a secure software development lifecycle, third-party security testing of our cloud environment and a bug bounty program that encourages responsible disclosure. Together, these capabilities are designed to reduce the "protection gap" between when an attack begins and when defenses can respond, while providing customers with consolidated visibility into their cyber posture.

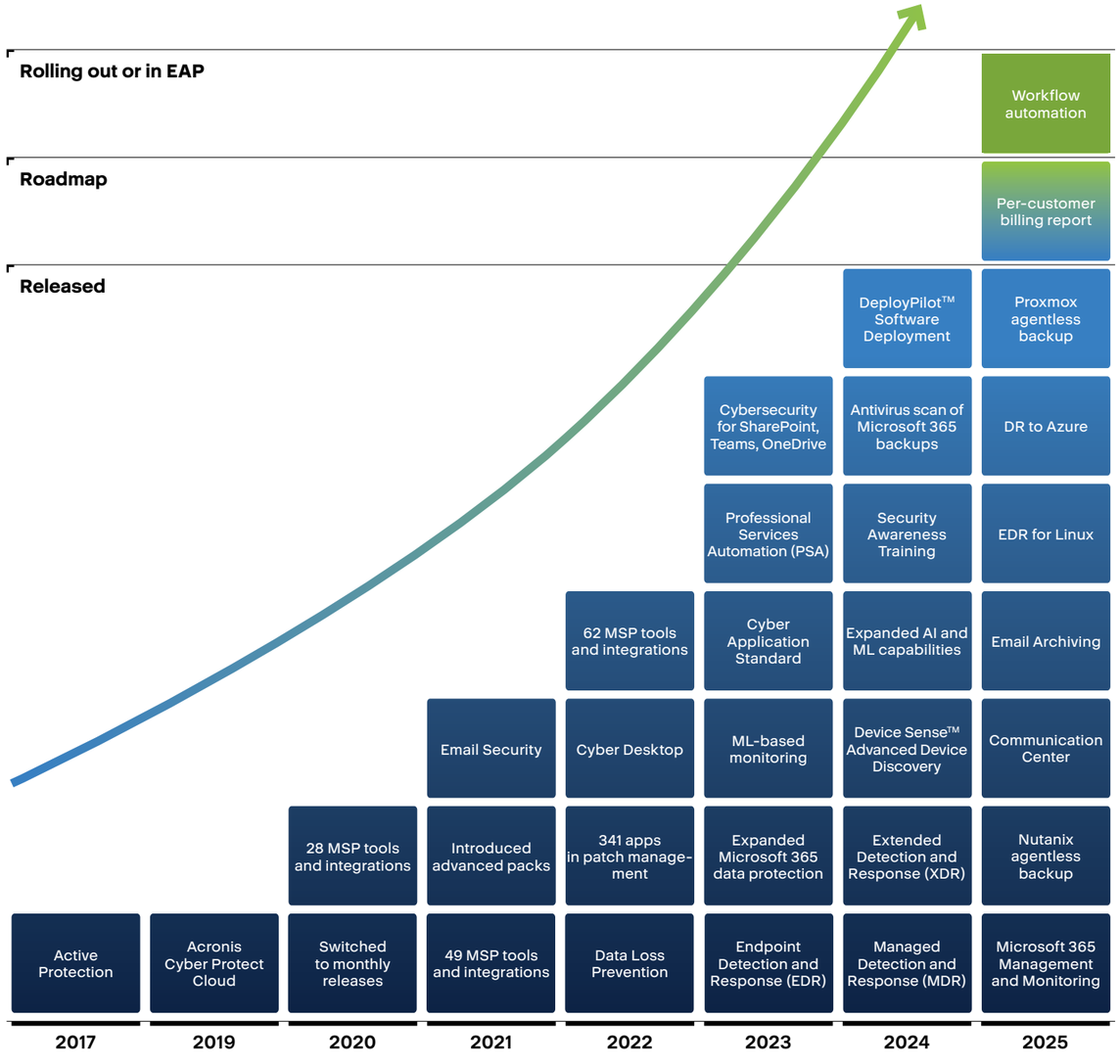


Product innovations

In 2025, Acronis delivered pragmatic innovation aimed at MSP scale — improving governance, strengthening protection, expanding workload coverage and increasing operational transparency. Updates focused on helping partners standardize service delivery across multitenant environments, reduce operational effort and support customer compliance with clearer controls and reporting.

First, we enhanced centralized governance and access control, including stronger policy and agent management and role-based controls aligned with least-privilege principles, helping reduce configuration drift and improve auditability. Second, we expanded coverage and continuity through broader infrastructure support, including new agentless backup options and additional disaster recovery scenarios across more hypervisors and Linux environments, alongside improvements in Microsoft 365 protection and archiving to support higher-volume tenants and long-term retention needs. Third, we strengthened security and response capabilities, including improvements to threat hunting and web controls, as well as efficiency-focused protection enhancements that aim to improve detection while minimizing endpoint performance impact. Finally, we increased partner operational transparency through improvements in usage, reporting and billing visibility — supporting clearer reconciliation and more predictable service operations.

These releases reflect a consistent direction: Enabling MSPs and IT teams to deliver secure, resilient services with less manual overhead, faster response and more consistent compliance outcomes.



Recognition and independent validation

Acronis' approach to responsible innovation is backed by external validation of both our technology performance and our broader cybersecurity ecosystem.

Across 2022–2025, our endpoint security capabilities have been repeatedly assessed through independent tests and certifications (including programs run by AV-TEST, AV-Comparatives, Virus Bulletin and SE Labs), demonstrating consistent third-party scrutiny over time. In 2025, this included strong results in publicly available AV-TEST benchmarking, where Acronis Cyber Protect ranked among the top performers for low performance impact in business Windows testing (May–June 2025). In addition, independent testing in 2025 validated effectiveness against advanced threats, including a perfect 35/35 score in AV-TEST Advanced Threat Protection (May–June 2025) and an SE Labs AAA rating for XDR, with 100% detection accuracy and 98% total accuracy (June 2025).

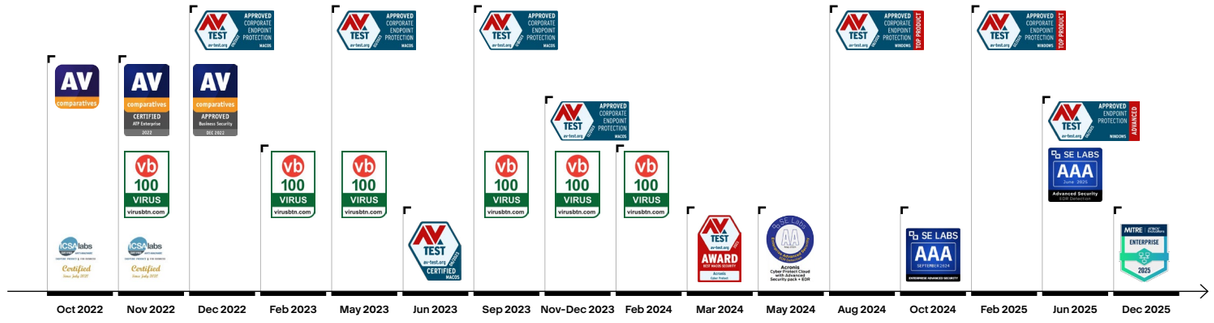
G2 CROWD — **Rating:** 4.7 out of 5

Gartner peerinsights — **Multiple ratings**
Cloud: Backup as a Service 4.6/5
Corp: Endpoint protection platforms 5.0
Corp: Enterprise Backup and Recovery 4.4

TrustRadius — **Multiple ratings**
Cloud: Endpoint security 9.0/10
Corp: Enterprise backup, Saas Backup, and Disaster Recovery 6.7/10

Trustpilot — **Rating:** 3.9 out of 5

SoftwareReviews — **Champion in:**
Backup & Availability, Endpoint Protection, XDR, DLP, Email Security, RMM, MDR, EDR



We also received analyst recognition for platform and ecosystem execution. In the 2025 Canalys Global Cybersecurity Leadership Matrix, Acronis was named a "Champion" alongside a small group of leading cybersecurity vendors. Canalys highlighted Acronis' MSP-first approach and the value of integrating cybersecurity, data protection, Microsoft 365 protection and MSP operations, with leadership and momentum scores of 52% and 62%, respectively, and also recognized Acronis in its Managed Backup & Disaster Recovery Leadership Matrix report. In parallel, Frost & Sullivan's 2025 Frost Radar: Endpoint Security recognized Acronis' unified platform model (single-agent approach spanning endpoint security, backup and recovery and endpoint management) and noted our ongoing R&D investment and innovation capacity. Further analyst and market recognition in 2025 included being named a Leader in the IDC MarketScape: Worldwide Cyber-Recovery 2025 Vendor Assessment.

Verified reviewer platforms also reflected strong customer sentiment, including Gartner Peer Insights Customers' Choice for backup as a service, #1 placement in G2's Fall 2025 EDR Grid Report (with 95% of reviewers indicating they are likely to recommend Acronis), and Champion-status in numerous Info-Tech SoftwareReviews.com categories including Endpoint Protection, Backup & Availability, EDR, XDR, MDR, DLP and RMM.

Canalys Global Cybersecurity Leadership Matrix 2025

Software efficiency

To reduce the environmental impact associated with running our cyber protection solutions, we focus on improving software efficiency — lowering the computing load on protected workloads while continuing to expand platform capabilities. A key element of this approach is consolidation: Instead of deploying separate tools for backup, malware protection, RMM and EDR, Acronis delivers these capabilities through a single, integrated agent. This helps customers and partners reduce operational complexity and avoid duplicative resource consumption across endpoints, while enabling MSPs to support more customers and workloads with fewer physical resources.

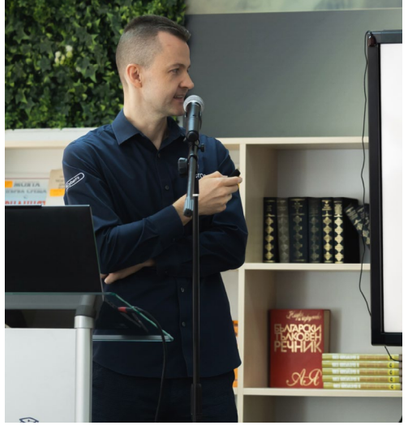
We also work to quantify and improve our software-related footprint. In 2024, we engaged an external ESG consultancy to assess the carbon footprint of our software, and we can provide this information to partners upon request to support their own sustainability assessments and reporting. In 2025, we continued prioritizing performance optimization as part of responsible product design. In the latest AV-TEST evaluation of Windows antivirus software for business users (May–June 2025), Acronis Cyber Protect ranked in the top three for performance impact, with an overall system performance impact of 8.11% in the published results. This supports our objective to deliver robust protection without disproportionately burdening endpoint resources — an important factor for both productivity and energy efficiency.

Report is available here:
www.av-test.org/en/antivirus/business-windows-client/windows-10/june-2025/

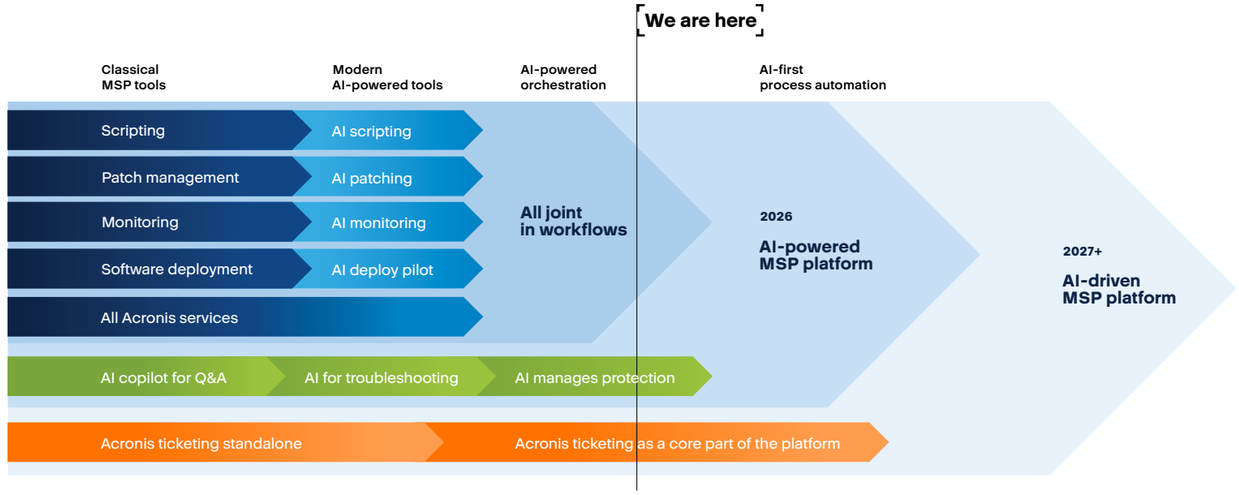
Vendor / Product	Performance Impact %	Rank
AhnLab V3 Endpoint Security	7.58%	1
Legendsec QI-ANXIN Tianqing	7.87%	2
Acronis Cyber Protect	**8.11%**	**3**
Microworld eScan Enterprise EDR	8.75%	4
Seqrite Endpoint Security	9.01%	5
WithSecure Elements Endpoint Protection	9.41%	6
Avast Ultimate Business Security	9.59%	7
Microsoft Defender Antivirus (Enterprise)	9.69%	8
Qualys Endpoint Protection	9.72%	9
Kaspersky Small Office Security	9.86%	10
ESET PROTECT Advanced	9.91%	11
Kaspersky Endpoint Security	9.93%	12
HP Wolf Security	10.39%	13
Sophos Intercept X Advanced	11.21%	14
Trellix Endpoint Security	11.41%	15
Bitdefender Business Security Enterprise	12.34%	16
Check Point Endpoint Security	22.43%	17

AI innovation

Acronis is advancing its strategic focus on artificial intelligence, embedding AI innovation deeply within both its product development and internal operations. The company is committed to evolving its unified platform model by leveraging AI to enhance endpoint security, backup and recovery and endpoint management, ensuring greater efficiency and resilience against cyberthreats. This direction is supported by continuous investment in research and development, with plans to further expand the scope of AI across its portfolio and processes in the coming years.



Nick Grebennikoff, Chief Development Officer at Acronis.



Acronis team at the “Innovation Summit.”

In 2026, Acronis will prioritize AI-enabled partner efficiency by advancing an agentic MSP operating model that combines automation with AI-driven decision support. The focus is to lower cost to serve, speed up incident response and improve compliance outcomes across multitenant environments. Key directions include stronger partner-level governance and least-privilege controls to reduce policy drift and improve auditability; more intelligent protection and triage to reduce incident volume and accelerate response; broader, more consistent coverage across workloads and environments to support continuity; and improved operational transparency in usage and billing to strengthen trust. Together, these capabilities are designed to help MSPs standardize delivery, shorten onboarding and differentiate their services through reusable, AI-assisted workflows and reporting.

AI for internal efficiency

Acronis is improving internal efficiency by adopting AI tools across teams and tracking adoption and productivity indicators to guide training and future rollouts.

Recent internal surveys show that at least 80% of employees use AI tools at least once a week, and around 40% use AI assistants or similar tools daily.

Nick Grebennikoff, Chief Development Officer at Acronis.

Key internal AI tools in use include:

- **Acronis AI Assistant (Microsoft Teams):** An internal conversational assistant that helps employees securely access and work with selected corporate knowledge bases. Introduced in October 2025, it averages 100+ requests per user per month and is used regularly by around 250 employees.
- **Conversation analytics (Gong):** Used by sales and support to record, transcribe and summarize calls and highlight follow ups and risks. Around 500 employees use it to analyze approximately 5,000 calls per month.
- **Azure AI Foundry:** A secure platform within the Acronis tenant for deploying and using large language models and building internal AI workflows while keeping company data protected.
- **Acronis True Image Support Bot:** A customer-facing assistant for the True Image product knowledge base. During the first three weeks of operation, it enabled ~25% contact avoidance in the pilot scope.
- **Departmental generative AI use cases:** Teams use enterprise AI tools for research, planning and content drafting. Marketing estimates ~5,000 hours per year saved from these use cases (with human review remaining part of the workflow).
- **AI-powered contract management** supports legal, sales and finance by extracting key terms and helping streamline reviews and obligation tracking.

AI for productivity in R&D

103
active Windsurf users (focus group)

1.1M+
AI-generated lines of code in five months

15%
increase in code-writing speed
(focus group, lines of code in git)

In R&D, AI tools are being used to support code development, code review and test automation. A focus group of early adopters tracked initial impact, including 103 Windsurf users, one million+ AI-generated lines of code in five months and a reported ~15% increase in code-writing speed within that group. AI assistance was also introduced into code review and test development workflows, generating automated review comments and supporting reported productivity gains of up to ~20% in test development for early adopters.

Based on these results, AI-enabled development has been expanded across R&D. Windsurf is now used by 300+ engineers, generating nearly two million lines of code to date. Looking ahead, Acronis' roadmap focuses on further efficiency improvements in development, QA and automation, with an emphasis on secure and responsible AI use and continued upskilling so that routine tasks are reduced and teams can spend more time on higher-value engineering work.

Acronis continuously monitors R&D efficiency by collecting data from the development tools used across engineering teams, including AI-assisted coding tools such as Windsurf and Copilot, as well as Atlassian Bitbucket and Jira. Using this data, Acronis tracks a set of quantitative KPIs, including AI-generated lines of code, committed lines of code and pull-request review duration, in order to measure overall engineering efficiency, understand the impact of AI and process changes and identify opportunities for improvement in development speed and quality.

200
respositories with AI code review enabled

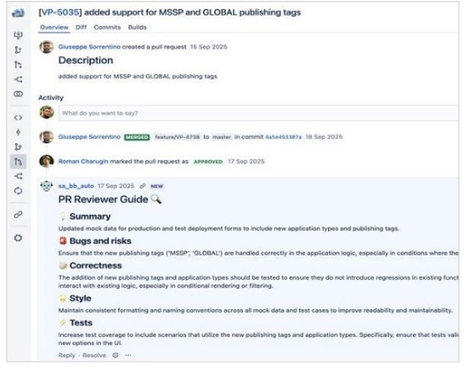
4K+
AI comments generated in Q3

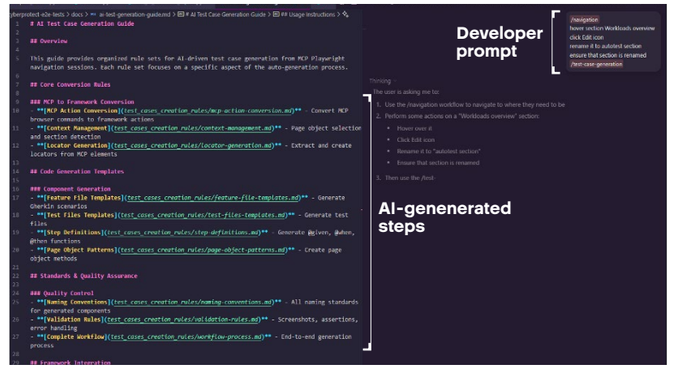
13%
AI comments "liked" by developers

20%
average test development speed boost*

10%
average test development speed boost*

* Test development includes review requirements, create autotest, execute, get results, analyze results.

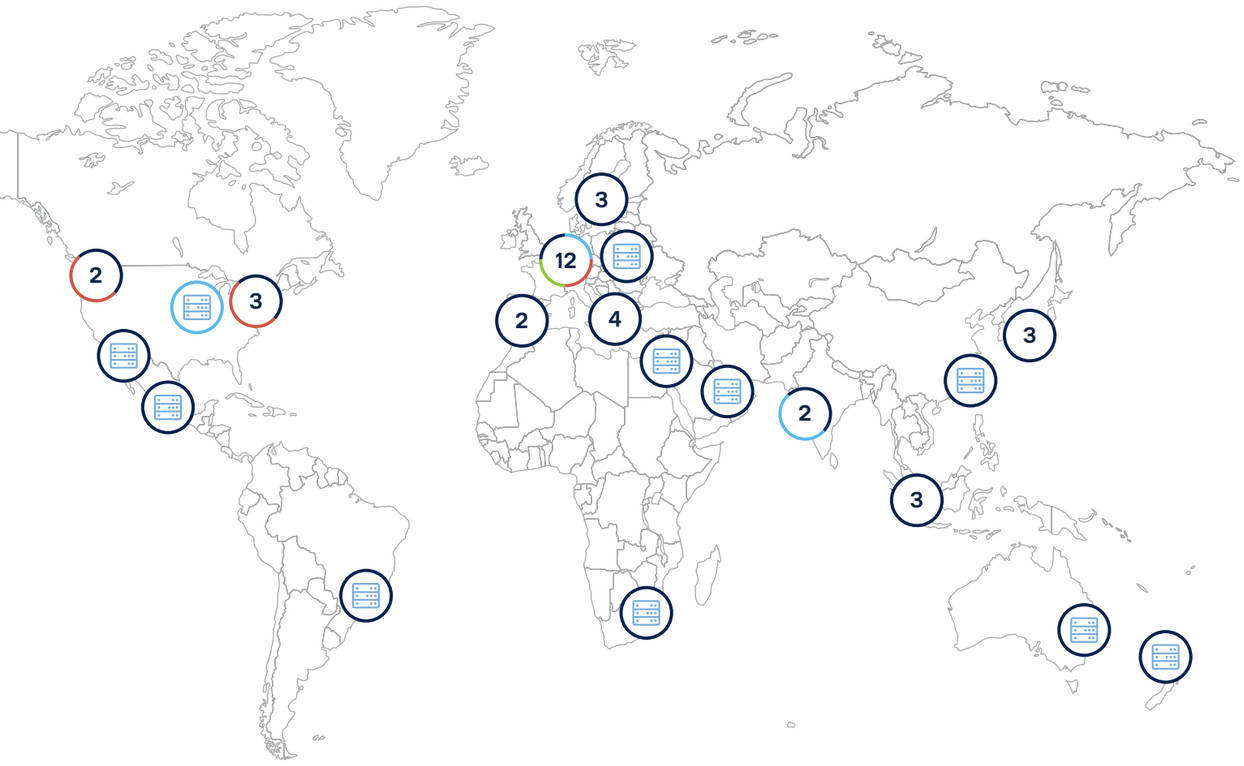




Acronis Cyber Cloud data centers

All facilities are operated by third-party colocation providers, while Acronis remains responsible for the deployment, maintenance and operational management of the hardware and software supporting our cloud services. Our data center footprint requires continuous electricity and cooling and is a material contributor to our environmental impact. Acronis operates data center infrastructure at an exabyte scale, managing over one exabyte (EB) of customer data globally.

Acronis operates 50+ data centers across 42 locations worldwide.



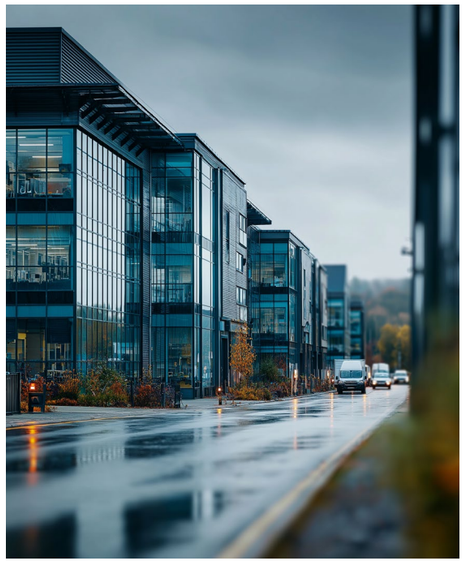
Acronis Cyber Cloud data centers

Acronis Cyber Cloud data centers, Google Cloud Platform or Microsoft Azure cloud storage

Acronis CyberNet data centers

Environmental impacts and emissions

The environmental impact of our data centers is primarily driven by electricity consumption, stationary combustion and refrigerant used for cooling. In 2025, our total GHG emissions associated with data center operations were 10,698.85 tCO_2e, based on information reported by data center operators and estimates applied where primary data was not available. Emissions increased compared to 2024 (9,518.59 tCO_2e), primarily due to increased power demand at several sites and improvements in our calculation methodology.



Improving data quality

We continue to strengthen the quality of data used in our emissions estimates. In 2025, we expanded vendor data requests to include power usage effectiveness (PUE), refrigerant details and water management information, among other factors. Data availability varies across regions and providers. In 2025, we obtained high-quality electricity consumption data from 73% of data centers, while 18% provided complete data on refrigerant leakage or refills. The level of detail collected was higher than in 2024, reducing the number of assumptions required and improving the precision of our estimates.

The Data Center Operations team manages capacity and energy demand through a structured nine-month, forward-looking capacity planning process, designed to support resilience and service continuity while limiting inefficient overprovisioning. The process limits additional deployed capacity to a 20% buffer above current needs. In 2025, we transitioned from manual capacity planning to AI-supported dashboards and demand forecasting to improve planning accuracy and decision making.

2025 infrastructure transition: Frankfurt DC migration

A key data center project in 2025 was the migration of workloads from our Frankfurt site. The building hosting the facility was scheduled to be demolished at the end of December 2025, and Acronis migrated workloads to an alternative facility with improved energy-efficiency characteristics and updated compliance expectations. The project involved 218 employees and required investment in planning and execution. More than 100 petabytes of customer data were migrated. Hardware reuse was prioritized, and a limited number of assets were decommissioned and disposed of through certified recycling vendors. The new Frankfurt facility holds ISO 14001 (Environmental Management) and ISO 50001 (Energy Management) certifications.

Data center ESG engagement

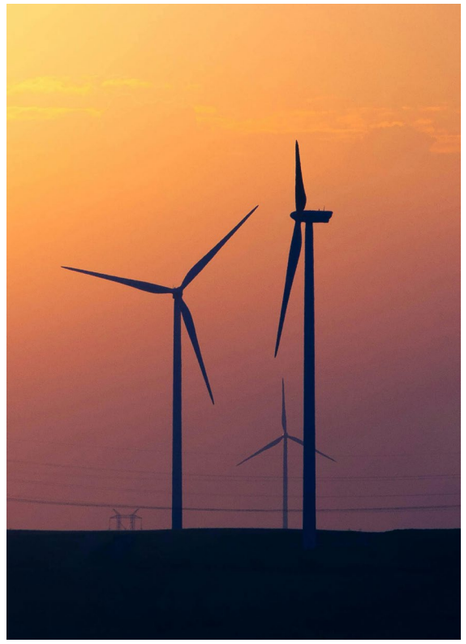
To support ongoing ESG improvements, Acronis conducts engagement with data center partners. In November 2025, Acronis organized an on-site visit to the London data center LHR3 (operated by VIRTUS) for colleagues from the EQT Sustainability Team. The visit reviewed ESG-related aspects of the facility, including renewable electricity arrangements, operational resilience and decarbonization planning and identified opportunities for further improvement.

Vendor standards and certifications

Our data center providers operate under a range of internationally recognized certification frameworks, including environmental and energy management, information security and business continuity. Approximately one third of Acronis data centers explicitly report the use of renewable electricity. Nearly half of the portfolio is supplied through public grid electricity; in these cases, renewable energy coverage is typically supported through energy attribution certificates or other procurement approaches, depending on the provider and region. We consolidate certification and energy-source information to support vendor selection, monitoring and continuous improvement.

Forward focus

Priority areas for further work include consolidating workloads into more energy-efficient facilities, prioritizing partners with renewable energy coverage and certified environmental and energy management systems, and strengthening responsible hardware lifecycle practices, including reuse and certified disposal. Major infrastructure transitions follow structured governance and change-management practices to support employee safety, operational resilience, regulatory alignment and consistent customer service as sustainability requirements evolve.



Pillar	Certification	Share of DCs
Environmental and energy certifications	ISO 14001 – Environmental management	**55%**
	ISO 50001 – Energy management	**40%**
	ISO 45001 – Health and safety	**15%**
	Green building labels (BREEAM, similar)	**<10%**
Governance, risk and security	ISO 27001 – Information security	**90%**
	ISO 27701 – Privacy	**25%**
	ISO 27017 / 27018 – Cloud and PII	**20%**
	Local cybersecurity frameworks (NIST, ENS, Cyber Essentials, etc.)	**15%**
Business continuity and operational resilience	ISO 22301 – Business continuity	**45%**
	ISO 20000 – IT service management	**30%**
	ISO 9001 – Quality management	**50%**
	Uptime / TIA Tier III–IV	**20%**

Renewable energy usage

Energy source category	Clarification	Share of DCs
Grid electricity (unspecified mix)	May include renewables, but not attributable	**45%**
Confirmed renewable energy	Explicitly stated renewable sourcing	**34%**
Unspecified / mixed	Insufficient clarity for ESG attribution	**19%**
Explicitly non-renewable	Clear non-renewable sourcing	**2%**

Social

Our people
Diversity initiatives
Training and development
Health and well-being
Employee engagement
Employee communications
Employee satisfaction
Communities
Acronis Academy for partners

Our people

Our success as a cyber protection company depends on a skilled, motivated and diverse workforce that can outthink evolving threats and support our partners around the world. As highlighted in our double materiality assessment, topics such as corporate culture, talent attraction and retention, and diversity, equity and inclusion are among Acronis' most material ESG factors — both in terms of financial performance and societal impact.

In 2025, we focused on three people priorities: Building a diverse leadership pipeline, strengthening continuous learning and career development and protecting employee well-being in a high-intensity cybersecurity environment. The following section summarizes how we manage these topics and the progress we've made against our metrics.

People metric	2024	2025
Voluntary attrition rate (%)	8.49%	7.51%
Percentage of women (overall workforce)	29.8%	28.7%
Percentage of women in extended management team	30.2%	29.3%
Percentage of women in C-suite	16.7%	18.2%
Number of participants in WIT Mentorship Program	36	41
Number of regions in #CyberWomen initiative	10	10
Number of participants in diversity events	879	712

2025 people highlights

1,800+
employees across 67 countries

8.49% to 7.51%
voluntary attrition reduced

16.7% to 18.2%
increase of women in the C-suite

Acronis team.

Diversity initiatives

We aim to build teams where different backgrounds, identities and perspectives can succeed. Our diversity approach combines internal programs, such as employee resource groups and targeted development, with external research into barriers facing underrepresented groups in tech.

Internal initiatives

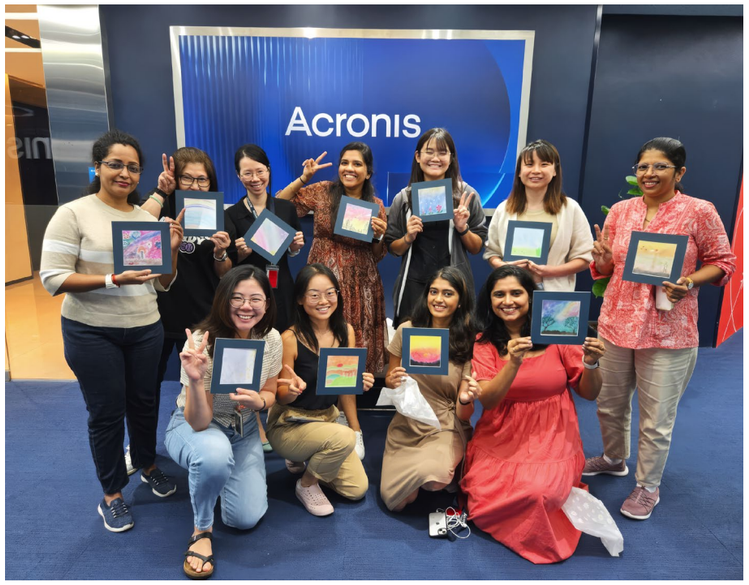
#CyberWomen and #CyberPride initiatives provide peer networks, mentoring and awareness activities focused on gender equity and LGBTQ+ inclusion. In 2025, our employees hosted over 30 internal events across 10 regions as part of our #CyberWomen initiative: Japan, Bulgaria, Romania, India, the United States (Burlington, Tempe), Italy, Singapore, Serbia and Switzerland, including panel discussions and learning sessions.

We continued the Women in Tech (WIT) Mentorship Program, which supports women at Acronis through one-to-one mentoring with senior leaders. In 2024, 38 women participated in the program; in 2025, the program expanded to 41 mentees (both women and men) with a focus on building leadership capabilities and cross-functional networks. It also includes Women-in-Tech community gatherings across the world to empower women in the IT sector within Acronis partner ecosystem.

FOMO at work: Research on opportunity gaps in tech

Beyond internal programs, Acronis runs external research to better understand how opportunity gaps show up in the technology workforce.

In 2025, we published new research in our report, "FOMO at work: The opportunity gap between men and women in tech," based on a survey of more than 650 IT professionals across eight countries: the United States, United Kingdom, Switzerland, Germany, Spain, Italy, Singapore and Japan. The sample reflected the global tech workforce, with about 29% women and 71% men.



#CyberWomen meetup in Singapore.

The findings point to a persistent perception gap. Only 60% of women, compared with 75% of men, believe that men and women have equal access to career development and growth, and 63% of women said work–life balance challenges significantly impact women's career progression in tech, while only 49% of men saw it that way. In parallel, 52% of women — versus 42% of men — were very or extremely concerned about missing career opportunities because of family responsibilities.

Women are also clear about what needs to change. A large majority — 82% of women — said that having more women in leadership would improve workplace culture, and 70% prioritized leadership development programs tailored to women, underlining the importance of visible and supported pathways into leadership roles.

We use insights from this research, together with internal feedback, to shape Acronis' diversity priorities, including expansion of women's leadership programs.

#CyberWomen breakfast meetup in Spain.

In 2025, we delivered 85+ structured training sessions across the organization

LinkedIn Learning

In 2025, we broadened our learning offer by rolling out LinkedIn Learning to all Acronis employees. By offering personalized learning paths in multiple languages, providing access to more than 64,000 expert-led courses, and continually updating content in line with emerging industry trends, we are equipping our global workforce with the skills needed to innovate responsibly and sustainably. By the end of 2025, 70% of employees accessed the platform. The most-studied topics are largely AI related (eight of the top ten), alongside cybersecurity and interpersonal communication. Moving more learning to digital formats can reduce travel-intensive training and support skills for responsible AI use, secure digital workplaces and long-term employability.

Acronis Academy for employees

Acronis supports continuous learning and professional development for employees through the Acronis Academy. The internal learning platform offers a wide range of educational tracks, providing employees with access to 93 courses or programs across technical, sales, marketing, compliance and other functional development areas. In 2025, our employees collectively completed more than 9,000 courses, and recorded 77,000 total learning hours, with an average of 385 hours per employee enrolled in the courses at Acronis Academy.

Beyond consuming content, employees are also encouraged to contribute as subject-matter experts by creating and publishing their own courses, ensuring that organizational knowledge is captured, shared and continuously expanded. This collaborative learning ecosystem empowers teams to grow their expertise while supporting the company's innovation and business goals.

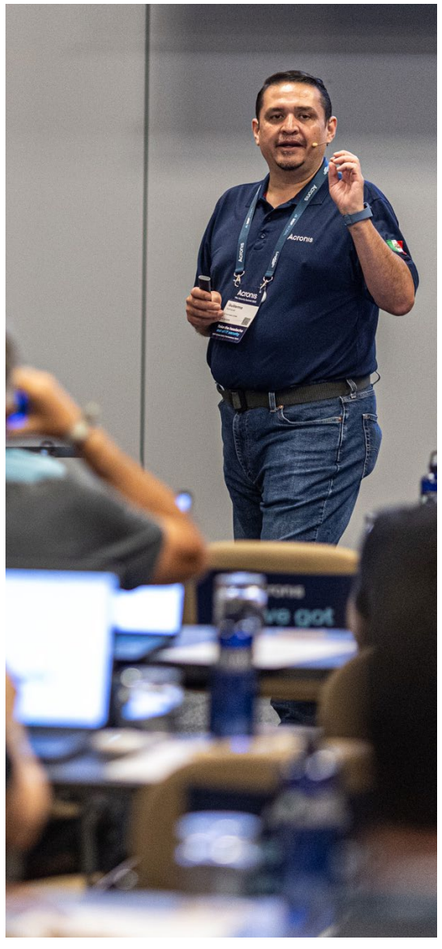
CXL learning

For specialized commercial skills, our marketing team used the CXL platform to deepen expertise in areas such as digital marketing, experimentation and conversion optimization. In 2025, 18 employees registered on the CXL platform and enrolled in a total of 96 courses, of which 50 were completed in full.

Training and development

Continuous learning is critical in cybersecurity, where technologies and threats evolve quickly. Acronis invests in technical skills, leadership capabilities and soft skills through a mix of structured programs and self-directed learning.

In 2025, we delivered 85+ structured training sessions across the organization, including 40 global training workshops, 21 department-specific trainings sessions, and 25+ HR-driven external tutorials. This training rollout was complemented by the launch of LinkedIn Learning, expanding access to on-demand development resources for employees globally. In addition, we delivered a mix of hard- and soft-skills workshops in areas such as AI, diversity and public speaking, and launched ESG training for the first time in 2025. We plan to run this training biennially starting next year to educate employees on sustainability topics and Acronis' initiatives.



Acronis Academy training.

Health and well-being

We recognize that cybersecurity is a high-intensity industry, and long-term performance depends on employees' physical and mental health.

Employees during Acronis Day.

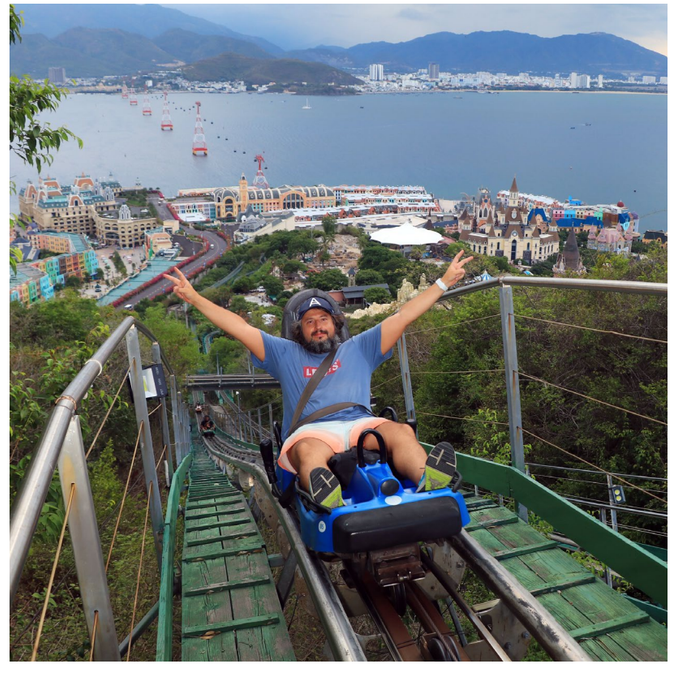
In 2025, our well-being approach included:

- **Acronis Days:** Company-wide days off during which most employees refrain from email, meetings or calls, creating space to rest and reset. In 2025, we maintained three such days.
- **Regional summer and winter #TeamUp events:** Annual company team-building events that combine strategy updates, cross-team workshops and social activities, helping employees connect across functions and geographies. In 2025, we hosted 44 summer and winter #TeamUps bringing 1,000+ employees together.
- **Global Kids Days:** Office-based events where employees invite their children for a day at the workplace, combining basic cyber safety and STEM activities with a simple introduction to IT professions. In 2025, Kids Days involved 217 children across 10 regions, supported by 62 Acronis volunteers.
- **Global mental health panel and sports and wellness challenges:** In 2025, Acronis ran two global challenges to encourage healthy routines and support connection across locations: One focused on physical activity and one on well-being activities. The physical activity challenge had 309 active participants (85.1% engagement), and the well-being challenge had 342 active participants (69.7% engagement). Employees logged over 40,000 miles in each challenge and over two million workout minutes per challenge.
- **Regional events:** Local office initiatives such as wellness sessions, sports and fitness activities, virtual coffee chats, first aid workshops and mental health awareness campaigns.

Employee Assistance Program (EAP)

A global EAP offering confidential counselling and support for employees and eligible family members, with utilization of 7.4% of employees during the year.

Well-being metric	2024	2025
Number of Acronis Days	3	3
EAP utilization rate (% of employees)	27.4%	7.4%
Summer / Winter #TeamUps held	24	44



Employee celebrating Acronis Day.

Employee engagement

Employee engagement is strengthened by opportunities to contribute beyond core roles. The Acronis Cyber Foundation Ambassadors Program serves as the primary mechanism for organizing and scaling employee-driven community initiatives, enabling employees to design and lead projects such as digital skills training, environmental cleanups, Kids Days and local community collaborations. In 2025, approximately 600 employees delivered 129+ community projects through the program.

Acronis Kids Day.

Holiday Campaign

Our global Holiday Campaign coordinated year-end support for local communities, with nine regions organizing local volunteering actions, personally purchasing and delivering holiday gifts and much-needed items to families in need.

Acronis Australia team purchasing goods for the holiday campaign.

600+
employees engaged
(32.6% of total workforce)

129
projects completed

2,378
volunteer hours contributed

Acronis Japan volunteers at a food bank supporting families in need.

Acronis Boston team supporting families in need during Thanksgiving.

Employee communications

The CEO and leadership team regularly communicate company strategy through global town halls, regional Q&A sessions, newsletters, a corporate Microsoft Teams channel and informal meet-ups. In 2025, the company shifted from a single global town hall to two sessions per cycle to better accommodate all time zones. As a result, eight global town halls were held, with an average attendance of 70% of Acronis employees, alongside 13 regional online and offline Q&A sessions.

Employees can raise questions or feedback using open Q&A and regional meetings. All questions are reviewed and addressed, either directly during sessions or through follow-up communications.

Transparent, two-way communication is central to how we manage change and involve employees in decisions.

Acronis CEO Jan-Jaap Jager.

Voice of Employees

The “Voice of Employees” (VoE) Program provides a structured way for employees to submit ideas and feedback on workplace improvements and culture. It was launched in 2024 with 72 people joining the working group and expanded to 84 people in 2025. In 2025, 60 ideas were submitted by employees, of which 30 were implemented or integrated into ongoing initiatives. A pulse check of 151 employees on VoE activities showed broadly positive sentiment, with 69.5% describing the program positively, and in-person events and opportunities to connect were consistently rated as the most valued format of interaction. The feedback is being used to refine the program and shape the next cycle of employee-led initiatives.

Employee satisfaction

We measure employee satisfaction and engagement through an annual survey that includes an Employee Net Promoter Score (eNPS) and thematic questions on leadership, development, well-being and inclusion.

Engagement metric	2023-2024*	2025
Overall eNPS score	-1	16
Survey participation rate	60.4%	73.5%
Percentage of employees participating in community / CSR activities	27.7%	32.6%

* The 2023 survey was postponed until February 2024; the score is shown as 2023–2024 to reflect this transition year.

In 2025:

- Our overall eNPS was 16, compared with -1 in 2023-2024.
- Survey participation reached 73.5% of eligible employees.
- Scores were strongest in company culture, work-life balance and the management team, and highlighted improvement needs in compensation and career growth.

The negative eNPS in the 2023–2024 cycle reflected the impact of a significant restructuring and associated uncertainty. The 2025 score of 16 shows the first phase of recovery, returning to positive territory, and broadly back to early-journey levels while we continue working on workload, communication and career development themes.

To improve engagement, we focused on four main levers: Strengthening communication and visibility through regular town halls; recognition of top-performing employees within the “Cyber Dragon” Program; amplifying employee voice via “Voice of the Employee” events and anonymous feedback channels with structured follow-up; and expanding learning, connection and benefits through a global learning platform, mentorship, virtual coffee chats with leadership and more competitive benefits, including meal allowances, paid time off and leave policies, health coverage and easier access to equipment and company merchandise.

In 2026, HR aims to conduct an annual pay gap analysis to further strengthen transparency and inform ongoing actions.

Acronis “Cyber Dragon” award for outstanding performance.

Communities

Acronis Cyber Foundation Program

The Acronis Cyber Foundation Program is our corporate social responsibility project focused on education, digital inclusion and cyber safety, and environmental action. The program is implemented with local NGO partners and supported by employee and partner volunteering in the communities where we operate and beyond.

Official opening ceremony of the Resource Center at Friends Secondary School Kibisi in Namboko, Kenya.

Schools and computer classrooms

In 2025, we advanced access to education through three new school and computer classroom projects reaching 1,289 children. These projects provide stable access to learning, connectivity and basic digital skills in rural communities in Argentina, Kenya and Niger.

Cyber safety workshop in Bulgaria.

IT Skills Program and cyber safety workshops

Our IT Skills Program continues to bridge the digital divide by providing essential digital skills to migrants, ex-offenders, seniors and young people. In 2025, working with partners in Bulgaria, Germany, Romania, Singapore and Switzerland, we delivered eight training programs for 550+ learners, helping them build confidence in basic computer use, productivity tools and introductory cybersecurity.

In parallel, our cyber safety initiative focused on seniors, children and young people in schools and community organizations. Over the year, 63 Acronis employees ran 40 workshops, teaching 2,100 participants how to recognize online risks, protect their data and behave responsibly in the digital environment.

Acronis team in Italy deliverying a cyber safety workshop.

Graduates with migratory backgrounds at the IT Skills Program in Switzerland..

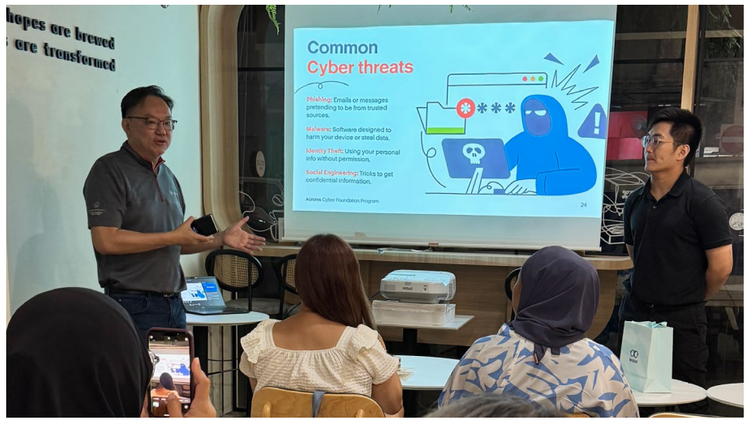
Mentorship for aspiring software and AI engineers

Through the Groundbreaker Talents Program, we support young women from financially constrained backgrounds in Uganda with scholarships and software and AI engineering training. In 2025, Acronis funded scholarships for three students and provided one-to-one mentoring to 15 participants by Acronis employees, helping them navigate their studies, explore tech careers and build confidence for further education and employment.

Partner engagement

Partners are central to scaling the reach of the Acronis Cyber Foundation Program. Many managed service providers and distributors are keen to invest in their local communities but have limited capacity to design and manage initiatives. Our partner engagement models are designed to address this gap, increasing the scope of our joint action and supporting partners in structuring their own community programs.

"CSR in a Box" is a turnkey framework that provides partners with ready-to-use cyber safety curricula, trainer guides, communication materials and advisory support from Acronis. This enables them to deliver consistent, high-quality educational activities for local schools and youth organizations, aligned with both their CSR priorities and our cyber protection expertise. In 2025, four 'CSR-in-a-Box' projects were implemented by partners to run cyber safety classes in their own communities in Japan and Singapore.



Alex Chan, Founder, Confinity, teaching a cyber safety workshop to females in Singapore.

#TeamUp Program creates co-designed community initiatives where Acronis and partners jointly define the focus, share resources and mobilize volunteers. In 2025, 29 partners supported our school building projects, two partners in India and Japan joined community cleanup initiatives, and a further two partners from the U.S. and Canada participated in #TeamUp projects. Together, these collaborations extended the impact of our education and community work while strengthening partners' ability to contribute to local social and environmental priorities.

3
school projects
(benefitting 1,289 children)

8
global IT skills programs
(550+ learners)

40
cyber safety workshops
(2,100 participants)

33
partners engaged

Carl Hagström, CEO of Gridheart, and Lena Gabdullina, Corporate Communications EMEA and Foundation Lead at Acronis, at the opening ceremony of the Resource Center at Friends Secondary School Kibisi in Namboko, Kenya.

Communities

"This resource center was built to address a simple but persistent gap: Talent exists everywhere, while access does not. In many communities across the Global South, educational potential is limited not by ambition, but by infrastructure. Through strong partnerships, we can pool resources and invest thoughtfully in facilities that strengthen local education systems. Visiting the school and meeting the students — their optimism despite having so little — left a lasting impression on me and reinforced why this work truly matters."

Carl Hagström, CEO of Gridheart (Sweden-based distributor)

Partner community

Partner communities are one of the ways Acronis integrates stakeholder input into its work. In 2025, we strengthened this approach by launching the Acronis Partner Ambassadors Program as part of our broader global partner community of more than 21,000 partners. The program brings together 40 MSP ambassadors from 20 countries who represent partner perspectives, co-create with us on product experience, go-to-market initiatives and thought leadership, and help amplify these messages across the wider community through the voice of partners. Throughout the year, the ambassadors supported 10+ industry events and webinars and engaged in 10 focused feedback groups, while our Partner Advisory Council (PAC) community grew to 200+ members and convened 28 online and in-person PAC meetings. Together, these activities strengthened our ability to test ideas earlier, improve solutions in line with real-world needs and build a more resilient partner ecosystem.

Key 2025 highlights:

40
ambassadors from 20 countries

10+
events and webinars

10
focus groups

200+
members of PAC

28
offline and online PAC meetings

Partner Advisory Council meeting in Spain.

Acronis partner ambassadors gathered in Spain during Acronis TRU Security Summit.

Partner community

As part of our ESG efforts, Acronis Academy provides free, structured education and skills development for partners and aspiring MSPs. By equipping learners with cybersecurity and business competencies, the Academy expands access to quality digital jobs and supports more resilient communities.

In 2025, the Academy trained more than 4,000 employees of Acronis partners every quarter, issuing, on average, three to four certifications per learner. Learners came from 162 countries and accessed content in seven languages, making the program truly global and inclusive. Over 2025, partner employees doubled the average number of certifications per person compared with the previous year, increasing from around two to more than four certifications annually. Internal data also indicates that partners whose employees complete Acronis Academy certifications achieve up to 60% higher revenue than partners who do not get regularly trained and certified by the Acronis Academy.

Key 2025 highlights:

4,000+
partner employees trained per quarter in 2025

3
certifications issued per learner on average in 2025 (x2 vs. 2024)

162
countries

7
languages

60%
revenue increase

40%
reduced support incidents

MSP Academy training for partners.

MSP Academy is a dedicated track within Acronis Academy designed for a broader, external audience. It's open to anyone interested in the MSP business, whether or not they are already an Acronis partner. Through short, vendor-neutral video courses, MSP Academy gives students, career changers and prospective MSPs a low-barrier means to explore how an MSP business works, develop relevant cybersecurity and business skills and assess whether they want to enter the field.

The Academy delivers learning in multiple formats, including on-demand courses, live webinars, and in-person sessions. Training focuses on two main areas: technical skills, including security-focused certifications, and sales and business enablement, helping learners develop practical, market-relevant expertise. Learners can earn digital badges and certifications that contribute to Acronis Partner Program requirements and formal recognition.

New courses are launched regularly to address evolving partner and market needs, and the platform encourages learners to combine technical, business and soft-skills training to build well-rounded expertise. By providing accessible, flexible and free learning opportunities and recognizing achievements through certifications and badges, Acronis Academy strengthens the capabilities of partners, future partners and cybersecurity enthusiasts, while contributing to a more secure and inclusive digital ecosystem worldwide.

Acronis partners attending the MSP Global event.

Governance

Corporate governance

In May 2025, Acronis entered a new ownership phase following EQT's acquisition of a majority stake, supporting a continued focus on governance maturity and long-term value creation.

Acronis is managed under the direction of the board of directors, which supervises the company's operations and provides oversight of compliance with applicable laws, policies and strategic objectives. At year-end 2025, the board consisted of seven seats and was chaired by Warren Adelman (Chairman of the Board). Our board structure and directors are determined by the shareholders entitled to elect directors under the Articles of Association and Swiss law. Directors are elected to staggered three-year terms, with elections held annually at shareholder meetings.

The board sets expectations for governance by defining responsibilities, delegations and internal standards, and by reviewing key risks together with management. The board is supported by an audit committee, which meets regularly and reports to the board. The audit committee supports the board's review of financial reporting, audit matters and compliance, including the independence and performance of the company's auditors and significant financial reporting topics. It also supports the board's review and oversight of the company's information security and technical risks, including data center security.

ESG governance

Our environmental and sustainability efforts are directed by our internal ESG committee. The committee is made up of cross-functional representatives from human resources, data center operations, office management, government relations, legal, finance, security, marketing and communications, and is chaired by Alona Geckler, SVP Business Operations and Chief of Staff, with the full support of our CEO. ESG results and commitments are reviewed by the board and the Acronis leadership team on an annual basis. To strengthen board-level oversight, Stefan Gaiser (board member) has been appointed as the Acronis Board Sustainability Champion.

Through regular meetings, the ESG committee reviews priorities and project proposals, assesses impacts on the environment, employees and other stakeholders, and assigns clear ownership to manage risks and drive progress.

Since May 2025, we have also strengthened our ESG governance through regular collaboration with EQT's sustainability team. This includes ongoing alignment on ESG priorities, data and reporting expectations and continuous improvement of our governance processes to ensure consistency and transparency across key ESG topics.

Corporate culture

As identified in our double materiality assessment, corporate culture is a material governance topic for Acronis because it shapes how we make decisions, manage risk and build trust with customers, partners and employees. Our corporate values — never give up, pride, ownership and care — set clear expectations for day-to-day behavior and accountability. We reinforce these values through leadership communication, mandatory training, internal standards (including information security, data protection and privacy and expected conduct), and formal channels for employees to ask questions or raise concerns, supported by a nonretaliation policy. We also use employee listening mechanisms (e.g., the Voice of Employees Program) to track culture and inform improvement actions, while related people and community programs are covered in the relevant sections of this report.

Corporate culture is also strengthened through summer and winter #TeamUps and off-sites that boost engagement and collaboration.

Acronis Bulgaria team gathered for a winter #TeamUp event.

Stakeholder engagement approach

Acronis engages stakeholders to understand expectations, improve our products and services and inform priorities for managing sustainability-related impacts and risks and opportunities, including inputs to our materiality process.

In 2025, our engagement approach combined ongoing channels and periodic touchpoints across key groups:

- **Employees:** Surveys, town halls, feedback channels, newsletters, direct manager-employee communications, team and all-hands calls, internal email communication, Microsoft Teams and SharePoint.
- **Partners:** Partner events, briefings, enablement and support channels.
- **Customers:** Customer support and service feedback loops.
- **Suppliers:** Procurement onboarding and supplier communications.
- **Communities:** Acronis Cyber Foundation Program and volunteer initiatives.
- **Investors / owners:** Regular meetings, updates and ESG data submissions.

Feedback from these channels is captured and reviewed by accountable teams and is used for shaping priorities, program design and reporting, with related details covered in the Our people, Acronis Cyber Foundation Program, and Supplier management sections.

Compliance and security

“Security-related impact to communities” and “customer privacy” are material topics for Acronis as a result of our double materiality assessment. We protect our customers’ data and help organizations worldwide achieve strong security and privacy standards using our software. Our solutions support compliance with regulations and help defend communities, data and infrastructure against cyberthreats.

Acronis protects customer data through encryption, both at rest and in transit. Backup data stored in Acronis-hosted storage is encrypted at rest using the AES-256 algorithm and additionally can be protected with a customer-defined encryption password. Data transfers between customer environments and the Acronis Cloud are protected using industry-standard transport encryption (TLS 1.2 or higher). Metadata and management communications with the Acronis Cloud are also protected in transit. We maintain and monitor the use of strong, reliable cipher suites for secure connections.

Our products are designed with security in mind from the very beginning. We use a Secure Software Development Life Cycle (S-SDLC), which means security is included in every step of product development. We also encourage a company culture focused on security. To further strengthen our defenses, Acronis runs a bug bounty program and holds semi-annual penetration tests of our cloud data centers, carried out by independent security experts.

Training	Target audience	Completion rate
General information security training	All employees	94%
Application security in Acronis: Processes, policies and secure development	Software developers and product managers	95%
Health information privacy acts and standards training 2025	Support, DCO and professional services	99%

Acronis ensures that all employees participate in a range of security training sessions designed to keep the workforce informed and prepared for evolving security challenges. General security training is regularly updated to reflect the latest industry standards, while new, topic-specific training is developed and distributed as needed. The company is committed to achieving high completion rates for these courses, demonstrating its dedication to a strong security culture.

Acronis is a CVE Numbering Authority (CNA) as part of the CVE® Program. This means we are responsible for publishing any cybersecurity vulnerabilities found in our products as CVE records. Our Acronis Security Advisory Database lists all fixed vulnerabilities and important updates, so customers can easily check the status of their products and services.

Security incidents are an inevitable part of any organization’s operations, and Acronis is committed to monitoring, managing and learning from these events to strengthen its security practices. In 2025, a total of 31 security incidents were identified and classified according to their severity:

1 high
incident

6 medium
incidents

24 low
incidents

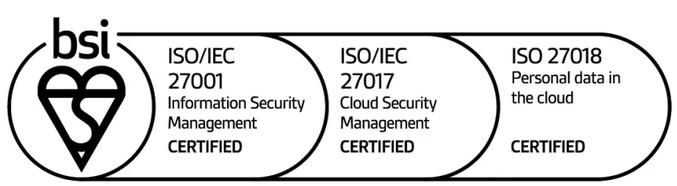
Importantly, there were no incidents reported that involved the compromise of Acronis’ production environment.

Compliance and security

Acronis holds many certifications and is regularly audited by third-party experts to confirm our security and compliance. Our certifications include:

- ISO/IEC 27001:2022 – Information Security Management System
- ISO/IEC 27017:2015 – Information security controls for cloud services
- ISO/IEC 27018:2019 – Protection of personally identifiable information
- ISO 9001 – Quality Management System
- IEC 62443-4-1 – Secure Product Development Lifecycle (SSDLC)
- SOC 2 Type 2 compliance for the Acronis Cyber Cloud platform
- Payment Card Industry Data Security Standards (PCI DSS)
- CSA STAR Level 2
- And many others

To learn more about our compliance, certifications and security practices, please visit the Acronis Trust Center.



Acronis Threat Research Unit (TRU)

Acronis Threat Research Unit

The Acronis Threat Research Unit (TRU) is Acronis' dedicated, in-house cyberthreat research organization. It is composed of approximately 25 highly skilled cybersecurity professionals distributed globally, including malware analysts, threat intelligence specialists, data scientists and AI-focused researchers. The team's core mission is intelligence-driven cyberthreat analysis, supporting Acronis products, customers and the broader cybersecurity community.

TRU conducts deep research into emerging and active threats, such as malware, ransomware, phishing and advanced persistent threats (APTs), and produces insightful reports plus strategic and technical guidance to help IT teams and the general cybersecurity community build stronger security frameworks.

TRU also plays a significant role in Acronis' detection ecosystem: In 2025 alone, Acronis EDR recorded more than 30 million detected and prevented incidents on customer endpoints, a figure influenced by TRU's threat intelligence contributions.

Additionally, TRU experts actively engage with customers, partners and the public through industry events. In 2025, Acronis organized 25 TRU Security Day events globally. These were attended by 5,100+ Acronis partners, demonstrating the team's commitment to cybersecurity education, outreach and community collaboration.

TRU's research and reports are grounded in telemetry collected across Acronis' global footprint. Depending on the publication cycle, threat analyses use signals from over 1,000,000 unique endpoints worldwide, enabling TRU to measure trends in malware prevalence, ransomware targeting and email-based attacks with statistically meaningful precision.

Publicly released outputs include large report deep dives, including the Acronis Cyberthreats Reports, with summaries of major global threat trends with quantified data for each reporting period (e.g., H1 2025, H2 2024).

Plus, there is additional research content on the dedicated TRU website, including:

- Regular cyberthreat updates, including monthly digests and weekly monitoring notes for MSPs and enterprises.
- Technical deep-dive investigations documenting active campaigns, new malware families, exploitation methods and threat actor infrastructure.

In 2025, Acronis organized 25 TRU Security Day events globally.

These documents are fully accessible, citable and based on reproducible telemetry-driven analysis.

Collectively, TRU's findings guide Acronis product tuning, support detection engineering and inform customers of evolving risks. By combining global telemetry with technical investigation, TRU provides both macro-level visibility into threat trends and actionable insights that enhance cybersecurity resilience.

Customer privacy and data protection

Acronis responsibly handles all customer data, product usage data and customer content. The Acronis Customer Privacy Statement describes how Acronis handles and protects personal information and the choices customers have about their personal information. It gives a comprehensive overview on what kind of information Acronis processes, data collection technologies, legal basis for processing personal information, and ways customers can exercise their privacy rights and choices about their data.

Acronis incorporates privacy protections directly into the architecture of its products and services.

This includes implementing features that support GDPR-compliant data processing and embedding privacy protections into product design. Beyond the EU, we monitor and assess additional privacy and data protection requirements globally and align relevant processes accordingly, including frameworks such as Singapore's Personal Data Protection Act (PDPA), Switzerland's Federal Act on Data Protection (FADP) and, where applicable, U.S. state privacy laws, including the California Consumer Privacy Act and other applicable data protection regulations worldwide. The Company regularly reviews and updates its internal procedures to remain aligned with evolving data protection guidelines, maintaining the security and confidentiality of customer information.

In 2025, Acronis launched Compliance Navigator, a new interactive web tool that helps MSPs and end clients understand which compliance requirements apply to them, and how Acronis solutions map to support those needs. Compliance Navigator simplifies complex regulations like NIS 2, DORA, HIPAA and others by translating them into clear, actionable requirements. It also provides a practical security best practices guide that supports both MSPs and their clients throughout the compliance journey. Each requirement is directly mapped to Acronis capabilities across data protection, cybersecurity, endpoint management, and more. This way Acronis helps its customers to navigate the developing cybersecurity standards, increasing resilience of communities to cyberthreats and protecting end-users' data.

Corruption and anti-bribery

Acronis sets expectations for ethical conduct through global policies, training and compliance oversight. We take a zero-tolerance approach to bribery and corruption. Our commitments, expectations and requirements are set out in the Acronis AG Global Anti-Corruption Policy and apply across the organization.

Anti-corruption and anti-bribery training is mandatory for all new hires as part of onboarding. Local HR teams are responsible for ensuring new hires reach 100% completion within their first two weeks of employment.

Reported concerns are reviewed and addressed through established internal processes, with appropriate actions taken based on findings.

Responsible use of artificial intelligence (AI)

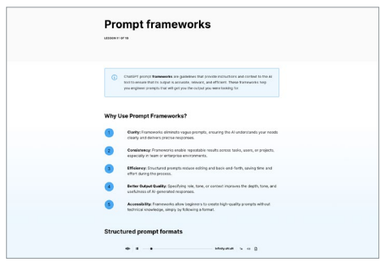
AI is a rapidly evolving topic for Acronis and, as identified in our double materiality assessment, responsible use of AI (including privacy and AI governance) is a material governance topic due to its relevance to data protection, information security, compliance and customer trust. We use AI in our products and internal tools to support productivity, efficiency and innovation, while recognizing that wider adoption of AI can introduce new risks and responsibilities, particularly related to data security, privacy and ethical use.

To manage these risks, we develop and deploy AI capabilities with security, privacy and ethical considerations integrated into design and operational practices. Our internal AI tools include controls intended to reduce the risk of unauthorized disclosure of sensitive or confidential information and to manage how data is processed when AI solutions are used.

Acronis maintains an AI Usage Policy that sets guidelines for responsible and ethical AI use across the organization.

The policy applies to AI developed in house and to third-party AI solutions, and is intended to support alignment with applicable regulations and internal standards. We assign an accountable owner for each AI system to oversee its use and adherence to company requirements. Employees are not permitted to enter confidential or sensitive information into AI systems unless the AI system has undergone rigorous testing and adequate organizational and technical controls are in place to protect the data. Customers can also find a dedicated section on AI usage terms and conditions in the Acronis Software License Agreement (EULA).

Education and awareness are important parts of our approach. Ethical and safe AI use is included in our annual mandatory security training for employees. We also provide voluntary learning opportunities on AI, including internally developed webinars, third-party training workshops and access to AI-related courses through LinkedIn Learning. In 2025, AI-related courses were among the most accessed learning resources on the platform by Acronis employees.



Acronis AI Fundamentals training.

Through these measures, Acronis ensures that AI is a force for good, driving productivity while upholding the highest standards of security, ethics and compliance. Our approach to AI ethics and governance reflects our broader dedication to responsible innovation and the protection of our customers, employees and the wider community.

Supplier management

Acronis aims to maintain a responsible and ethical value chain that reflects our corporate values and supports sustainable business practices. In recent years, we have been strengthening our supplier qualification and review processes to support responsible purchasing and reduce risk exposure. As part of this approach, we use a supplier questionnaire as a standard element of vendor qualification and require new vendors to complete it before contracting. We also use third-party vendor vetting to assess open-source and commercial software suppliers for security and other supply chain risks.

In 2025, we continued this work while strengthening our procurement foundation through the implementation of Coupa, a procure-to-pay system designed to improve process efficiency, transparency and scalability. The platform also provides a stronger basis for future supplier data collection and analysis, including a more structured way to capture and review sustainability-related information as expectations evolve. To support adoption and internal alignment, employees participated in internal webinars covering the objectives of the new system and the role procurement plays in responsible value chain practices. In 2026, we plan to implement Coupa Analytics, which will strengthen our ability to generate consistent vendor reporting and improve visibility into supplier data over time.

Human rights and modern-day slavery

In our supply chain, we unequivocally reject any involvement in human trafficking. We are committed to avoiding the use of child or forced labor, and we are vigilant about partnering only with entities that uphold similar ethical standards. To enforce this commitment, we use an extended supplier questionnaire, ensuring that our partners align with our values and adhere to our standards.

Key ESG metrics

Category	Metric	Unit	2024 (base year)	2025
Environmental	Scope 1	tCO2e	**78.81**	**1266.76**
	Scope 2 (location based)	tCO2e	**868.85**	**730.71**
	Scope 3	tCO2e	**178,805.49**	**105,527.38**
	Total GHG emissions (location based)	tCO2e	**179,753.16**	**107,524.85**
	Electricity	MWh	**2,332**	**1,500**
	Renewable electricity	%	**0%**	**70%**
Social	Percentage of women (overall)	%	**29.9**	**28.7**
	Percentage of women in leadership	%	**16.7**	**18.2**
	Percentage of women in extended management team	%	**30.2**	**29.3**
	Voluntary attrition	%	**8.49**	**7.51**
	Employee satisfaction	eNPS	**-1***	**16**
	Community engagement	#	**500**	**600**
	Employees volunteering	hours	**2,970**	**2,378**
	Average training hours per employee	hours	**30**	**30**
Governance	Board gender diversity	% gender split	**82 / 18**	**100 / 0**
	Code of conduct training completion	%	**100**	**100**
	Data protection training completion	%	**97**	**94**

*The metric refers to 2023-2024 base year combined. See more in the “Employee satisfaction” section.

Year-over-year trends

Total greenhouse gas (GHG) emissions decreased by 40% in 2025 compared to 2024, primarily driven by a reduction in Scope 3 emissions, especially from the use of sold products. Scope 2 emissions declined due to lower electricity consumption and 70% renewable electricity matching, while Scope 1 increased, mainly due to improved estimation methodology. Overall, the year-on-year change reflects both operational shifts and strengthened data quality.

2025 showed progress across our operational footprint and people outcomes. Electricity use decreased materially due to office footprint optimization and hybrid utilization, while renewable electricity coverage increased through renewable attribute procurement. Headcount grew while attrition improved and eNPS rose significantly; representation of women in the C-suite increased year on year; community participation expanded through more scalable formats; and compliance training remained strong, with targeted actions identified to close minor gaps.

Alignment with the U.N. Sustainable Development Goals (UN SDGs)

Our ESG priorities and community programs are linked to the U.N. Sustainable Development Goals (SDGs) to help clarify where we contribute through our operations, products and philanthropy. We focus on the goals most closely connected to our material topics and where we can have a practical, measurable influence.

SDG 1: No poverty

We support remote communities by expanding access to basic education infrastructure through Acronis Cyber Foundation school and computer classroom projects. By helping children take the first steps in learning where local educational facilities are limited, these initiatives aim to strengthen long-term opportunities and contribute to pathways out of poverty.

SDG 3: Good health and well-being

We support employee well-being by promoting healthy routines and mental resilience in a high-intensity cybersecurity environment. Our approach includes company-wide rest days, global wellness initiatives that encourage physical activity and connection across locations, access to confidential counselling through an Employee Assistance Program, and locally delivered health and mental health awareness activities.

SDG 4: Quality education

We support skills development through structured learning for partners and customers (including Acronis Academy), and through community education delivered via the Acronis Cyber Foundation Program, such as IT skills training and cyber safety workshops. We've also expanded access to learning infrastructure through school and computer classroom projects in underserved communities.

SDG 5: Gender equality

We promote inclusion and equal opportunities through internal and external initiatives, including employee-led diversity communities (e.g., #CyberWomen) and women-focused mentorship and networking activities. In our community programs, we also support education pathways for young women through targeted initiatives delivered with local partners.

SDG 8: Decent work and economic growth

We invest in skills and professional development for both our ecosystem and our workforce. We deliver structured training and certification pathways through the Acronis Academy for partners and customers, and we provide ongoing learning opportunities for employees, including role-relevant development and mandatory training that reinforces secure and responsible ways of working. We operate workplaces globally, including in developing countries, providing fair compensation and sustainable economic opportunities for more than 1,800 employees across 67 countries.

Alignment with the U.N. Sustainable Development Goals (UN SDGs)

SDG 9: Industry, innovation and infrastructure

As a cyber protection company, we contribute to resilient digital infrastructure by helping organizations strengthen cybersecurity and privacy practices.

SDG 10: Reduced inequalities

We address digital inclusion by focusing community programs on groups that can face barriers to access — such as migrants, ex-offenders, seniors and young people — through IT skills training and cyber safety workshops delivered with local partners and employee volunteers. We also support underserved communities through school and computer classroom projects that expand access to learning and basic digital infrastructure.

SDG 13: Climate action

We address climate impacts by measuring our greenhouse gas emissions, improving emissions transparency, reducing electricity-related emissions through efficiency actions and increased renewable electricity coverage across our operations, planting trees and organizing environmental days.

SDG 16: Peace, justice and strong institutions

We are committed to conducting business with honesty and integrity as captured in our Code of Conduct, sanctions and export controls compliance policy, global anti-corruption policy and ongoing data protection and security training. We also promote responsible use of AI through our AI Use Policy and related governance to help manage risks linked to security, privacy and ethical use.

Appendix

Statement of use

Acronis has reported the information cited in its GRI content index for the period January 1, 2025 through December 31, 2025 (unless otherwise specified), with reference to the GRI Standards.

GRI Standard area	Disclosure	Location / Comments
GRI 2-1	Organizational details	Name of the organization: Acronis AG Location of headquarters: Rheinweg 9, 8200 Schaffhausen, Switzerland **Location of operations:** www.acronis.com/en/company/contacts
GRI 2-3	Reporting period, frequency and contact point	Reporting period: January 1, 2025–December 31, 2025 (unless stated otherwise) Reporting cycle: annual Publication date: March 9, 2026 Contact: esg@acronis.com
GRI 2-4	Restatements of information	After an external review, we revised 2024 Scope 3 Category 5 calculations and updated total Scope 3 emissions. All 2024 data reflects these changes (see Prior-year restatement, p. 18).
GRI 2-5	External assurance	Commissioned an external third party to perform GHG emissions assessment.
GRI 2-6	Activities, value chain and other business relationships	Security partnerships and memberships: www.acronis.com/trust-center; Sports partnerships: www.acronis.com/en-us/sports; plus, many other activities described throughout this report.
GRI 2-7	Employees	Page 8 About Acronis Page 38 Our people Pages 39 Diversity initiatives
GRI 2-9	Governance structure and composition	Pages 51 Corporate governance
GRI 2-10	Nomination and selection of the highest governance body	Pages 51 Corporate governance
GRI 2-11	Chair of the highest governance body	Warren Adelman, Chairman of the Board, appointed May 15, 2025
GRI 2-12	Role of the highest governance body in overseeing the management of impacts	Pages 51 Corporate governance
GRI 2-14	Role of the highest governance body in sustainability reporting	Pages 4 About this report Pages 51 ESG governance
GRI 2-17	Collective knowledge of the highest governance body	Acronis' internal business processes are geared to comprehensive and continuous improvement and innovation. This also entails the inclusion of stakeholders' concerns relating to economic, environmental and social topics. The board of directors and the Acronis leadership team receive feedback and input on these aspects from discussions with various stakeholder groups such as customers and investors. Acronis' governance bodies thus advance their collective knowledge about the sustainability aspects that are relevant to the company.

GRI Standard area	Disclosure	Location / Comments
GRI 2-19	Remuneration policies	Acronis does not publicly disclose this information.
GRI 2-20	Process to determine remuneration	Acronis does not publicly disclose this information.
GRI 2-21	Annual total compensation ratio	Acronis does not publicly disclose this information.
GRI 2-22	Statement on sustainable development strategy	Page 6 Message from our CEO Pages 16 Our commitment to ESG
GRI 2-23	Policy commitments	Pages 50 Governance
GRI 2-25	Processes to remediate negative impacts	Suspected instances of improper or unethical activity are examined and handled in accordance with the Code of Conduct and applicable laws.
GRI 2-26	Mechanisms for seeking advice and raising concerns	Sustainability and governance page www.acronis.com/en-us/sustainability-governance
GRI 2-28	Membership associations	Security partnerships and memberships: www.acronis.com/trust-center; Sports partnerships: www.acronis.com/en-us/sports
GRI 2-29	Approach to stakeholder engagement	Suspected instances of improper or unethical activity are examined and handled in accordance with the Code of Conduct and applicable laws. Page 11 Double materiality assessment Page 46 Partner engagement Page 43 Communicating with employees Page 53 Stakeholder engagement approach
GRI 2-30	Collective bargaining agreements	None of our employees are covered by collective bargaining agreements.

GRI 203 Indirect economic impacts 2016

GRI Standard area	Disclosure	Location / Comments
GRI 203-1	Infrastructure investments and services supported	Building schools and setting up computer classrooms in developing countries. Pages 45 Acronis Cyber Foundation Program

GRI 305 emissions 2016

GRI Standard area	Disclosure	Location / Comments
GRI 305-1	Direct (Scope 1) GHG emissions	Page 18 Greenhouse gas emissions
GRI 305-2	Energy indirect (Scope 2) GHG emissions	Page 18 Greenhouse gas emissions
GRI 305-3	GHG emissions intensity	Page 18 Greenhouse gas emissions

Appendix

GRI 403 Occupational health and safety 2018

GRI Standard area	Disclosure	Location / Comments
GRI 403-3	Occupational health services	All team members have access to the Employee Handbook, which includes information and procedures related to fulfilling employees' job requirements. Additionally, all employees have access to relevant training. Page 41 Health and well-being; EAP reference
GRI 403-4	Worker participation, consultation and communication on occupational health and safety	Acronis communicates environmental, health and safety programs to employees and encourages them to report any environmental, health or safety concerns.
GRI 403-5	Worker training on occupational health and safety	We hold regular webinars where we discuss occupational health and safety, mental health and other issues.
GRI 403-6	Promotion of worker health	Page 62 Health and well-being
GRI 403-7	Prevention and mitigation of occupational health and safety impacts directly linked by business relationships	We hold regular webinars where we discuss occupational health and safety, mental health and other issues.

GRI 404 Training and education 2016

GRI Standard area	Disclosure	Location / Comments
GRI 404-1	Average hours of training per year per employee	30 hours
GRI 404-2	Programs for upgrading employee skills and transition assistance programs	Page 40 Training and development
GRI 404-3	Percentage of employees receiving regular performance and career development reviews	Acronis conducts annual employee performance reviews for all full-time employees, providing them with an opportunity to set and discuss career development goals with their managers.

GRI 405 Diversity and equal opportunity 2016

GRI Standard area	Disclosure	Location / Comments
GRI 405-1	Diversity of governance bodies and employees	Pages 38 Our people Page 39 Diversity initiatives

About Acronis:

Acronis is a global cyber protection company that provides natively integrated cybersecurity, data protection, and endpoint management for managed service providers (MSPs), small and medium businesses (SMBs), and enterprise IT departments. Acronis solutions are highly efficient and designed to identify, prevent, detect, respond to, remediate, and recover from modern cyberthreats with minimal downtime, ensuring data integrity and business continuity. Acronis offers the most comprehensive security solution on the market for MSPs with its unique ability to meet the needs of diverse and distributed IT environments.

A Swiss company founded in Singapore in 2003, Acronis has 15 offices worldwide and employees in 50+ countries. Acronis Cyber Protect is available in 26 languages in 150 countries and is used by over 21,000 service providers to protect over 750,000 businesses. Learn more at acronis.com.

Acronis

Environmental, Social and Governance Report 2025

Learn more at acronis.com