Wie Acronis die wichtigsten Herausforderungen im Bereich der industriellen Cybersecurity durch Plattformisierung angeht

ARC View

12. März 2026

Autor: Larry O'Brien

Keywords: Cybersecurity, Plattformisierung, ungeplante Ausfallzeiten, Zusammenführung von IT und OT, Compliance, industrielle KI, maschinelles Lernen

Überblick

Da die Betriebskosten weiter steigen und Cyberbedrohungen zunehmen, suchen Endbenutzer:innen in OT-Cybersecurity-Teams nach Möglichkeiten, ihren Cybersecurity-Ansatz zu vereinfachen. Ziel ist es, Kosten zu senken und bessere Einblicke in die Bedrohungslage zu gewinnen, um so die allgemeine Cyberresilienz zu verbessern. Cybervorfälle sind mittlerweile eine der Hauptursachen für ungeplante Ausfallzeiten in der produzierenden Industrie und bei kritischen Infrastrukturen. Dadurch entstehen finanzielle, sicherheitstechnische und ökologische Risiken. Die aktuellen geopolitischen Ereignisse haben dieses Risiko noch weiter erhöht. Die OT-Cybersecurity-Teams benötigen zur Bewältigung dieser Herausforderung entsprechende Tools, können sich aber Zeit, Energie und Kosten für die Verwaltung einer Patchwork-Lösung aus verschiedenen, noch zu integrierenden Tools nicht mehr leisten. Stattdessen setzen sie vermehrt auf plattformbasierte Ansätze, die eine einfachere Handhabung und eine effektivere Datenintegration im Bereich der Cybersecurity ermöglichen.

Cybervorfälle sind mittlerweile eine der Hauptursachen für ungeplante Ausfallzeiten in Fertigungsunternehmen. Angesichts dieser Herausforderungen ist es eine sinnvolle Strategie, die benötigten Cybersecurity-Tools unter einer einheitlichen Plattform zusammenzuführen, um die Erkennungs-, Abwehr- und Compliance-Fähigkeiten in IT- und OT-Umgebungen zu verbessern.

Das globale regulatorische Umfeld verleiht diesen Bemühungen zusätzliche Dringlichkeit, da Fertigungsunternehmen, die in der EU tätig sind, nun die NIS2-Anforderungen erfüllen müssen. Gleichzeitig wird es zunehmend wichtig, die Anforderungen des Cyber Resilience Act (CRA) zu erfüllen, da ab September 2026 mit den entsprechenden Standards gerechnet werden muss. Während die NIS2-Anforderungen eher für Unternehmen in der Prozessindustrie relevant sind, werden die CRA-Anforderungen diskrete und hybride Hersteller sowie Automatisierungsanbieter betreffen. Viele in der EU tätige Unternehmen sind noch nicht darauf vorbereitet, die Anforderungen dieser Regelwerke zu erfüllen, und versuchen nun mit Hochdruck aufzuholen. Beide Regelwerke enthalten zahlreiche Anforderungen dazu, Cybervorfälle zu melden und technische, betriebliche sowie organisatorische Maßnahmen nachzuweisen und zu dokumentieren, mit denen sich Cyberrisiken steuern lassen. Das bedeutet, dass die entsprechenden OT-Cybersecurity-Expert:innen deutlich mehr Zeit damit verbringen werden, die Einhaltung dieser Standards zu organisieren und nachzuweisen, und weniger Zeit haben werden, die komplexen Geflechte aus individuell integrierten Cybersecurity-Lösungen unterschiedlichster Anbieter zu verwalten.

Acronis ist ein führender Anbieter von Cybersecurity-Lösungen für die Industrie, der sein Angebot zu einer umfassenden Cyber-Protection-Plattform weiterentwickelt hat. Diese bietet proaktiven Ransomware-Schutz und eine zentrale Verwaltung sowohl im IT- als auch im OT-Bereich. Die Plattform unterstützt auch ältere Betriebssysteme, die in Industrieanlagen und Fabriken nach wie vor weit verbreitet sind. Zudem ist der Einsatz von KI-gestützter Erkennung, Verhaltens-Baselines und automatisierten Gegenmaßnahmen für Acronis ein erheblicher Vorteil beim Schutz zunehmend vernetzter Industrieumgebungen.

Cybersecurity-Vorfälle tragen mittlerweile erheblich zu ungeplanten Ausfallzeiten in der Fertigung bei

In der Vergangenheit waren die meisten ungeplanten Ausfallzeiten auf Bedienungsfehler oder unerwartete beziehungsweise abnormale Situationen in den gesteuerten Prozessen zurückzuführen. OT-Cybersecurity-Teams erkennen nun, dass Cybervorfälle mittlerweile in erheblichem Maße zu ungeplanten Ausfallzeiten in der Fertigung beitragen. ARC schätzt, dass ungeplante Ausfallzeiten in Industrie und kritischer Infrastruktur weltweit zu Umsatzeinbußen von über einer Billion US-Dollar führen. Beispielsweise kann eine einzige ungeplante Abschaltung in einer Raffinerie den gesamten Jahresgewinn zunichtemachen. In bestimmten Bereichen können ungeplante Stromausfälle sogar das Risiko bergen, Menschenleben zu gefährden oder wichtige Versorgungsleistungen zu unterbrechen.

OT-Teams vereinfachen ihre Ansätze in der industriellen Cybersecurity

In der Fertigungsindustrie und bei kritischen Infrastrukturen sind die verfügbaren Ressourcen zur Bewältigung der Cybersecurity-Anforderungen zumeist sehr begrenzt. Selbst große Unternehmen mit gut ausgebauten Abteilungen für industrielle Cybersecurity haben mit begrenzten Ressourcen zu kämpfen. Manche Unternehmen können offene Stellen nicht besetzen, weil sie kein geeignetes Cybersecurity-Fachpersonal finden, während andere ihre Fachkräfte aufgrund von Sparauflagen nicht halten können. Letztlich bedeutet dies, dass mit wenig Personal ein immer größerer Aufgabenbereich bewältigt werden muss.

OT-Teams können den komplexen Flickenteppich aus unterschiedlichen Tools und Applikationen nicht nachhaltig verwalten

Ein ganzes Sammelsurium an Cybersecurity-Tools verwalten zu müssen, die jeweils unterschiedliche Anforderungen eines übergreifenden Cybersecurity-Frameworks abdecken, wird immer schwieriger. Die Welt der industriellen Cybersecurity befindet sich erst jetzt in einer Phase, in der sie ihre anfänglichen Entwicklungsstadien hinter sich lässt. In der Vergangenheit gab es eine Vielzahl kleinerer Cybersecurity-Anbieter, von denen jeder unterschiedliche Funktionsbereiche abdeckte. Dies beginnt sich nun zu ändern, da sich der Markt konsolidiert und die OT-Cybersecurity-Anbieter beginnen, ein breiteres Funktionsspektrum in ihren Lösungen anzubieten. Diese Lösungen sind in eine besser integrierte Umgebung eingebettet, die als zentrale OT-Cybersecurity-Plattform eingesetzt werden kann. Für OT-Cybersecurity-Teams hat dies den

zusätzlichen Vorteil, dass sich die Zahl der Anbieter verringert, mit denen sie sich auseinandersetzen müssen. Da die verschiedenen Anbieter unterschiedliche Lizenzmodelle, Preisstrukturen und SLA-Konditionen anbieten, kann das Lieferantenmanagement bei einer großen Zahl von Anbietern schnell zu einem zeitaufwändigen und komplexen Prozess werden.

Plattformbasierte Ansätze für industrielle OT-Cybersecurity haben konkrete betriebswirtschaftliche Auswirkungen

Plattformbasierte Ansätze senken die Betriebskosten und lassen sich mit weniger Personal effektiver verwalten. Noch wichtiger ist, dass solche Plattformen die Bedrohungserkennung und -abwehr verbessern können. Sollte es dennoch zu einem Vorfall kommen, können diese Plattformen die Herausforderungen bei der Zusammenführung von IT und OT abfedern, indem sie die bisherigen, fragmentierten Einzelwerkzeuge für die Sicherheit durch eine einheitliche und integrierte Lösung ersetzen. Indem sie Datenmanagementsysteme (IT) mit Betriebstechnologie (OT) unter einer einzigen Managementkonsole integrieren, können Unternehmen die erhöhten Risiken vernetzter Systeme besser bewältigen und über die gesamte hybride Infrastruktur hinweg für Transparenz, Sicherheit und Compliance sorgen.

Diese Plattformen können zudem besser auf Vorfälle reagieren. Die eng integrierte Umgebung einer solchen Sicherheitsplattform, kombiniert mit einem umfassenden Überblick über potenzielle Bedrohungen im gesamten Unternehmen, sorgt dafür, dass Bedrohungen schneller erkannt werden können. Dies wiederum ermöglicht schnellere Abwehr- und Eindämmungsmaßnahmen. Die Plattform kann somit eine einheitliche, verlässliche Datenbasis schaffen, die für mehr Transparenz sorgt, bis hin zu älteren OT-Anlagen.

Wie das regulatorische Umfeld die Plattformisierung vorantreibt

Das regulatorische Umfeld für industrielle Cybersecurity verändert sich derzeit drastisch. Neue Vorschriften in der EU, im Nahen Osten, in Asien und in anderen Teilen der Welt werden die Investitionen in Anwendungen für industrielle Cybersecurity erheblich ankurbeln. Für die Fertigungsindustrie, also sowohl für die Prozessindustrie als auch für die diskrete Fertigung, bringt NIS2 erhebliche neue Pflichten und mögliche Haftungsrisiken mit sich. Die Richtlinie hebt Cybersecurity zu einer strategischen Notwendigkeit hervor, die von der Unternehmensleitung überwacht werden muss, und verlangt umfassende Sicherheitsmaßnahmen für IT- und OT-Umgebungen. Diese Compliance-Anforderungen machen erhebliche Investitionen in Cybersecurity-Infrastrukturen, -Prozesse und -Personalschulungen unumgänglich.

Viele Unternehmen bemühen sich derzeit intensiv um die Einhaltung dieser neuen Vorschriften, denn die EU ist für ihre strenge Rechtsdurchsetzung bekannt. Den Unternehmen bleibt nicht viel Zeit, um in Lösungen zu investieren, die die vielen benötigten Data-Protection- und Cybersecurity-Fähigkeiten auf einer einzigen Plattform integrieren. ARC erwartet, dass das Wachstum der Plattformisierung durch den Wettlauf um die Einhaltung dieser neuen Vorschriften weiter angetrieben wird.

Der Ansatz von Acronis für plattformbasierte Cybersecurity in OT-Umgebungen

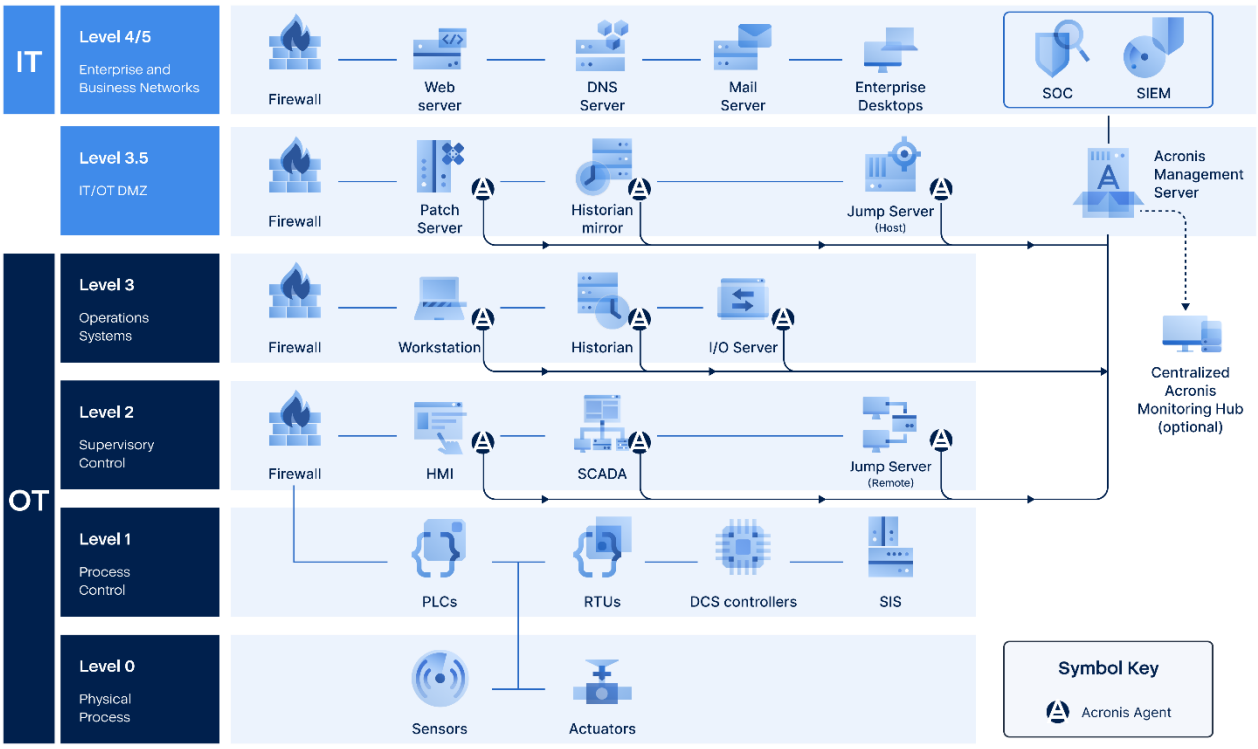
Acronis hat den Wandel vom Point-Solution-Anbieter zu einem echten Cybersecurity-Plattformanbieter erfolgreich vollzogen. Acronis ist ein Schweizer Unternehmen, das sich vom Entwickler traditioneller Backup-Programme zu einem umfassenden Cyber-Protection-Dienstleister entwickelt hat, der nativ integrierte Lösungen für Cybersecurity, Data Protection und Infrastrukturmanagement anbietet. Mit seiner vereinheitlichten Plattform, die sowohl IT- als auch OT-Umgebungen absichern kann, ist Acronis ein Vorreiter, wenn es um Plattformisierung und den Übergang von anlagenbezogenen zu unternehmensweiten Cybersecurity- und Data-Protection-Lösungen geht.

Die Wurzeln des Unternehmens liegen im Backup & Recovery-Bereich

Acronis begann als Unternehmen, das sich auf die Sicherung und Wiederherstellung von Daten konzentrierte. Eine solche Backup & Recovery-Funktionalität gehört zu den wichtigsten Aspekten der industriellen Cybersecurity. Wenn ein Vorfall eintritt oder die Produktion ausfällt, ist eine schnelle Wiederherstellung der Betriebsfähigkeit von entscheidender Bedeutung, denn jede verlorene Minute verursacht Umsatzverluste für das Unternehmen. Acronis True Image, das Flaggschiff unter den Prosumer-Produkten, wurde zum Industriestandard für Disk Imaging – also die Erstellung einer exakten Laufwerkskopie (auch Replikat genannt). Mit einer solchen Kopie können komplette Systeme wiederhergestellt werden, wenn die entsprechende Hardware ausfällt oder beschädigt wird. Die Entwicklung von Acronis zum OT-Cybersecurity-Anbieter wurde durch zwei Entwicklungen vorangetrieben: die Zusammenführung von IT- und industriellen Systemen sowie die Zunahme von Ransomware-Angriffen, bei denen zunehmend Backup-Dateien zum Angriffsziel wurden. Diese Ransomware-Varianten versuchen gezielt, Backup-Dateien zu finden und zu löschen, um den Opfern damit die Möglichkeit zu nehmen, ihre Daten ohne Zahlung der Lösegeldforderung wiederherzustellen.

Der Übergang von Backup & Recovery zu Active Protection

Dadurch hat Acronis erkannt, dass ein Backup allein nicht mehr ausreicht. Im Jahr 2017 führte Acronis eine aktive Anti-Ransomware-Technologie in seine Backup-Software ein. Dies war eine branchenweit einzigartige Neuerung, die erstmals „reaktive" Wiederherstellungsfähigkeiten mit „proaktiver" Bedrohungserkennung verband. Im Jahr 2020 brachte das Unternehmen dann Acronis Cyber Protect auf den Markt: eine All-in-one-Plattform, die Backup-, Disaster Recovery-, Antimalware- und Management-Funktionalitäten in einer Lösung integriert. Damit hatte das Unternehmen den Übergang zu einem Full-Service-Anbieter für Cyber Protection-Lösungen vollzogen.



*List of protected systems not exhaustive

Cyber Protect Local: Speziell für OT-Umgebungen entwickelt

2025 hat Acronis Cyber Protect Local eingeführt, eine On-Premise-Bereitstellung der einheitlichen Cyber-Protection-Plattform von Acronis, die speziell für Unternehmen entwickelt wurde. Mit dieser Lösung können Unternehmen selbst strenge gesetzliche Anforderungen an Datenhoheit und Compliance erfüllen und abgelegene und/oder per Air Gap isolierte Umgebungen schützen, wie sie beispielsweise bei Fertigungsunternehmen mit OT-Applikationen üblich sind. Acronis Cyber Protect Local vereint Backup-&-Recovery-, Cybersecurity- und Endpoint-Management-Fähigkeiten in einer einzigen Plattform. Es gehört zur umfassenderen Acronis-Cyber-Protect-17-Plattform, die die zentrale Verwaltung von IT- und OT-Umgebungen über eine zentrale, übersichtliche Managementkonsole ermöglicht.

Acronis hat bei der Entwicklung dieser Lösungen stets die besonderen Cybersecurity-Herausforderungen in OT-Umgebungen im Blick. Dazu gehört beispielsweise der Einsatz älterer Geräte, die oft in gemischten Umgebungen zusammen mit neuen Systemen laufen. Manche dieser Legacy-Systeme können 20 Jahre oder älter sein. In vielen Fabriken laufen immer noch veraltete Windows- und Linux-Betriebssysteme wie Windows XP oder noch ältere Versionen, deren offizieller Supportzeitraum längst abgelaufen ist. Viele dieser „End-of-Life"-Betriebssysteme, die von den jeweiligen Herstellern längst aufgegeben wurden, werden von Acronis jedoch weiterhin unterstützt.

Acronis verfolgt einen vereinheitlichten, agentenbasierten Cybersecurity-Ansatz und arbeitet mit einem einzelnen Agenten pro Endpunkt. In diesem einen Agenten sind dann alle Funktionalitäten (wie KI-gestützter Malware-Schutz, Schwachstellenbewertung und Backup) integriert. Dieser Ansatz ermöglicht Echtzeitschutz,

Verhaltenserkennung von Bedrohungen und umgehende Wiederherstellungen, was wiederum den Verwaltungsaufwand und die Risiken für Ransomware- und Zero-Day-Angriffe deutlich reduziert. Der Agent wird sowohl bei physischen als auch bei virtuellen Maschinen eingesetzt und unterstützt umfassende, granulare Sicherheits- und Data Protection-Funktionen. In Verbindung mit agentenlosen Ansätzen kann er zudem für Backups auf Hypervisor-Ebene genutzt werden.

Die Beziehungen von Acronis zu Anbietern von integrierten Automatisierungslösungen

Acronis unterhält enge Beziehungen zu den meisten großen Anbietern von integrierten Automatisierungslösungen (wie ABB, Emerson, Honeywell, Siemens, Rockwell, GE Vernova, Intel und Yokogawa). Das Unternehmen ist in deren Umgebungen eingebettet und die Partnerschaft wurde mittlerweile ausgeweitet, sodass jetzt auch Acronis Cyber Protect einbezogen ist.

Wie Acronis industrielle KI einsetzt

Acronis nutzt KI-gestützte Technologien und verhaltensbasierte Heuristiken, um auch komplexe Angriffsmuster analysieren und schädliches Verhalten in Echtzeit erkennen zu können. Dadurch können auch komplexe oder Zero-Day-Angriffe abgewehrt werden, die bei herkömmlichen, signaturbasierten Ansätzen leicht übersehen werden. Bei der „Active Protection"-Technologie kommt eine spezielle KI zum Einsatz, die Ransomware-Angriffe erkennen und Verschlüsselungsversuche unterbinden kann, indem sie Prozesse auf bestimmte Schreib-/Lese-Muster überwacht.

Festlegen einer Basislinie für die normale Systemleistung und Verhaltensanalyse

Acronis Cyber Protect nutzt insbesondere für seine Active Protection-Funktion künstliche Intelligenz, um Systemprozesse kontinuierlich auf anomales oder schädliches Verhalten zu überwachen, das auf Ransomware-Angriffe hindeuten könnte. Durch die Analyse von Stack-Traces (Aufrufstapeln) und das Festlegen von Referenzwerten für normales Systemverhalten kann die Lösung Ransomware und andere Malware (einschließlich Zero-Day-Angriffen) erkennen und stoppen, bevor Daten verschlüsselt werden. Dieser Ansatz ist besonders für OT-Systeme wichtig, die oft anfällig für neue Angriffsvektoren sind, die von herkömmlichen signaturbasierten Erkennungsmethoden nicht abgedeckt werden.

Über die Erkennung bekannter Bedrohungen hinaus konzentriert sich die Verhaltensanalyse von Acronis darauf, böswillige Absichten anhand des Verhaltens von Applikationen und Prozessen zu identifizieren, statt sich allein auf Signaturen zu verlassen. Dadurch kann Acronis unbekannte und neu auftretende Bedrohungen, einschließlich solcher, die Schwachstellen in älteren OT-Systemen ausnutzen, besser erkennen und entschärfen. Die KI-gestützte Threat Intelligence von Acronis sammelt Daten von Millionen von Endpunkten, um die entsprechenden ML-Modelle zu trainieren, mit denen Angriffe frühzeitig erkannt und proaktiv verhindert werden können. Maschinelles Lernen wird außerdem zur Überwachung der Festplattenintegrität (Drive Health Monitoring) eingesetzt. Durch die rechtzeitige Vorhersage von Festplattenausfällen können weitere Datenverluste und Ausfallzeiten verhindert werden.

Automatisierte Schadensabwehr und Schadensbehebung bei Sicherheitsvorfällen

Acronis setzt KI außerdem in seiner EDR-Lösung ein, um seine Vorfallsreaktionsfähigkeiten in OT-Umgebungen zu optimieren. Dadurch können die Erstbewertung von Vorfällen, deren Schweregradeinstufung und die Erstellung zielgerichteter Lösungsvorschläge automatisiert werden. Dank der KI-gestützten Angriffsanalyse können die zuständigen Sicherheitsanalyst:innen die jeweiligen Vorfälle besser verstehen und effizienter darauf reagieren. Die Lösungen von Acronis unterstützen außerdem die Erstellung zielgerichteter Skripte, um bei Angriffen schnell mit vordefinierten und automatisierten Gegenmaßnahmen reagieren zu können. Dadurch lassen sich Angriffe besonders schnell eindämmen und mögliche Schäden minimieren.

Fazit

Industrieunternehmen stehen unter zunehmendem Druck, ihre Umgebungen für Betriebstechnologie (OT) und Informationstechnologie (IT) zuverlässig vor hochentwickelten Cyberbedrohungen schützen zu müssen. Die Plattformisierung – also die Integration mehrerer Sicherheitsfunktionalitäten in einer einheitlichen Lösung – bietet erhebliche geschäftliche Vorteile. Durch die Konsolidierung der entsprechenden Tools und Prozesse können Unternehmen ihr Sicherheitsmanagement optimieren, die operative Komplexität reduzieren und die Transparenz über unterschiedliche Systeme hinweg verbessern. Dieser einheitliche Ansatz stärkt nicht nur die Sicherheitslage, sondern unterstützt auch die Einhaltung regulatorischer Vorgaben und die Kostenkontrolle. Damit wird er zu einem wichtigen Treiber der digitalen Transformation in industriellen Umgebungen.

Die Plattform von Acronis nutzt fortschrittliche KI-gestützte Technologien und spezielle Hardwarebeschleunigung, um bei geringem Ressourcenverbrauch eine optimale Leistung zu erzielen. Dies ist besonders in OT-Umgebungen wichtig, in denen Hardwareressourcen oft begrenzt sind, Effizienz und Zuverlässigkeit jedoch von entscheidender Bedeutung sind. Dank Acronis One-Click Recovery kann das Fachpersonal vor Ort ein ausgefallenes OT-System selbst wiederherstellen. Besondere Fachkenntnisse oder dedizierter IT-Support sind dafür nicht erforderlich. Der ganzheitliche Ansatz der Acronis-Plattform ermöglicht eine nahtlose Integration in bestehende Infrastrukturen sowie einen umfassenden Schutz vor einer Vielzahl von Bedrohungen, einschließlich Ransomware- und Zero-Day-Angriffen.

Zusammenfassend markiert der Einsatz von KI in der industriellen Cybersecurity einen Wendepunkt hin zu Verteidigungsstrategien, die vorausschauend und anpassungsfähig sind. Denn KI-gestützte Tools können fortlaufend aus neu auftretenden Bedrohungen lernen, die Resilienz stärken und Unternehmen helfen, ihren Angreifern immer einen Schritt voraus zu bleiben. Da Industrieanlagen immer stärker vernetzt und komplexer werden, ist KI unverzichtbar, um die Sicherheit aufrechtzuerhalten, Ausfallzeiten zu minimieren und weitere Innovationen in der Branche zu ermöglichen.

Für weitere Informationen oder um Feedback zu diesem Artikel zu geben, wenden Sie sich bitte an Ihren Account Manager oder an den Autor unter lobrien@arcweb.com*. Die ARC Insights werden von der ARC Advisory Group veröffentlicht und sind urheberrechtlich geschützt. Diese Informationen sind Eigentum von ARC, und kein Teil davon darf ohne vorherige Genehmigung von ARC vervielfältigt werden.*