



Più di un terzo delle organizzazioni industriali considera il rischio di cybersecurity uno dei principali ostacoli alla crescita, secondo un nuovo studio globale

## Descrizione

COMUNICATO STAMPA - CONTENUTO PROMOZIONALE

Le aziende industriali incrementano gli investimenti in cybersecurity mentre la crescente connettività delle operations, l'adozione dell'AI e la convergenza IT/OT aumentano il rischio operativo

MILWAUKEE, 22 settembre 2026 /PRNewswire/ - Rockwell Automation, Inc. (NYSE: ROK), la principale azienda mondiale di automazione industriale e trasformazione digitale, ha pubblicato oggi "Operational Resilience in the Age of Connectivity", un report di approfondimento sul settore basato sul contributo di 1.500 responsabili decisionali delle attività produttive e delle operations industriali in 17 Paesi. La ricerca rivela un divario tra la fiducia in una protezione completa della sicurezza informatica e il rischio operativo. Sebbene le organizzazioni industriali stiano investendo nella sicurezza informatica, tali investimenti non si traducono automaticamente in resilienza operativa.

Man mano che le organizzazioni continuano a connettere i sistemi IT e OT, a estendere su larga scala le iniziative di AI e a espandere l'uso dei dati operativi a livello aziendale, aumenta l'esposizione al rischio cyber. Infatti, più di un terzo delle organizzazioni industriali considera il rischio di cybersecurity uno dei maggiori ostacoli esterni alla crescita, sottolineando la necessità di rafforzare la resilienza in un contesto caratterizzato da una connettività sempre maggiore.

I risultati principali del rapporto includono:

Le organizzazioni industriali sono consapevoli che la cybersecurity influisce direttamente su uptime, continuità operativa, produttività e crescita, ma i soli investimenti tecnologici non creano resilienza operativa o fiducia nella postura di sicurezza di un'organizzazione, ha affermato Rick Kaun, direttore globale dei servizi di cybersecurity presso Rockwell Automation. La vera resilienza si costruisce quando la sicurezza informatica diventa parte integrante della strategia aziendale. Le organizzazioni che gestiscono in modo proattivo il rischio e si preparano ad affrontare eventuali

interruzioni sono nella posizione migliore per proteggere le operazioni, assicurare la continuità nella produzione e ottenere un vantaggio competitivo.â•

Il report completo â•?Operational Resilience in the Age of Connectivityâ•? Ã• disponibile QUI e analizza come le organizzazioni industriali stiano rafforzando la cybersecurity, gestendo la convergenza IT/OT e sviluppando una maggiore resilienza operativa in un ambiente sempre piÃ¹ connesso.

Domande frequenti: Cos'Ã• la resilienza operativa? La resilienza operativa Ã• la capacitÃ di un'organizzazione di sostenere operazioni industriali sicure, protette e affidabili gestendo proattivamente il rischio, limitando le discontinuitÃ operative e garantendo un rapido ripristino dagli incidenti.

PerchÃ© la convergenza IT/OT sta aumentando il rischio di cybersicurezza? La convergenza IT/OT aumenta il rischio di cybersicurezza perchÃ© espande la superficie di attacco, introduce nuovi punti di connettivitÃ e consente a minacce che hanno origine in ambienti IT di avere un potenziale impatto sulle operazioni industriali. PoichÃ© dati operativi, sistemi, utenti e connessioni di terze parti diventano sempre piÃ¹ interconnessi, un singolo incidente informatico puÃ² avere conseguenze piÃ¹ ampie su produzione, sicurezza, qualitÃ e continuitÃ operativa.

In che modo le organizzazioni industriali utilizzano l'AI per la cybersecurity? Secondo la ricerca, il 45% delle organizzazioni industriali prevede di applicare l'AI e il machine learning alla cybersecurity nei prossimi 12 mesi per contribuire a migliorare le capacitÃ di rilevamento, monitoraggio e gestione del rischio.

Metodologia Il report analizza il feedback di 1.560 intervistati in 17 dei principali Paesi manifatturieri, con ruoli che spaziano dal management al C-suite, ed Ã• stato condotto da Sapio Research in collaborazione con Rockwell Automation. Il sondaggio ha preso in esame una serie di settori industriali, tra cui quello dei prodotti di consumo confezionati, (CPG) dell'industria alimentare, dell'automotive, dei semiconduttori, dell'energia, delle scienze della vita e altri ancora. Grazie a una distribuzione bilanciata di aziende di diverse dimensioni, con fatturati compresi tra i 100 milioni e oltre 30 miliardi di dollari, offre un'ampia panoramica delle prospettive del settore manifatturiero.

Informazioni su Rockwell Automation Rockwell Automation, Inc. (NYSE: ROK), Ã• leader mondiale nell'automazione industriale e nella trasformazione digitale. Connettiamo l'immaginazione delle persone al potenziale della tecnologia per espandere ciÃ² che Ã• umanamente possibile, rendendo il mondo piÃ¹ produttivo e piÃ¹ sostenibile. Rockwell Automation, con sede a Milwaukee, Wisconsin, conta circa 26.000 dipendenti impegnati a supportare i nostri clienti in oltre 100 Paesi, secondo i dati di fine anno fiscale 2025. Per saperne di piÃ¹ su come stiamo realizzando The Connected Enterprise® nelle imprese industriali, visitate il sito [www.rockwellautomation.com](http://www.rockwellautomation.com).

View original content to download multimedia: <https://www.prnewswire.com/it/comunicati-stampa/piu-di-un-terzo-delle-organizzazioni-industriali-considera-il-rischio-di-cybersecurity-uno-dei-principali-ostacoli-alla-crescita-secondo-un-nuovo-studio-globale-302885238.html>

Copyright 2026 PR Newswire. All Rights Reserved.

---

COMUNICATO STAMPA - CONTENUTO PROMOZIONALE: Immediapress - un servizio di diffusione di comunicati stampa in testo originale redatto direttamente dall'ente che lo emette. Adnkronos e Immediapress non sono responsabili per i contenuti dei comunicati trasmessi

-

[immediapress/pr-newswire](https://immediapress/pr-newswire)

### Categoria

1. Comunicati

### Tag

1. ImmediaPress

### Data di creazione

Settembre 22, 2026

### Autore

redazione

default watermark