

Resilienza operativa nell'era della connettività

Nuova ricerca sulla preparazione alla sicurezza informatica negli ambienti di produzione connessa

Rockwell Automation

La nuova realtà della Sicurezza OT

Le aziende industriali stanno connettendo più sistemi, scalando l'IA più velocemente e spingendo le operazioni a muoversi in tempo reale. Quegli investimenti creano velocità e flessibilità. Inoltre espandono il rischio operativo.

Nuovi dati di Rockwell Automation mostrano una discrepanza tra la fiducia e l'esposizione operativa.

Quasi la metà delle organizzazioni (46%) ha subito un incidente informatico nell'ultimo anno, eppure il 90% si dichiara fiducioso di poterlo contenere. Più di un terzo (34%) identifica la sicurezza informatica come uno dei maggiori ostacoli esterni alla crescita per i prossimi 12 mesi.

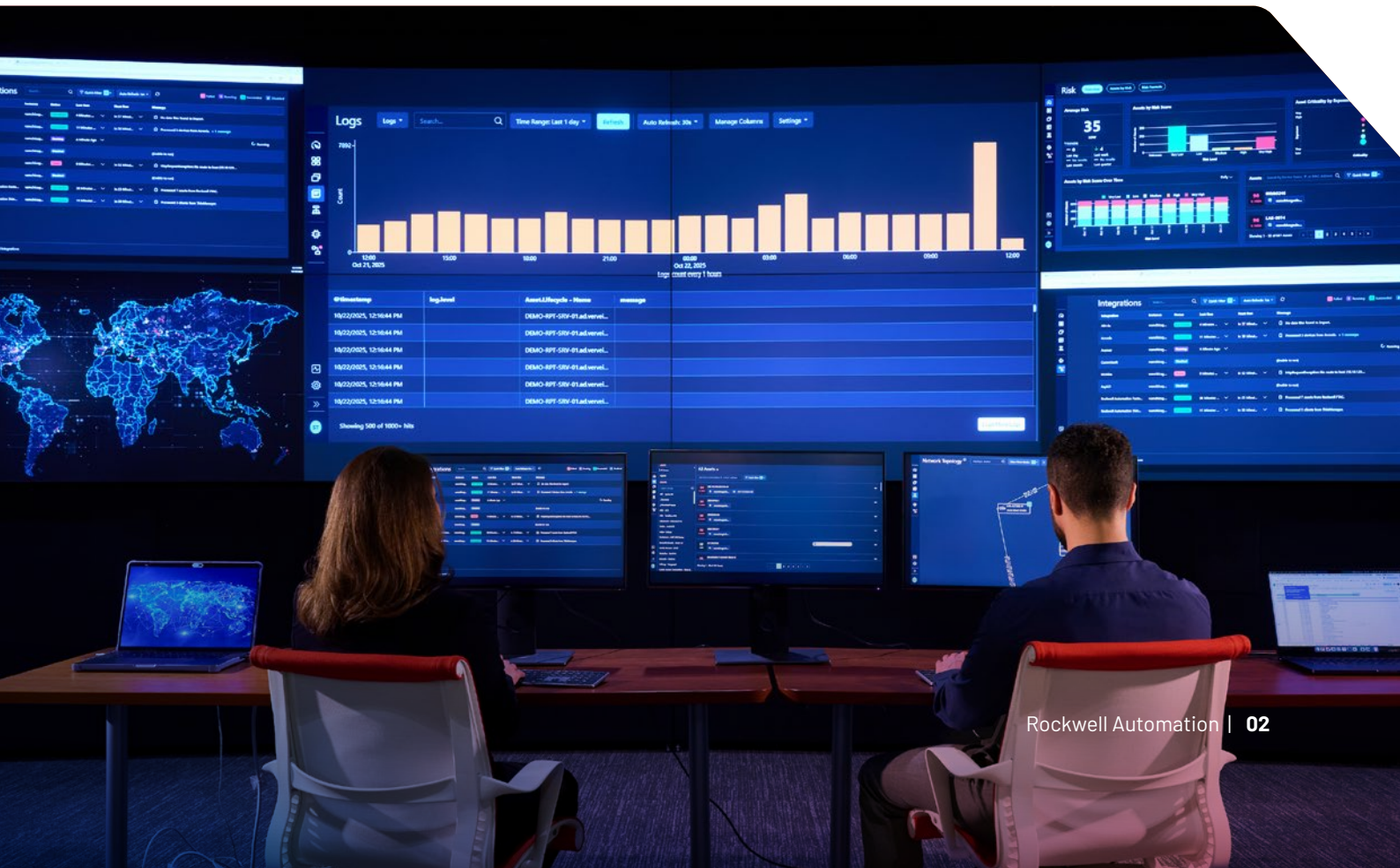
Nonostante ciò, le organizzazioni comprendono la posta in gioco e stanno agendo per rafforzare la propria resilienza e fiducia. Il 62% ha già investito in piattaforme di cybersicurezza come l'inventario degli asset, i sistemi di rilevamento delle intrusioni e l'accesso remoto sicuro. La sicurezza informatica si è inoltre classificata tra le principali tecnologie che hanno generato un ROI negli ultimi 12 mesi.

La questione non è la consapevolezza. Le organizzazioni industriali sanno che il rischio informatico influisce su tempi di attività, continuità operativa, produttività e crescita. La sfida deriva dalla messa in sicurezza di operazioni che continuano a diventare sempre più connesse e complesse.

L'adozione dell'IA continua a crescere. Gli ambienti IT e OT continuano a convergere. Il flusso dei dati operativi include sempre più asset, utenti, dispositivi e applicazioni che mai. Ogni connessione crea un'altra dipendenza. Ogni connessione crea un altro punto di esposizione.

La buona notizia è che le organizzazioni si stanno dimostrando all'altezza della sfida. Non considerano più la cybersecurity come un'iniziativa IT separata, ma la vedono sempre più come parte delle prestazioni operative.

Le aziende che guideranno la prossima fase delle operazioni industriali saranno quelle che costruiranno visibilità, architettura sicura e capacità di risposta in grado di mantenere attiva la produzione durante le interruzioni.



Cresce la fiducia grazie agli investimenti – ma è abbastanza?

Le organizzazioni non sono statiche. Stanno investendo nelle tecnologie, nelle architetture e nelle capacità necessarie per rafforzare la resilienza informatica. Il passo successivo è riunire tali investimenti in un programma di cybersicurezza che migliori continuamente la visibilità, riduca il rischio e si adatti alle mutevoli esigenze operative. I dati mostrano dove si stanno concentrando le organizzazioni oggi.

I risultati principali includono:

- I punti di integrazione IT/OT sono classificati come tra i più vulnerabili agli incidenti informatici, subito dopo i sistemi IT/le reti aziendali. Inoltre, gli investimenti in cybersicurezza hanno generato uno dei più alti ROI negli ultimi 12 mesi
- La sicurezza informatica è il secondo fattore di ROI tra gli investimenti tecnologici

Questi risultati indicano un chiaro cambiamento: le organizzazioni stanno integrando la cybersicurezza in strategie di trasformazione digitale più ampie, insieme a intelligenza artificiale, automazione, tecnologie cloud e operazioni connesse. Ma man mano che gli ambienti diventano più interconnessi, la resilienza dipende dalla capacità delle organizzazioni di tradurre gli investimenti in azioni coordinate.



62%

hanno già investito in piattaforme di sicurezza informatica

45%

prevedono di utilizzare l'IA e l'apprendimento automatico per la sicurezza informatica nei prossimi 12 mesi

35%

Più di un terzo delle organizzazioni industriali identifica la cybersecurity come uno dei maggiori ostacoli esterni alla crescita, secondo solo alla carenza di manodopera nei prossimi 12 mesi.

37%

affermano che la messa in sicurezza dell'architettura IT/OT porterà a risultati di business positivi nei prossimi cinque anni

Gestire operazioni OT resilienti

Le aziende industriali hanno compiuto progressi significativi investendo nella sicurezza informatica. La prossima sfida è trasformare tali investimenti in resilienza operativa.

Una sicurezza OT resiliente richiede più che semplici strumenti e soluzioni mirate. Richiede un approccio proattivo end-to-end, allineato a framework e standard riconosciuti a livello globale come NIST, NIS2 e IEC 62443. Ciò offre alle organizzazioni un modo strutturato per migliorare la maturità della sicurezza e al contempo soddisfare i requisiti normativi.

Le seguenti capacità evidenziano le azioni intraprese dalle organizzazioni leader e mostrano come ciò avviene in pratica.



Consulenza strategica

Costruisci una strategia di cybersecurity basata sul rischio

La resilienza della cybersicurezza inizia con la comprensione del rischio nel contesto delle priorità operative, degli obiettivi di business e della realtà organizzativa. Prima di poter ridurre efficacemente i rischi, migliorare la resilienza o soddisfare i requisiti di conformità, le organizzazioni devono avere una visione chiara della loro attuale postura di cybersecurity e delle lacune che presentano gli impatti maggiori. Senza tali fondamenta, gli investimenti nella cybersecurity possono diventare frammentati, reattivi e difficili da rendere operativi.

Le organizzazioni che implementano servizi di consulenza strategica possono:

- Identificare i rischi, stabilire le priorità e allineare gli investimenti con i risultati di business
- Sostituire le decisioni di sicurezza reattive e ad hoc con una roadmap basata sul rischio e su priorità definite, in linea con gli obiettivi operativi e di business.
- Comprendere l'esposizione attuale a livello di asset, vulnerabilità, processi e pratiche di governance, consentendo di concentrare le risorse laddove avranno il maggiore impatto.
- Migliorare la preparazione alla conformità identificando le lacune di sicurezza e allineando gli interventi di risoluzione agli standard e ai requisiti applicabili
- Creare un allineamento interno tra IT, OT e leadership basato su una comprensione condivisa del rischio, delle priorità e di risultati di sicurezza misurabili

Infrastrutture e reti industriali

Le organizzazioni continuano a modernizzare l'architettura IT/OT man mano che le operation diventano più connesse. Sebbene ogni nuova connessione aumenti il rischio informatico, un'architettura difendibile aiuta a evitare che la complessità si trasformi in una superficie di attacco estesa. Le organizzazioni leader che integrano la sicurezza informatica nella progettazione delle proprie attività sono in una posizione migliore per ridurre i rischi, migliorare la resilienza e dedicare meno tempo a rispondere agli incidenti e più tempo a promuovere i risultati operativi.

Le organizzazioni proattive possono:

- Portare avanti le iniziative di trasformazione digitale con sicurezza, contribuendo a proteggere i sistemi operativi critici
- Riduci la probabilità e l'impatto delle interruzioni attraverso la segmentazione della rete per contenere le minacce prima che colpiscano la produzione
- Abilita un accesso remoto sicuro che supporti la flessibilità operativa, la produttività e la collaborazione senza creare punti di ingresso non gestiti.
- Implementare architetture secure-by-design che riducano il rischio lungo tutto il ciclo di vita degli asset
- Ridurre i costi di sicurezza a lungo termine affrontando i rischi in modo proattivo attraverso l'architettura e la progettazione anziché con interventi di risoluzione reattivi

Inventario degli asset e gestione del ciclo di vita

Ottenere visibilità su asset e rischi

La visibilità limitata è una delle barriere più comuni alla costruzione della resilienza. Senza una visione completa dell'ambiente – inclusi i sistemi legacy, i dispositivi connessi in serie o le connessioni temporanee – le organizzazioni non dispongono del punto di partenza necessario per pianificare ed eseguire una significativa riduzione del rischio.

La visibilità completa degli asset consente alle organizzazioni di:

- Comprendere e dare priorità al rischio informatico in tutto l'ambiente operativo
- Riduci i punti ciechi che possono creare rischi operativi, di sicurezza e di cybersecurity
- Prendi decisioni più rapide e consapevoli comprendendo quali asset sono connessi, quali sono esposti a rischi e quali sono più critici per la produzione e le operazioni aziendali.
- Accelerare la riduzione dei rischi dando priorità alle attività di risoluzione in base all'impatto operativo, non solo alla gravità della vulnerabilità.
- Migliorare la resilienza operativa attraverso una gestione continua del ciclo di vita degli asset che aiuta a mantenere un ambiente sicuro e supportato nel tempo
- Fare affidamento sulle fondamenta del programma per sviluppare controlli di compensazione e altri componenti per una cybersicurezza end-to-end

Gestione dei rischi e delle vulnerabilità

Dai priorità e risolvi i rischi che contano di più

Le organizzazioni non possono eliminare tutti i rischi informatici, ma possono migliorare la propria postura di sicurezza rafforzando la rapidità con cui identificano, assegnano le priorità e rispondono alle minacce prima che queste abbiano un impatto sulle operazioni.
Man mano che le operazioni industriali diventano più connesse, una gestione dei rischi efficace dipende dalla visibilità contestuale, da un processo decisionale basato sul rischio e dal mantenimento della continuità operativa nonostante le criticità.

Un programma di gestione delle vulnerabilità basato sul rischio aiuta le organizzazioni a:

- Dai priorità alla remediation in base all'impatto operativo, non solo ai punteggi di severità
- Ridurre il tempo medio di ripristino per gli asset OT
- Dimostrare un progresso misurabile di conformità rispetto a IEC 62443, NIST CSF e NIS2
- Consentire decisioni di investimento informate allineando gli investimenti in cybersecurity alla tolleranza al rischio aziendale e agli obiettivi operativi

Rilevamento e risposta gestiti

Mantenere una consapevolezza continua in tutte le operazioni

Poiché gli ambienti IT e OT diventano sempre più interconnessi, le organizzazioni affrontano una sfida crescente nel distinguere i normali eventi di sicurezza dalle minacce che potrebbero interrompere le operazioni. Il monitoraggio continuo aiuta a comprendere i rischi più importanti prima che causino interruzioni.

Un programma proattivo di rilevamento e risposta aiuta le organizzazioni a:

- Accelera il rilevamento e la risposta mantenendo un monitoraggio 24/7 e una visibilità continua negli ambienti IT e OT
- Consentire un processo decisionale più rapido e informato con insight contestuali che aiutano i team a comprendere quali minacce richiedono un'azione immediata
- Colmare il divario di competenze migliorando le capacità interne con un'esperienza dedicata alla sicurezza OT, senza i costi di creazione e mantenimento di un SOC interno completo
- Rafforzare l'efficacia del programma integrando il rilevamento delle minacce con la gestione delle vulnerabilità, la risposta agli incidenti, la governance e le iniziative di miglioramento continuo

Risposta agli incidenti e ripristino

Contenere, ripristinare e migliorare

Quando si verifica un incidente di cybersecurity, una risposta rapida è fondamentale per determinare l'entità dei danni, dei tempi di inattività e dei costi che un'organizzazione potrebbe dover affrontare. Contenere un incidente è solo una parte della sfida. Le organizzazioni devono comprendere l'importanza della prontezza al ripristino quando si tratta di resilienza operativa. Quando si verifica il peggio, devono avere la capacità di ripristinare rapidamente i servizi e tornare alle normali operazioni.

Un programma maturo di risposta agli incidenti consente alle organizzazioni di:

- Ridurre l'impatto degli incidenti informatici attraverso procedure di risposta e contenimento predefinite e testate
- Accelerare il ripristino operativo coordinando la risposta e il recupero tra i team IT, OT e operativi
- Riduci al minimo i tempi di inattività migliorando la prontezza di ripristino per i sistemi critici
- Rafforzare la fiducia degli stakeholder attraverso una comunicazione chiara, la governance e la gestione degli incidenti durante e dopo un evento
- Sviluppare un'indagine dettagliata sull'incidente per identificare la causa radice e applicare le lezioni apprese per rafforzare continuamente la resilienza informatica



La resilienza sta diventando un vantaggio competitivo

Le organizzazioni industriali stanno investendo molto nella cybersecurity, nell'IA e nelle operazioni connesse. Quegli investimenti stanno aumentando la fiducia, ma la tecnologia da sola non crea resilienza.

Le organizzazioni che traggono il maggior valore dalla cybersicurezza saranno quelle che adottano un approccio proattivo e programmatico. Integrando visibilità, processi decisionali basati sul rischio, architetture sicure, monitoraggio continuo e preparazione al ripristino nelle loro operazioni fin dall'inizio, possono ridurre il rischio operativo, sostenere la produzione e consentire all'azienda di progredire con fiducia.

In un ambiente industriale più connesso, la cybersecurity non riguarda più solo la protezione degli asset. Si tratta di abilitare operazioni resilienti in grado di adattarsi, ripristinarsi e continuare a fornire valore di business.

Per ulteriori informazioni, contattare il rappresentante Rockwell Automation di zona.

Rockwell Automation

Contattaci su.

rockwellautomation.com — expanding **human possibility**®

AMERICHE: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000
EUROPA/MEDIO ORIENTE/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgio, Tel: (32) 2 663 0600
ASIA PACIFICO: Rockwell Automation SEA Pte Ltd, 2 Corporation Road, #04-05, Main Lobby, Corporation Place, Singapore 618494, Tel: (65) 6510 6608
ITALIA: Rockwell Automation S.r.l., Via Ludovico di Breme 13 A, 20156 Milano, Tel: +39 02 334471, www.rockwellautomation.it
SVIZZERA:Rockwell Automation AG, Via Cantonale 27, 6928 Manno, Tel: 091 604 62 62, Customer Service: Tel: 0848 000 279

Allen-Bradley ed expanding human possibility sono marchi commerciali di Rockwell Automation, Inc.
I marchi commerciali non appartenenti a Rockwell Automation sono di proprietà delle rispettive società.

Pubblicazione GMSN-SP043A-IT-P - Agosto 2026

Copyright © 2026 Rockwell Automation, Inc. Tutti i diritti sono riservati. Stampato negli USA.