How Acronis Addresses Primary Industrial Cybersecurity Challenges Through Platformization

ARC VIEW

April 23, 2026

By Larry O'Brien

ARC Advisory Group

VISION, EXPERIENCE, ANSWERS FOR INDUSTRY, ENERGY, & INFRASTRUCTURE

KEYWORDS: Industrial Cybersecurity, Platformization, Unplanned Downtime, IT/OT Convergence, Regulatory Compliance, Industrial AI, Machine Learning

Overview

As the cost of doing business continues to rise and cyber threats mount, end users on OT cybersecurity teams are looking to simplify their approach to cybersecurity to reduce costs and gain better insights into the threat environment, thereby improving overall cyber resilience. Cyber incidents have become a major driver of unplanned downtime across manufacturing and critical infrastructure, creating financial, safety, and environmental risks. Current geopolitical events have only increased the risk. OT cybersecurity teams need the right tools, but they can no longer spend the time, energy, and cost required to manage a patchwork of tools they must integrate. Instead, they are adopting more "platformized" approaches that offer greater ease of use and more effective cybersecurity data integration.

Cyber incidents are now a major cause of unplanned downtime in manufacturing, leading to significant financial and safety concerns. Consolidation of cybersecurity tools into unified platforms is a practical strategy to enhance detection, response, and compliance across IT and OT environments. Acronis is a supplier that has adopted a platform-centric approach that also leverages AI.

The global regulatory environment is adding urgency to these efforts, as manufacturing companies doing business in the EU must now comply with NIS 2 standards. Meanwhile, adherence to the Cyber Resilience Act (CRA) standards is approaching in September of 2026. While NIS 2 standards are more applicable to end users in the process industries, CRA standards will affect discrete and hybrid manufacturers, as well as automation suppliers. Many companies doing business in the EU are still unprepared to meet the requirements of these standards and are furiously playing catch-up. Both of these standards have numerous requirements for reporting cyber incidents and demonstrating and documenting technical, operational, and organizational measures to manage cyber risk. This means that OT cyber professionals will spend much more time managing adherence to standards and will have less time to manage complex webs of custom-integrated cybersecurity solutions from a wide range of suppliers.

Acronis is a leading industrial cybersecurity supplier that has evolved its offering into a broader cyber protection platform, providing proactive anti-ransomware protection and centralized management across both IT and OT domains, while continuing to support legacy systems that remain common in industrial facilities and plants. Acronis' adoption of AI-enabled detection, behavioral baselining, and automated response is also a significant advantage in defending increasingly interconnected industrial environments.

Cybersecurity Incidents Are Now a Significant Contributor to Unplanned Downtime in Manufacturing

In the past, most unplanned downtime could be attributed to operator error or some unexpected or abnormal situation in the process being controlled. OT cybersecurity teams are now realizing that cyber incidents are a significant contributor to unplanned downtime in manufacturing operations. ARC estimates that unplanned downtime represents over a trillion dollars in lost revenue worldwide for the industrial and critical infrastructure sectors. A single unplanned shutdown at a refinery can wipe out its entire annual profit. An unplanned power outage can present extreme risks like loss of life and interruption of essential services.

OT Teams Are Simplifying How They Approach Industrial Cybersecurity

In the world of manufacturing and critical infrastructure, cybersecurity resources are already stretched incredibly thin. Even large end users with well-developed industrial cybersecurity organizations are facing constrained resources. Some companies cannot fill the open positions they have because they can't find the right cybersecurity personnel, while others are faced with cost-cutting measures, and they cannot afford to keep the cybersecurity professionals they have. Basically, this means fewer people to do the job with a greater range of responsibilities.

Key Drivers for Platformized Industrial Cybersecurity

OT Teams Cannot Sustainably Manage Complex Patchworks of Tools and Applications

Managing a pastiche of cybersecurity tools that each address different requirements for an overall cybersecurity framework is becoming increasingly challenging. The world of industrial cybersecurity is only now moving past its initial formative stages. In the past, we had a vast landscape of smaller cybersecurity vendors, each offering different areas of functionality. This is all starting to change as the market consolidates and OT cybersecurity suppliers start to offer a wider range of functionality in their solutions within a more integrated environment that can act as a central platform for OT cybersecurity. For OT cybersecurity teams, this also means significantly reducing the number of OT cybersecurity suppliers they must deal with. Supplier relationship management can quickly become a time-consuming and complex process, as different suppliers offer different licensing schemes, pricing structures, and service level agreements.

Platformized Approaches to Industrial Cybersecurity Have Real Business Impact

Platformized approaches reduce operational costs and can be managed more effectively with fewer personnel. More importantly, platforms can improve threat detection, response, and remediation. If an incident does occur, platforms can address the challenges of IT/OT convergence by replacing fragmented, point-product security tools with a unified, cohesive solution. Integrating data management systems (IT) with operational technology (OT) under a single management console enables organizations to manage the heightened risks of interconnected systems by providing visibility, security, and compliance across the entire hybrid infrastructure.

Platforms also offer enhanced incident response capabilities. The tightly integrated environment of a security platform combined with its holistic view of potential threats across the organization means that threats are identified more quickly, providing a faster response and containment. The platform can provide a "single version of the truth" that offers enhanced visibility into OT legacy assets.

How the Regulatory Environment Drives Platformization

The industrial cybersecurity regulatory landscape is changing drastically. New regulations in the EU, the Middle East, Asia, and other parts of the world will significantly drive investment in industrial cybersecurity applications. For the manufacturing industry, encompassing both process and discrete sectors, NIS2 introduces substantial new obligations and potential liabilities. It elevates cybersecurity to a strategic imperative overseen by senior management, demanding comprehensive security measures across IT and OT environments. Compliance requires significant investment in cybersecurity infrastructure, processes, and personnel training.

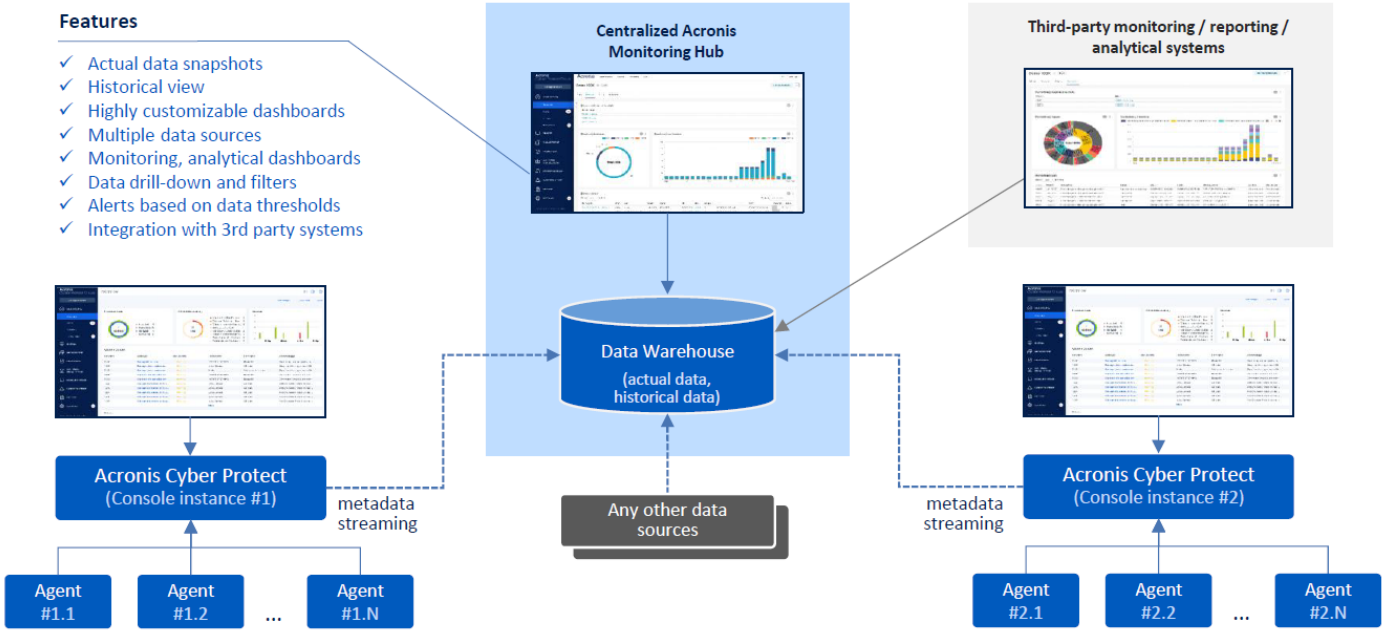
Many companies are scrambling to comply with these new regulations, and the EU has a reputation for strict enforcement. Companies do not have much time to piece together and invest in integrating multiple cybersecurity solutions into a single framework. ARC expects platformization growth to be further driven by the race to comply with these new regulations.

The Acronis Approach to Platformized OT Cybersecurity

Acronis has successfully transitioned from a point-solution provider to a true cybersecurity platform provider. Acronis is a Swiss company that evolved from a traditional backup provider to a cyber protection company delivering natively integrated cybersecurity, data protection, and infrastructure management. Offering a single platform for securing both OT and IT, Acronis aligns with the trend toward platformization and the shift from plant-level to enterprise-wide cybersecurity and data protection.

Roots in Backup and Recovery

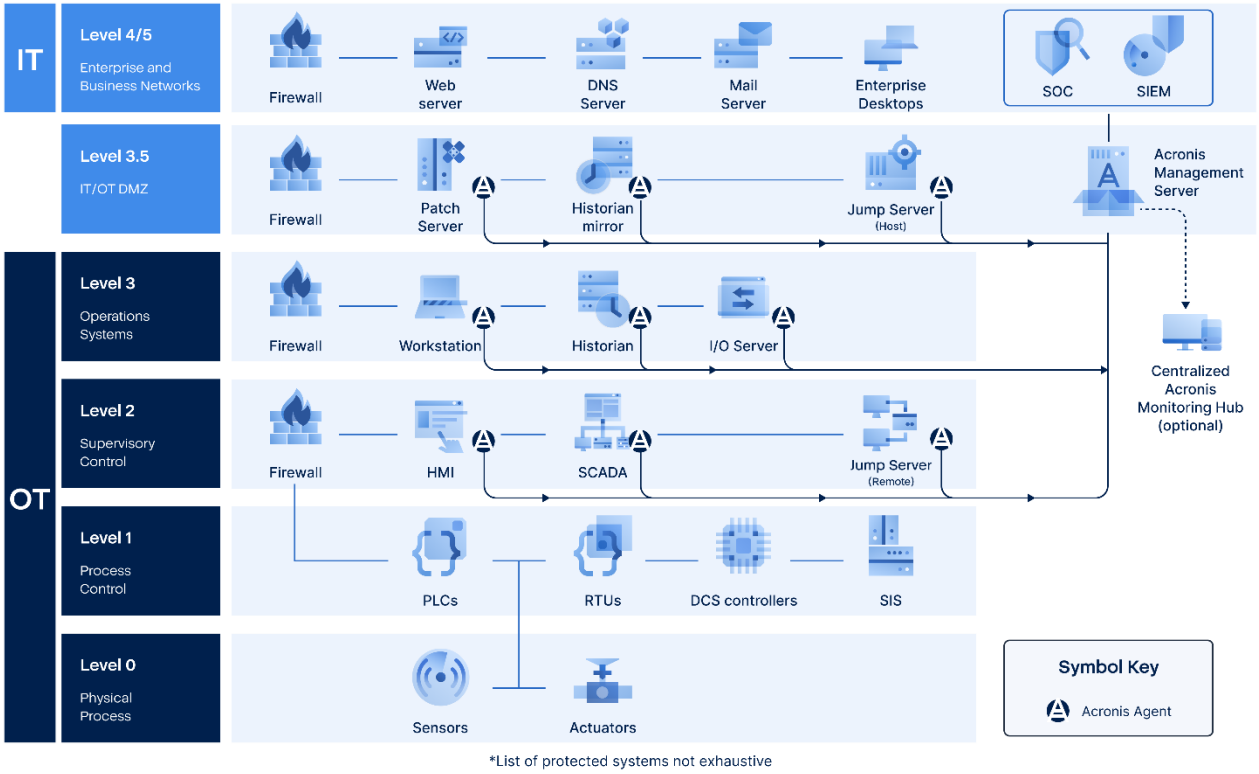
Acronis began as a company focused on data backup and recovery. Backup and recovery functions are among the most crucial in industrial cybersecurity. If an incident occurs or production is interrupted, getting back online and recovering from it is of paramount importance, and every minute lost means lost revenue for the enterprise. Its flagship prosumer product, Acronis True Image, became the industry standard for disk imaging—creating exact replicas of hard drives to restore systems after hardware failure or corruption. Acronis' evolution into OT cybersecurity was driven by the convergence of IT and industrial systems, as well as the rise of ransomware attacks targeting backup files. The company's evolution began when ransomware strains started actively hunting for and deleting backup files to prevent victims from restoring data without paying.



Acronis Enables Multi Site OT System Protection

From Backup and Recovery to Active Protection

Acronis realized that backup alone was no longer sufficient. In 2017, Acronis introduced active anti-ransomware technology into its backup software. This was a market-first move, blending "reactive" recovery with "proactive" threat detection. In 2020, the company launched Acronis Cyber Protect, a single platform that integrated backup, disaster recovery, anti-malware, and management. This effectively marked their transition into a full-service cyber protection provider.



Acronis Cyber Protect Across the Purdue Reference Model/ISA 95 Hierarchy

Cyber Protect Local: Specifically Designed for OT Environments

In 2025, Acronis introduced Cyber Protect Local, an on-premises deployment version of Acronis' unified cyber protection platform designed specifically for organizations that require strict data sovereignty, regulatory compliance, and protection for isolated or air-gapped environments such as those found in industrial and OT applications. Acronis Cyber Protect Local combines backup and recovery, cybersecurity, and endpoint management in a single platform. Acronis Cyber Protect Local is also part of the broader Acronis Cyber Protect 17 platform, which enables centralized management of IT and OT environments through a single pane of glass.

Acronis addresses many of the unique issues facing OT cybersecurity. First among these is older equipment, specifically a mix of new and legacy equipment, some dating back 20 years or more. Many factories still run outdated Windows- and Linux-based operating systems like Windows XP and even older operating systems

long past their end-of-life date. Acronis continues to support many end-of-life operating systems that their vendors no longer support.

Acronis uses a unified, agent-based approach to cybersecurity, deploying a single agent on endpoints to integrate AI-driven anti-malware, vulnerability assessments, and backup into a single solution. This approach enables real-time protection, behavioral threat detection, and immediate recovery, reducing management complexity and increasing security against ransomware and zero-day attacks. The agent is used for both physical and virtual machines to provide deep, granular security and data protection, or it can be utilized in conjunction with agentless approaches for hypervisor-level backup.

Acronis' Relationships with Integrated Automation Suppliers

Acronis has strong relationships with most major integrated automation suppliers, including ABB, Emerson, Honeywell, Siemens, Rockwell, GE Vernova, Intel, and Yokogawa. Acronis embedded in these environments, and the relationship has expanded to include Acronis Cyber Protect.

How Acronis Incorporates Industrial AI

Acronis uses AI-driven technologies and behavioral heuristics, to analyze complex patterns and detect malicious behavior in real time against zero-day and sophisticated attacks that traditional signature-based methods might miss. Their "Active Protection" technology specifically employs AI to recognize and halt ransomware attacks by monitoring processes read/write patterns and detecting encryption attempts.

Baselining Normal System Performance and Behavioral Analysis

Acronis Cyber Protect, particularly through its Active Protection feature, utilizes AI to constantly monitor system processes for anomalous or malicious behavior indicative of ransomware attacks. By analyzing stack traces and establishing baselines of normal system behavior, it can detect and stop ransomware and other malware, including zero-day threats, before they can encrypt data, according to Acronis. This approach is particularly important for OT systems, which are often susceptible to novel attack vectors not covered by traditional signature-based detection.

Beyond recognizing known threats, Acronis' behavioral analysis focuses on identifying malicious intent based on how applications and processes behave, rather than solely on signatures. This allows Acronis to detect and mitigate unknown and emerging threats, including those exploiting vulnerabilities in legacy OT systems. Acronis' AI-driven threat intelligence gathers data from millions of endpoints to train ML models that can predict and proactively prevent attacks. This also includes features like hard drive health monitoring, leveraging machine learning to predict potential failures and prevent data loss and downtime.

Automated Incident Response and Remediation

Acronis also uses AI in its EDR solution to streamline incident response in OT environments by automating incident triage, severity assessment, and remediation suggestions. AI-powered attack interpretation can help security analysts understand and respond to incidents more efficiently. Acronis' solutions also enable the

creation of targeted remediation scripts during active breaches, allowing for rapid containment and minimizing potential damage.

Conclusions

Industrial organizations face increasing pressure to secure operational technology (OT) and information technology (IT) environments against advanced cyber threats. Platformization—the integration of multiple security functions into a unified solution—offers significant business benefits. By consolidating tools and processes, organizations can streamline security management, reduce operational complexity, and improve visibility across diverse systems. This unified approach not only strengthens security posture but also supports regulatory compliance and cost control, making it a strategic driver for digital transformation in industrial settings.

Acronis' platform leverages advanced AI-driven technologies and specialized hardware acceleration, optimizing performance while minimizing resource consumption. This is especially valuable in resource-constrained OT environments, where efficiency and reliability are critical. Acronis One-Click Recovery enables any local non-IT worker to recover a failed OT system without IT support. The holistic nature of Acronis' platform allows for seamless integration with existing infrastructure and provides comprehensive coverage against a broad spectrum of threats, including ransomware and zero-day attacks.

More broadly, the adoption of AI within industrial cybersecurity solutions represents a transformative shift toward proactive and adaptive defense strategies. AI-powered tools can continuously learn from emerging threats, improving resilience and enabling organizations to stay ahead of adversaries. As industrial environments become more interconnected and complex, leveraging AI will be essential for maintaining robust security, reducing downtime, and supporting future innovation in the sector.

For further information or to provide feedback on this article, please contact your account manager or the author at lobrien@arcweb.com. ARC Insights are published and copyrighted by ARC Advisory Group. The information is proprietary to ARC, and no part may be reproduced without prior permission from ARC.