Publication date:
25 Feb 2025
Author(s):
Hollie Hennessy, Principal Analyst

On the Radar: Acronis delivers backup and recovery for OT cybersecurity resilience

Summary

Catalyst

Acronis' operational technology (OT) offering focuses on the "recover" piece of the cybersecurity puzzle. It provides backup, recovery, and data security for OT environments to enhance cybersecurity resilience. Acronis' strong partner and channel network also solidifies its reputation in the OT security space.

Omdia view

OT security includes several different objectives, one of which is recovery in the event of an incident or attack. In operational and critical infrastructure environments, perhaps even more than in some IT environments, business continuity is key—given the regulatory requirements for many critical infrastructure organizations and the often large financial impact or potential harm caused by downtime.

Having an effective, tried, and tested backup and recovery plan is vital in any environment. Even with the best protection in place, an attack may still happen. Thus, knowing what to do in this event and being able to get systems back online in the shortest possible window should be a fundamental part of any cybersecurity strategy. Regular backups are key, alongside a process to restore exfiltrated data quickly and efficiently.

Acronis' backup and recovery offering is predominantly channel-focused. It offers service providers and industrial vendors the opportunity to include backup and recovery in their services and platforms, as well as a direct-to-enterprise point product for OT-centric organizations.

Why put Acronis on your radar?

Acronis has partnered with OEMs, featuring as the backup and recovery solution for a significant number of leading industrial automation vendors across the manufacturing, healthcare, and energy verticals. The vendor's product helps to ensure compliance with regulatory requirements (e.g., for NIS2) and standards (such as ISA/IEC 62443). Additionally, it can enhance the product offering of industrial automation vendors by providing a more robust and trusted service to their customers. Given its expertise in the backup and recovery space, Acronis has been able to develop a solution that suits the needs of industrial environments and the legacy systems still used within them.

Market context

The OT security market is dominated by asset management, monitoring, detection, and response—with many of the leading vendors in the space offering capabilities across all or most of these areas. That said, there are additional capabilities required in the market to meet both regulatory requirements and the needs of industrial and OT-focused organizations.

Business continuity (whether for safety, operational, or financial reasons) is of utmost importance in these environments. Thus, being able to detect breaches or attacks is key, as is being able to prevent known threats. Additional capabilities have emerged to address the latter, whether they be preventive automation or more proactive approaches such as risk and vulnerability management, breach and attack simulation, and attack surface management.

However, since no system is completely infallible, there is still a need to be able to recover from any given incident. This portion of the market focuses on cybersecurity resilience, encompassing incident response tooling and services, forensics, and data and system recovery—where Acronis' solutions are a good fit for OT.

The NIST Cybersecurity Framework (CSF) 2.0 is a good indication of the cybersecurity requirements for critical (and, in fact, all) organizations. Initially focused on critical infrastructure, the framework is widely adopted and referenced—though its remit is now broader. The updated version of the framework spans various capabilities:

- Identify
- Protect
- Detect
- Respond
- Recover
- Its latest addition, govern

Product/service overview

Acronis' data protection capabilities broadly span two areas, "Backup" and "Disaster Recovery," which make up part of its platform, Acronis Cyber Protect. Features include the following:

- Full image backup on a running system, with fail-safe patching that creates an image backup before system or application patches are applied
- Self-service with "One Click Recovery"
- Universal restore, allowing recovery to any hardware or hypervisor
- Instant restore to boot and run while recovery continues
- Immutable backups for enhanced security
- Support of Windows, Linux, and other OS/applications, including legacy versions such as Windows XP that are still in use in industrial environments
- Anti-malware scans and antivirus updates automated within the recovery process
- Fully integrated disaster recovery as a service

Tailored to the OT environment, Acronis Cyber Protect performs installation and backups live, so it is not necessary to take systems offline, and no reboot is required. In addition, Acronis' offering can support recovery to new hardware if needed. This is done through the Acronis Cyber Protect agent, which can be installed with or without anti-malware components depending on customer constraints and requirements.

Recovery is simplified with One Click Recovery, meaning that those who are not IT or security professionals can get systems back up and running without having any particular technical expertise. This is especially important in remote, distributed environments such as deep sea oil rigs, where onsite access can be challenging, as well as in time-sensitive scenarios such as restarting operations on a manufacturing line. There is also the option to recover with a reboot from a local disk backup or from the Acronis cloud. In addition, the backed-up data is automatically scanned for malware and updated to the latest antivirus.

Insights and control are aggregated in a centralized dashboard called the Centralized Acronis Monitoring Hub, which utilizes metadata for analysis, as well as for integration with third-party software.

Company information

Background

Founded in Singapore in 2003 and incorporated in Switzerland in 2008, Acronis now has over 1,800 employees in 45 locations. It serves over 750,000 corporate customers in 150 countries.

The vendor has seen significant growth, building on its data protection roots in recent years to offer a range of cybersecurity products to its partners and customers. It has also been pioneering the concept of merging the two fields with its Acronis Cyber Protect platform.

Acronis has a strong focus on research and development with Acronis Labs, which is staffed by over 500 engineers, more than 20 with PhDs, and holds over 200 patents awarded during its 17-year existence. The

Acronis Threat Research Unit (TRU) also regularly publishes insights and discoveries on current and emerging cyberthreats.

In August 2024, it was announced that EQT, a European private equity firm, would acquire a majority stake in Acronis at an estimated $4bn valuation. This transaction is expected to be completed in 1Q25 or 2Q25. Prior to this, Acronis had raised over $500m from investors such as CVC Capital Partners, BlackRock, and Goldman Sachs.

Current position

Acronis has a range of cybersecurity technologies that extend beyond backup and recovery in the OT space, including its newly launched Extended Detection and Response (XDR) product and its supporting generative artificial intelligence (AI) assistant. The vendor's portfolio broadly covers the following:

- Data protection (discussed above)
- Cybersecurity (endpoint security, malware prevention, EDR/XDR, etc.)
- Endpoint management (patch management, vulnerability management, remote access, etc.)

While some portion of Acronis' business is selling direct to the end user, its primary route to market is through the channel, including resellers, managed service providers (MSPs), and OEMs. In the industrial automation space, these include a number of vendors, including ABB, Emerson, Siemens, Schneider Electric, Rockwell Automation, and Yokogawa.

Notably, Acronis offers a freemium version of its platform with more advanced features that are paid for on a pay-as-you-go basis.

Future plans

Although Acronis is looking to develop its AI platform with further cybersecurity functionality, it does not have plans to cover Internet of Things (IoT) and OT.

Key facts

Table 1: Data sheet: Acronis

Product name	Acronis Cyber Protect	**Product classification**	Endpoint protection and backup/recovery
Version number	v16	**Release date**	February 2024
Industries covered	Manufacturing Healthcare Lab research (a.k.a. biopharma) Oil & gas Power generation/energy Logistics Automotive Retail Education/government Construction	**Geographies covered**	North America Central & South America EMEA APAC
Size of target companies	Enterprise, midsize, SMB	**Licensing options**	Perpetual or subscription software licenses
URL	www.acronis.com https://www.acronis.com/en-us/products/cyber-protect-enterprise/	**Route(s) to market**	Direct
Company headquarters	Schaffhausen, Switzerland	**Number of employees**	~2,000

Source: Omdia

Analyst comment

Acronis' numerous innovations and specialization in the data protection and recovery space have led to an attractive offering for industrial environments. It provides several options for deployment, backup, and recovery, enabling flexibility and meeting individual customer needs. Many of the OT security vendors that service providers or industrial automation vendors may partner with do not offer data recovery capabilities, which leaves a sizable opportunity for Acronis. Its competitors in the data recovery space tend to focus more on the IT side of the house. They also lack the specialization Acronis can offer in industrial environments and the reputation it has gained through close integration and partnerships with leading industrial OEMs.

That said, Acronis' offering to the channel and its partners is the wider platform—which does not meet OT security requirements above and beyond "recover" and has no current plans to do so. Its MSP/managed security service provider (MSSP) partners are more focused on delivering IT to end users. In addition, moving into the IoT/OT space with a security operations solution would likely require significant development, given device behaviors and proprietary protocols. The platform would allow partners to offer key IT security-related capabilities, but they will likely turn to other OT security vendors for detection,

prevention, and visibility to support industrial clients if needed. While the OT security leaders do not currently focus on data protection and recovery, there is an opportunity for these vendors to also try to fill the gap, creating a more competitive landscape.

Appendix

On the Radar

On the Radar is a series of research notes about vendors bringing innovative ideas, products, or business models to their markets. On the Radar vendors bear watching for their potential impact on markets as their approach, recent developments, or strategy could prove disruptive and of interest to tech buyers and users.

Further reading

Omdia Market Radar: OT Cybersecurity Platforms, 2025 (January 2025)

2025 Trends to Watch: IoT Cybersecurity (September 2024)

"Xage Security announces new partnership with Armis and Yokogawa Engineering Asia to provide secure remote access" (September 2024)

Omdia Secure Industrial Networks Survey 2023: Overall Findings (December 2023)

Author

Hollie Hennessy, Principal Analyst, IoT Cybersecurity

askananalyst@omdia.com

Citation policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the "Omdia Materials") are the copyrighted property of TechTarget, Inc. and its subsidiaries or affiliates (together "Informa TechTarget") or its third party data providers and represent data, research, opinions, or viewpoints published by Informa TechTarget, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa TechTarget does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa TechTarget and its affiliates, officers, directors, employees, agents, and third party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa TechTarget will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.

CONTACT US

omdia.com

askananalyst@omdia.com