Acronis

Ransomware in 2023:

Market Insights & Cross-NIST Protection with Acronis

Featuring ransomware trends for 2023 and why Acronis is a Gold Medalist in the 2022 SoftwareReviews Endpoint Protection Data Quadrant

INFO~TECH RESEARCH GROUP

SoftwareReviews

Table of Contents

Trends in Ransomware: An Ever-Evolving Threat

In 2022, over 30% of organizations worldwide experienced a ransomware attack, where employees were denied access to their files and businesses lost millions of dollars in extortion payments. RiskRecon analyzed 633 publicly disclosed ransomware events that disrupted operation through encryption between 2017 and 2021. This year, ransomware attacks show no signs of slowing down; cybercriminals continue to target organizations of all shapes and sizes and existing variants of malware continue to resurface while new ones are constantly emerging.

To ensure that your organization remains #CyberFit and resilient in the face of a ransomware attack, we met with Carlos Rivera, Principal Advisory Director at

Info-Tech Research Group, to get his insight on trends and how to protect against cyberthreats.

1 Based on your research, what are the top ransomware trends that organizations should be aware of in 2023?

In my opinion, the biggest trend we'll see in 2023 is an increase in initial access brokers (IABs).

IABs follow an outsourcing model like Ransomware as a Service. They gain access to a compromised corporate network sold by cybercriminal groups and then grant an attacker the initial foothold to mount their attack.

Another trend we're seeing is Ransomware as a Service (RaaS). Some cybercriminals are now offering RaaS, making it incredibly convenient to mount an attack globally. Tools and infrastructure are provided for others to carry out ransomware attacks in exchange for a cut of the ransom. 2022 also witnessed the return of Lockbit 3.0, a new version of the notorious ransomware-as-a-service platform, which holds the record for the fastest encryption rate on the market.

Carlos Rivera

Principal Research Advisor Security & Privacy
Info-Tech Research Group

Trends in Ransomware

Finally, organizations need to be wary of double extortion. This is a combination of ransomware and extortion attacks. They involve an attacker deploying malware that both encrypts and exfiltrates data. Agents will extract sensitive data before encrypting files and deploying their ransom requests, making it difficult to disengage from negotiations. The attackers will not only leave the victim's data encrypted but also start leaking sensitive information, causing significant damage to a company and its clients.

Expect ransomware to remain a persistent threat in 2023 as the new cartels focus on small and medium organizations as well as softer targets that are less likely to draw attention from law enforcement. This trend also increases the risk to municipal and county government systems.

> 2 Endpoint protection refers to the measures taken to secure the devices that connect to an organization's network, such as desktop computers, laptops, and networked mobile devices. Why is it challenging for organizations to protect their endpoint devices against ransomware attacks?

There are several challenges at play. Firstly, there's a lack of visibility across complex networks. It can be difficult to monitor activity on every employee's endpoint device, which makes it harder to track and secure all devices.

Also, endpoint protection can be especially challenging when it comes to mobile devices, which are often used outside of the organization's network and may not have the same level of security as desktop computers.

There is also the factor of human error. Endpoint devices are often used by employees who may make mistakes that compromise security, such as falling for a phishing attack or downloading malware.

"It is crucial to take steps toward protecting your organization against ransomware attacks. This includes keeping all software up to date, using strong passwords and two-factor authentication, and being cautious when opening emails or downloading attachments and running those files," Rivera recommends.

Trends in Ransomware

3 How can organizations prepare for these new threats?

Many organizations lack the ability to orchestrate an effective IR plan. An IR playbook provides organizations with steps in response to scenarios like zero-day threats as well as procedures to escalate potential security breaches. Some organizations may not have the right endpoint protection or response procedure in place. This can be damaging to a business because without implementing the right endpoint protection, their security team will lack awareness about a potential ransomware attack.

To address these challenges, organizations are advised to adopt a comprehensive and integrated endpoint protection solution. Having an integrated solution delivers many benefits, as it equips businesses with a proactive cybersecurity strategy that detects and reacts against external threats. An integrated solution also enables businesses to guard their data and bridge gaps such as the lack of an experienced cybersecurity team or the time and resources required to manage multiple, complex cybersecurity solutions.

Apart from implementing the right integrated solution, businesses can identify agents to perform regular security backups of critical endpoints to meet continuity expectations during a potential ransomware event. Teams within organizations can create alignment on security policies and initiatives to protect data against breaches or theft. To further protect an organization's assets, security leaders can provide in-house training courses to educate employees on the latest cybersecurity trends, how to identify a security threat, and how to prevent a ransomware attack.

4 Why should MSPs seize the opportunity to address this problem for businesses?

In July 2022, BlackHat USA surveyed hundreds of attendees and found that cybersecurity professionals are mentally exhausted, with a little less than half expressing some form of mental burnout and little time to respond to threats. In that same survey, over 60% found that detecting attacks and threats in an IT environment that is decentralized and perhaps cloud oriented poses the biggest challenge to their organization. The survey goes on to state that 52% of cybersecurity professionals claim finding potential security vulnerabilities in a complex and decentralized IT environment poses the biggest risk from cyberattacks.

Trends in Ransomware

MSPs have a unique opportunity to help businesses reduce costs and increase efficiency with robust security services and visibility over potential threats.

Ultimately, MSPs can support their clients by protecting their information using competitive data recovery and endpoint protection solutions. By enabling businesses to succeed in today's digital environment with low operational overhead, MSPs can directly fuel their own growth and secure long-term business partnerships.

5 What is a cross-NIST approach, and why is it important to maintaining a secure environment?

A cross-NIST approach refers to a method in cybersecurity that involves the use of multiple standards and guidelines from the National Institute of Standards and Technology (NIST). NIST is a non-regulatory agency of the U.S. Department of Commerce that develops and promotes standards, guidelines, and best practices for information technology, including cybersecurity.

The NIST Cybersecurity Framework (CSF) is a widely used framework that provides guidance for organizations to manage and reduce cybersecurity risks. It is based on five core functions including identify, protect, detect, respond, and recover. A cross-NIST approach involves using multiple standards and guidelines from NIST in an integrated and coordinated manner to address an organization's cybersecurity needs. This may include using multiple NIST frameworks, such as the CSF, and other NIST standards and guidelines.

A cross-NIST approach is important because it enables organizations to protect their data and mitigate cybersecurity risk. By taking a cross-NIST approach, organizations can ensure that their cybersecurity and ransomware protection efforts are comprehensive and aligned with current best practices.

Additionally, a cross-NIST approach allows organizations to customize their cybersecurity efforts for their needs by combining multiple NIST standards and guidelines. Using multiple standards and guidelines allows organizations to build a defense-in-depth approach that helps prevent, detect, and respond to cybersecurity incidents. Ultimately, a cross-NIST approach equips organizations to effectively manage and reduce their cybersecurity risks and become more resilient to cyberthreats like ransomware attacks.

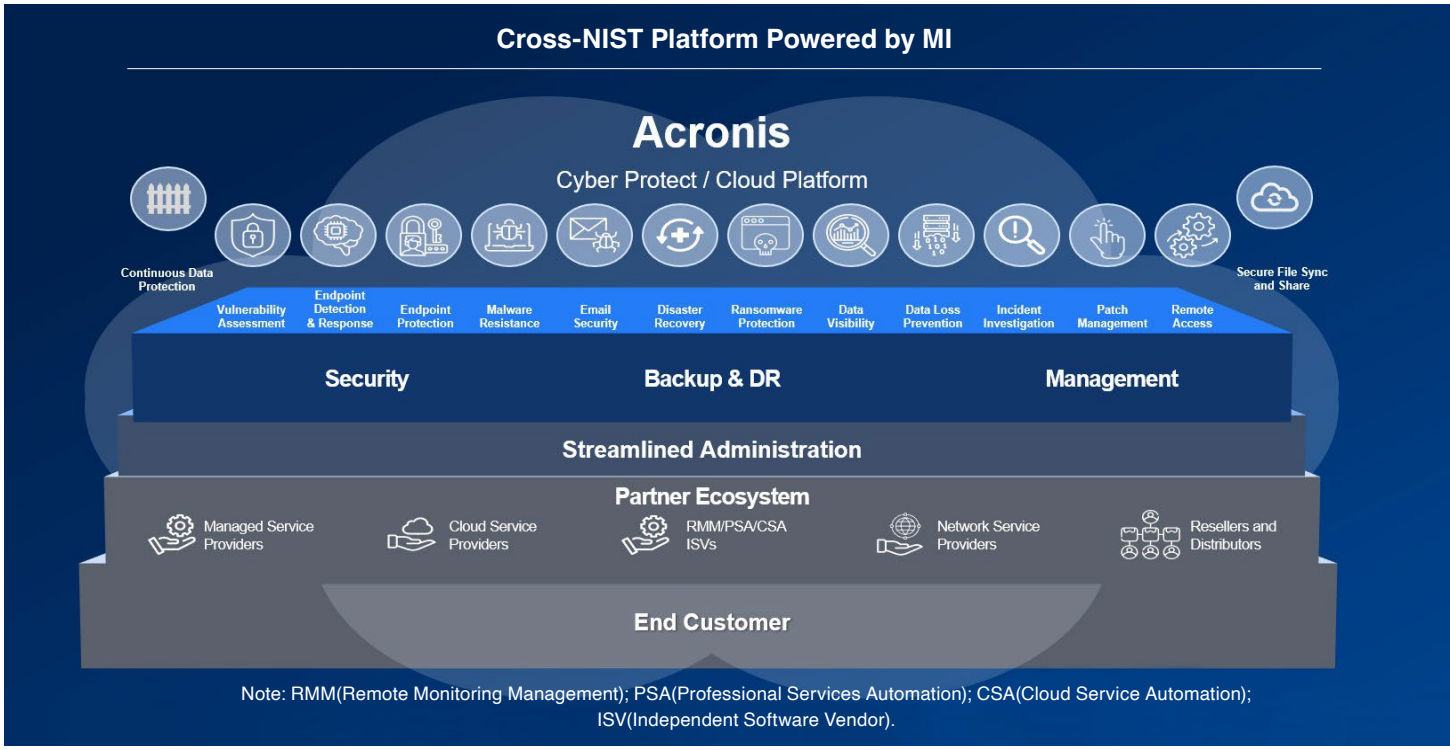
Introducing Acronis Cyber Protect Cloud Platform

Founded in 2003, Acronis is a global technology vendor headquartered jointly in Switzerland and Singapore. Its flagship platform, Acronis Cyber Protect Cloud, is used by over 50,000 technology partners (including managed service providers and value-added resellers) in over 150 countries to provide cybersecurity, data protection, and endpoint management to more than half a million businesses.

The Acronis platform is bolstered by Acronis Cyber Cloud, a global network of over 50 secure data centers, and over 140 integrations with independent software vendors. The brand is strengthened by Acronis Cyber Protect Home Office, a consumer offering with over five million users that is cited by many IT professionals as the first backup product they used at home or school.

Acronis is a pioneer in cyber protection - the integration of cybersecurity, data protection and endpoint management - delivered as a suite of services by MSPs or as a single software product by VARs, with a single agent on each endpoint and managed from a single console.

The Acronis platform delivers a comprehensive set of capabilities to protect business uptime and data against cyberattacks, infrastructure failures, natural disasters, and human error, as shown in Figure 1:



Cybersecurity, Data Protection, and Endpoint Management Capabilities of the Acronis Platform

Achieve Cross-NIST Support Using Acronis

These capabilities span the entire US National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF), a widely adopted set of standards and best practices for reducing cyber risk. The CSF categorizes cybersecurity functions into five phases: identify, detect, protect, respond, and recover. Acronis supports each of these phases with a broad and growing list of data protection and cybersecurity features.

This end-to-end approach to protecting business uptime and data has become essential in a world where:

- Cybercriminals generate hundreds of thousands of novel iterations of malware every day
- The scale, ingenuity, and destructiveness of ransomware attacks grows every year
- New AI tools like ChatGPT have emerged to enable low-skilled criminals to succeed with cyberattacks based on phishing and exploitation of known software vulnerabilities
- Compliance regulations are imposing more stringent demands on how businesses protect sensitive data and where they store it
- Climate change is amplifying the destructive power of floods, storms, and fires

Backed by $500M in private capital, Acronis continues to invest in:

- Additional cybersecurity, data protection, and endpoint management capabilities
- Machine learning and artificial intelligence to help businesses increase the automation, efficiency, and adaptability of their efforts to protect their uptime and data
- Integration with many more ISVs to extend the platform's functionality for service providers and vertical applications
- Expansion of the global footprint and number of secure data centers in Acronis Cyber Cloud
- Promotion of the Acronis Cyber Foundation, a non-profit institution that builds schools for and provides technical training to children and adults in need around the world.

Identify

- SW & HW inventory
- Data Classification
- Unprotected endpoint discovery

Protect

- Vulnerability assessments
- Patch management
- Exploit prevention
- Backup integration
- Device control

Detect

- Emerging threats feed
- Search for IOCs of emerging threats
- Anti-malware & anti-ransomware
- URL filtering
- Email security

Respond

- Rapid analysis and interpretation
- Workload remediation with isolation
- Remote investigation and forensic backups

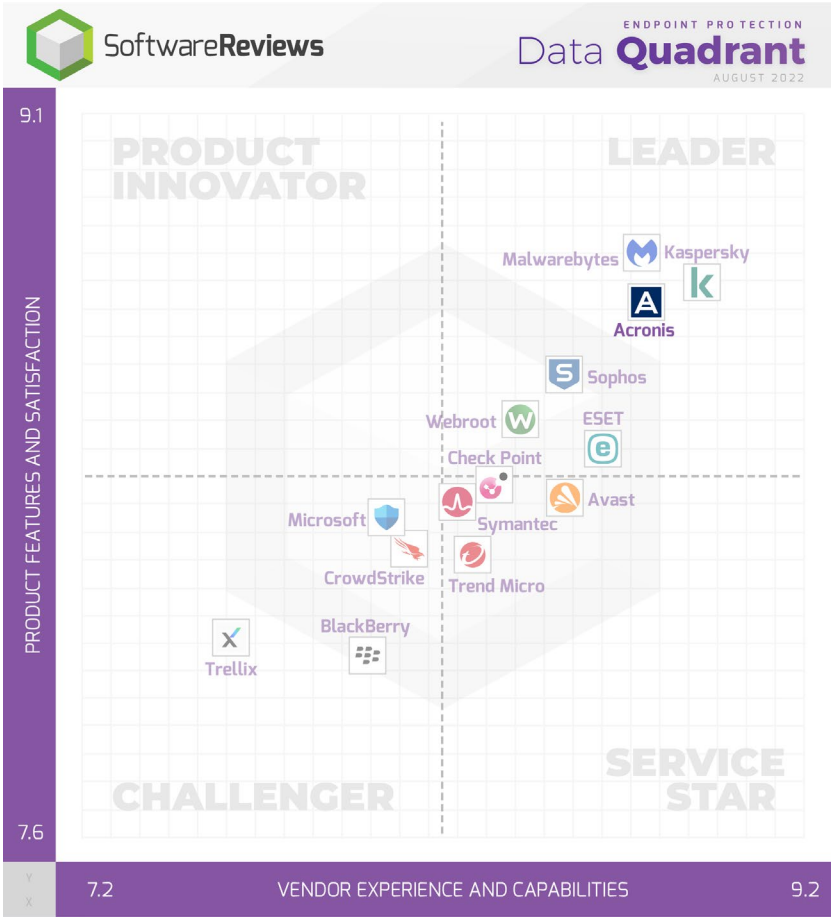
Recover

- Rapid rollback of attacks
- Pre-integrated with disaster recovery
- One-click mass recovery
- Self-recovery

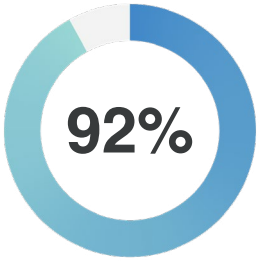
Acronis Is a Gold Medalist in the 2022 SoftwareReviews Endpoint Protection Data Quadrant

What is the Data Quadrant?

SoftwareReviews evaluates aspects of software capabilities and features using a weighted average of user satisfaction scores. These ratings use a satisfaction scale to determine whether software delights or disappoints, creating a powerful indicator of overall user value.



Plan to Renew



Likeliness to Recommend

"If you're looking for one solution for most of your endpoint protection, management and backup, this is it."

VP of Technology, Electronics

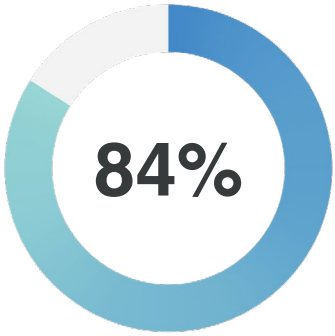
Customers are highly satisfied with Acronis, rating the software an 8.7/10 Composite Score. The Composite Score is an average of four different areas of evaluation: Net Emotional Footprint, Vendor Capabilities, Product Features, and Likeliness to Recommend.

Acronis Drives Business Value

Endpoint protection software supports organization effectiveness results by securing data, minimizing ransomware threats, and ensuring business continuity.

With an emphasis on innovation to support modern threats, the ability to provide next generation security features, and outstanding feedback on customer support, it's no wonder customers appreciate working with Acronis.

Based on an 84% satisfaction score for business value created, survey results prove that Acronis paves the path for organizations to protect themselves against ransomware.



Business Value Created

"Best cyber protection company around! Dive headfirst in and don't look back. You won't be disappointed."

Founder, MSP

"No more sleepless nights worrying about backups! Acronis works wonders."

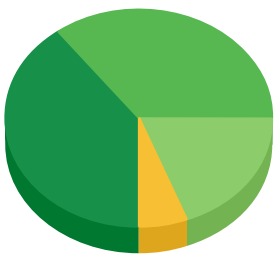
Senior Security Engineer, IT Services

Acronis is a critical part of any organization's security environment

Endpoint protection is the first line of defense in protecting the organization's environment.

94% of customers recognize the importance that Acronis plays in contributing to their success and combatting ransomware attacks.

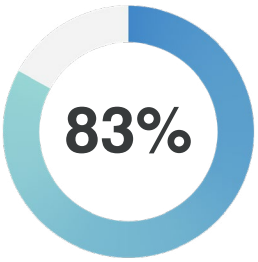
CRITICAL
94%



A Focus on Innovation to Support Modern Threats

Acronis's mission is to protect the data, applications, systems, and productivity of its customers. This means an emphasis on continuing to build the best solutions to meet modern security environments.

Acronis integrates backup, recovery, and next-generation, AI-based anti-malware, and protection management into one solution. With an ever-evolving solution designed to improve security and reduce threats, it's no wonder Acronis was rated #1 in product strategy and rate of improvement.



Rated 1st Overall for Product Strategy and Rate of Improvement

"Acronis is the ideal full-stack solution. It streamlines the process of adding new users, overall security, workflow, reporting, monitoring, and fights the most sophisticated attacks with its complex algorithms and innovative use cases."

Consultant, Infrastructure Development

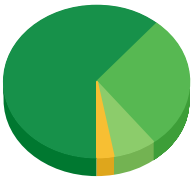
Bad actors won't stop thinking of new ways to get your data; Acronis won't stop innovating ways to stop them

The nature of security threats is constantly changing, with new threats continuously appearing. If your security partner is not continuously improving, this can leave your organization vulnerable without even knowing the threats exist.

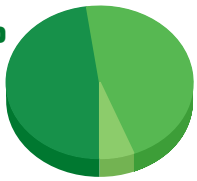
Acronis customers rate the platform highly on its ability to continually improve, inspire, innovate, and deliver product enhancements to meet the needs of organizations to mitigate potential security threats and prevent ransomware attacks.

With an emphasis on inspiring customers to meet today's threat environment, it's no surprise that Acronis is trusted by over five million individual users and 500,000 businesses across the globe.

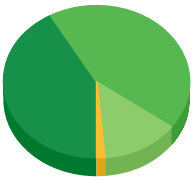
CONTINUALLY IMPROVING
97%



HELPS INNOVATE
100%



INSPIRING
99%



"Revolutionary product that is constantly improving!"

Managing Director, Cloud Security

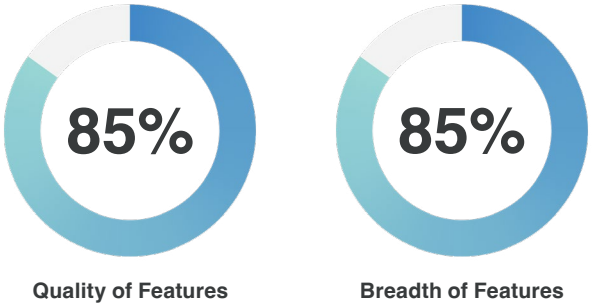
Next-Generation Security Features

When evaluating features in an endpoint protection software, organizations should consider a solution that is compatible with NIST standards and guidelines so security teams can easily align their cybersecurity efforts with industry standards.

Acronis provides next-generation security features that are compatible with NIST standards and help security teams automate processes, customize the platform to their needs, and integrate seamlessly with their existing systems. This is validated by data that reveals Acronis customers rate the solution favorably for its quality and breadth of features.

"In terms of product features and accessibility, Acronis nailed it."

Business Development, Food and Beverage



Quality of Features **Breadth of Features**

Key Features

Dynamic Malware Detection

Easily monitor potential security threats by applying heuristics to files, which identify and block malware.

Cross-Platform Support

Take control of multiple client devices and operating systems supported by one secure, powerful omnichannel solution.

Centralized Management Portal

Streamline processes and drive efficiency with tools to optimize comprehensive policies, synchronization, and more.

System Hardening

Automate workflows and save time with instant vulnerability patching and vulnerability assessment.

Ransom Recovery and Removal

Effortlessly recover files removed by ransomware attacks and access encrypted data.

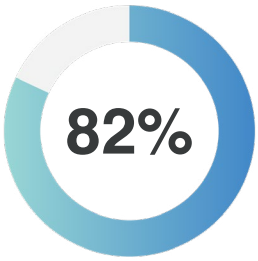
Endpoint Detection and Response

Leverage machine learning to simplify the process of detecting active threats and combat against known and unknown malware.

Effective Customer Support and Training

Partnering with an endpoint protection solution that provides superior customer support is crucial to protect your organization against a ransomware attack. Acronis ensures an exceptional customer support experience in multiple ways, including:

- #CyberFit Academy to access technical training
- Acronis Forum to participate in product discussions, share ideas, and connect with the community
- Knowledge Base to troubleshoot issues using how-to guides and technical documentation
- Acronis Support Team to address issues instantly and minimize bottlenecks



Vendor Support

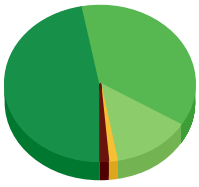
"The feature suite is incredible. World class support, both technical and sales. Everyone I've interacted with is super friendly."

Senior Security Engineer, IT Services

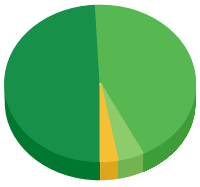
An efficient, respectful, and caring support experience

Vendor support goes beyond simply addressing technical questions from customers. It's about sharing resources and guiding customers whenever and wherever they need assistance and providing a positive service experience. Data reveals that Acronis elevates vendor support by guaranteeing an efficient, respectful, and caring support experience. With access to effective vendor support and training material, it's no surprise that customers rate Acronis highly for vendor support and availability and quality of training.

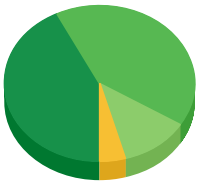
EFFICIENT
97%



RESPECTFUL
97%



CARING
96%



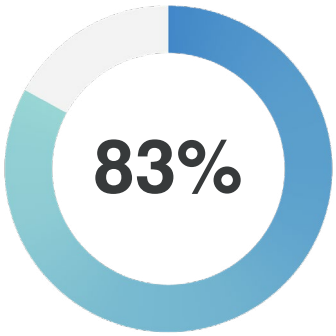
"I would recommend switching to Acronis because it is by far the best backup software I've ever used. Our Acronis Sales Manager, who is both supportive and educational, calls us once a month for a catch-up conversation. I'm delighted to recommend that you try out this fantastic product."

Manager, Technology

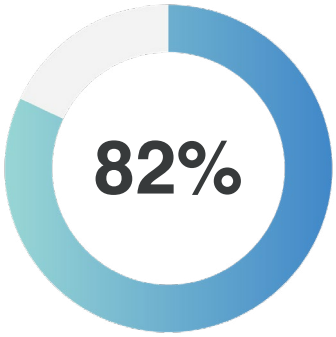
Easy to Implement, Easy to Operate

Endpoint protection software that is designed with an easy-to-use interface will expedite the ramp-up time for new users and help current users gain confidence in the platform. To ensure the highest return on investment and maximum protection against ransomware threats, security teams need to choose a solution that is developed for the needs of the end user.

The Acronis platform offers users a clean interface, straightforward navigation, and intuitive features to simplify adoption and implementation. The platform also allows users to quickly launch, integrate with existing systems, and adapt the ransomware solution to their specific needs.



Ease of Implementation



Ease of IT Administration

Customer feedback confirms that Acronis is easy to implement and easy to use. More specifically, survey results reveal that 83% of users are satisfied with the ease of implementation and 82% of users are satisfied with the ease of IT administration.

"I really love how Acronis crosses my expectations. It's simple to use and performs admirably. The visual editor makes integrating and using the platform simple for non-technical users. The feature set is extensive, and the API-first approach enables easy customization and functionality addition. It's incredibly user-friendly."

Manager, Technology

"If you are looking for a cost-effective solution to have more than just backup capabilities and an easy-to-use centralized console, then look no further and go for Acronis Cyber Protect."

Tech Lead, IT Service Provider

A Long-Term Partner to Protect Your Company

When securing the right long-term partnership, it is important to consider aspects of the solution beyond features and price. SoftwareReviews research shows that in addition to meeting critical functional needs, it is the vendor relationship that also contributes to long-term success.

The SoftwareReviews Word Cloud aggregates the most commonly experienced pain points and prevailing opinions held by its users. With strong words like Trustworthy, Altruistic, and Friendly, it is clear that customers have a strong positive sentiment toward working with Acronis.

"This is one of the best cyber security software in this budget. If you need a reliable cyber security software, then you should try Acronis."

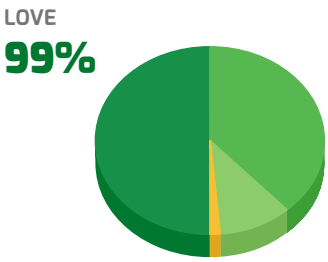
Project Manager, FinTech

Word Cloud

Customers love working with Acronis

With an outstanding product, a focus on innovation, and outstanding customer support, it's no wonder that 99% of customers indicate they love working with Acronis.

For more information, product demos, and a free trial visit:
www.acronis.com/en-us/products/cyber-protect



About Acronis

Acronis unifies data protection and cybersecurity to deliver integrated, automated cyber protection that solves the safety, accessibility, privacy, authenticity, and security (SAPAS) challenges of the modern digital world. With flexible deployment models that fit the demands of service providers and IT professionals, Acronis provides superior cyber protection for data, applications, and systems with innovative next-generation antivirus, backup, disaster recovery, and endpoint protection management solutions powered by AI. With advanced anti-malware powered by cutting-edge machine intelligence and blockchain based data authentication technologies, Acronis protects any environment – from cloud to hybrid to on premises – at a low and predictable cost.

Acronis is a Swiss company, founded in Singapore. Celebrating two decades of innovation, Acronis has more than 2,000 employees in 45 locations. Acronis Cyber Protect solution is available in 26 languages in over 150 countries and is used by 16,000 service providers to protect over 750,000 businesses.

About Info-Tech Research Group and SoftwareReviews

SoftwareReviews is a division of Info-Tech Research Group, a world-class IT research and analyst firm established in 1997. Backed by two decades of IT research and advisory experience, SoftwareReviews is a leading source of expertise and insight into the enterprise software landscape and client-vendor relationships.

By collecting data from real IT and business professionals, the SoftwareReviews methodology produces the most detailed and authentic insights into the experience of evaluating and purchasing enterprise software.

Data quality is paramount. That's why SoftwareReviews bends over backwards to ensure the data it is collecting is from experienced users, so you can trust it and make decisions with confidence.

Every review is thoroughly checked for authenticity through a robust QA process. Dynamic reviews adapt according to the reviewer's role and experience, avoiding inaccurate guesses.

About the Research

Endpoint protection platforms defend against malware, phishing attacks, and virus attacks to minimize risk and ensure smooth business operations.

SoftwareReviews data referenced in this report is sourced from 1,308 survey respondents, the August 2022 Endpoint Protection Data Quadrant report, and the Acronis Cyber Protect Product Scorecard.

SoftwareReviews Data Quadrant Methodology

SoftwareReviews collects user insights that help organizations more effectively choose software that meets their needs, measure business value, and improve selection.

Data and insights shown in this report were gathered from 1,308 validated users from the Endpoint Protection category.

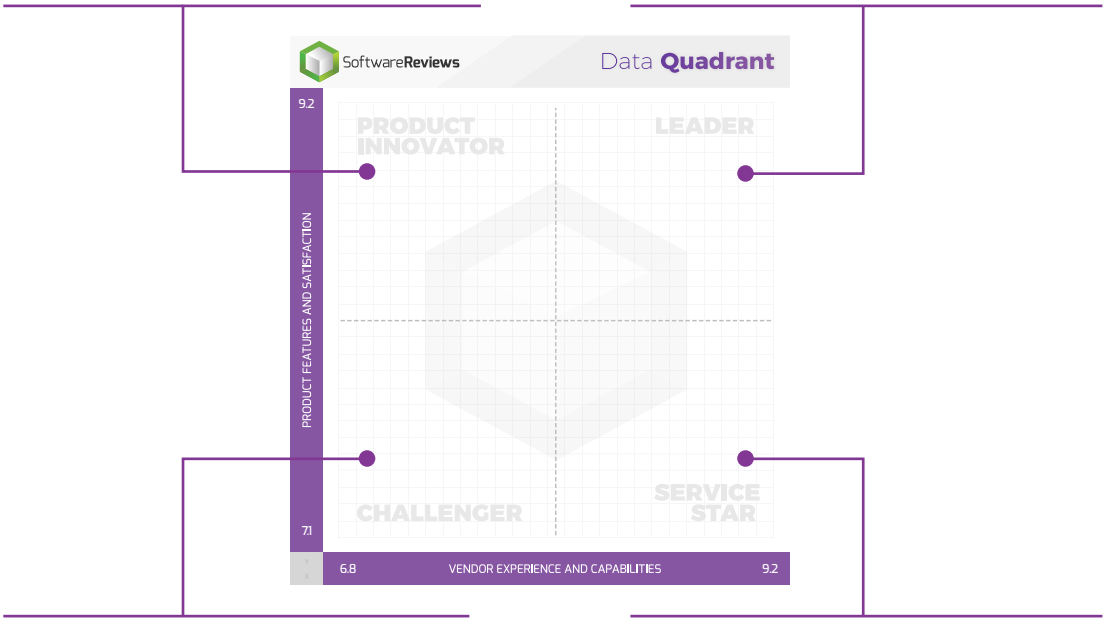
Rankings, results, and positioning on SoftwareReviews reports is based entirely on end-user feedback solicited from a proprietary online survey engine.

Product Innovators

Products that emphasize product features, gaining strong recommendations from their customers.

Leaders

Products that resonate strongest in the market, balancing features with a great user experience.



Challengers

Products that are strong performers in some areas and trail in others. Often up-and-coming vendors.

Service Stars

Products that emphasize a good experience and build strong relationships with customers.

Acronis