Acronis
Cyber Protect per il settore petrolifero e del gas, dell'elettricità e dell'energia

Resilienza digitale pensata appositamente per operazioni industriali critiche

Sintesi riepilogativa

Le operazioni nel settore petrolifero e del gas, dell'elettricità e dell'energia dipendono da sistemi di tecnologia operativa (OT) basati su PC per la produzione, la trasmissione e la distribuzione in sicurezza dell'energia. Questi ambienti presentano vincoli esclusivi: sistemi legacy con ciclo di vita lungo, siti con connettività limitata e bassa tolleranza alle interruzioni operative. Al contempo, si registra un aumento degli attacchi ransomware mirati alle tecnologie OT.

Acronis Cyber Protect per OT è progettato per fornire backup sicuro, ripristino rapido e resilienza operativa per i sistemi OT, senza interrompere la produzione. La soluzione aiuta le organizzazioni a ripristinare stati di sistema convalidati, ridurre i tempi di ripristino e supportare i requisiti di ripristino e audit più comuni degli standard di cyber security industriale.

Scelto dai fornitori di automazione

YOKOGAWA · Honeywell · GE VERNOVA · ABB · EMERSON

Perché scegliere Acronis per il settore petrolifero e del gas, dell'energia e dell'elettricità

- Agente a impatto ridotto
- Operatività offline/ air-gapped
- Ripristino bare-metal veloce
- Convalida del backup/ scansione anti-malware
- Ripristino con un clic
- Supporto per sistemi operativi legacy
- Universal Restore
- Storage immutabile + replica + crittografia

Acronis Cyber Protect per OT è stato appositamente sviluppato per soddisfare le priorità dell'OT: disponibilità, praticità, ripristino, prevenzione, ambienti legacy reali e ambienti misti, oltre a flussi di lavoro di ripristino gestiti dagli operatori per ambienti remoti e con risorse limitate.

Valore per l'azienda

Valore operativo

- Ridurre al minimo il tempo medio di ripristino (MTTR) per i sistemi OT critici.
- Mantenere la continuità produttiva.
- Ridurre il rischio ripristinando stati di sistema convalidati.

Protezione del brand e dai rischi

- Ridurre la probabilità di ripristini non sicuri o compromessi.
- Dimostrare la resilienza digitale e la preparazione al ripristino alla governance interna, ai Partner e agli enti regolatori.

Incidenza sul costo totale di proprietà (TCO)

- Contenere le spese operative riducendo al minimo le interruzioni e semplificando il ripristino dei sistemi OT critici.
- Ottimizzare le spese di capitale estendendo il ciclo di vita delle risorse legacy e facilitando il ripristino su hardware sostitutivo.

Valore per OEM e Partner

- Integrare la resilienza nei sistemi forniti.
- Ridurre le attività di supporto dopo l'implementazione.
- Ottenere ricavi ricorrenti tramite servizi di resilienza e supporto del ciclo di vita.

Settori interessati

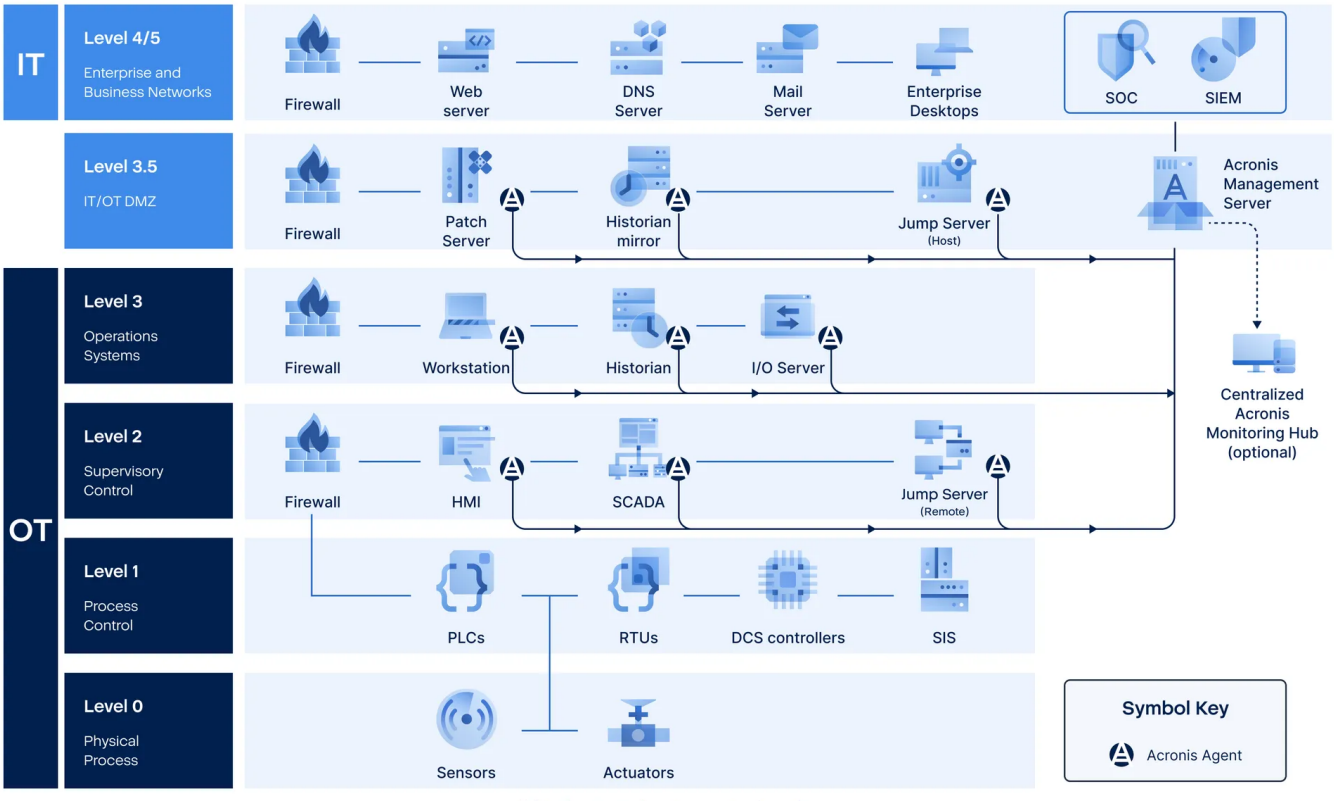
Energia ed elettricità		
Produzione di energia termica, nucleare, idroelettrica, eolica, solare, da biomasse e da rifiuti (termovalorizzazione).	Trasmissione e distribuzione (reti di trasmissione, inclusi i sistemi HVDC, le sottostazioni, le reti di distribuzione).	Rete periferica ed energia distribuita (risorse energetiche distribuite (DER), microreti, sistemi di accumulo a batteria (BESS)).
Petrolio e gas		
Upstream (esplorazione, perforazione, produzione offshore/onshore, produzione di gas naturale e trattamento sul campo).	Midstream (compressione e trasporto del gas, trasporto tramite pipeline, terminali di stoccaggio, liquefazione e spedizione del GNL).	Downstream (raffinazione, produzione chimica e petrolchimica, conversione da gas a liquidi (GTL), rigassificazione del GNL).

Le sfide operative degli ambienti OT del settore petrolifero, del gas e dell'energia

Sfida	Perché è importante
Costo elevato delle interruzioni operative	Le interruzioni possono generare rischi per la sicurezza, perdita di produttività, interruzione dei servizi e conseguenze normative. Il ripristino rapido è fondamentale.
Sfide legate alla cyber security	Ransomware e attacchi informatici mirati colpiscono sempre più spesso sistemi SCADA, HMI, historian, workstation per l'ingegneria e altri sistemi OT critici.
Siti air-gapped e con connettività limitata	Nei siti remoti e distribuiti, la connettività può essere limitata. Poiché la continuità produttiva, le reti segmentate e i sistemi legacy complicano l'applicazione delle patch, backup e ripristino devono funzionare a livello locale.
Sistemi operativi e hardware legacy	Molti sistemi OT eseguono versioni di Windows e/o Linux datate o immagini vincolate al fornitore, creando scenari in cui gli aggiornamenti sono rischiosi o non consentiti.
Sistemi fragili e deterministici	Criticità delle operazioni: gli ambienti OT esigono un controllo rigoroso su riavvii, aggiornamenti software, distribuzione degli agenti e modifiche alla configurazione. La protezione non può essere invasiva, ma deve essere prevedibile e sicura dal punto di vista operativo.
Supporto IT in sede limitato	I siti distribuiti sono spesso gestiti da operatori o ingegneri OT. In assenza del supporto IT in sede, i ripristini devono essere semplici e rapidi.
Requisiti di conformità e garanzia	Gli operatori devono far fronte alle crescenti aspettative in termini di preparazione al ripristino, prove per gli audit e garanzia dei fornitori, in linea con i framework di cyber security del settore.
Vincoli con i fornitori	Software OEM proprietari, immagini con licenza e configurazioni specifiche per hardware limitano la flessibilità, aumentano i costi e complicano la migrazione, il ripristino e la ricostruzione dei sistemi.

Sistemi e dati protetti da Acronis Cyber Protect

Area dell'ambiente OT	Sistemi protetti	Dati protetti
Principali sistemi OT e ICS	Server/client SCADA, workstation HMI, stazioni operatore DCS, workstation di ingegneria, sistemi historian, server applicativi OT.	Immagini del sistema operativo, stack di applicazioni, configurazioni SCADA/HMI, database historian, logica degli allarmi, parametri operativi.
Infrastruttura per l'energia	PC di controllo delle sottostazioni, server HVDC/FACTS, controller per DER/microreti, controller per siti di sistemi BESS, server di gestione della ricarica per veicoli elettrici.	Software di controllo del sito, file di configurazione, dataset operativi, driver dei dispositivi, immagini di ripristino.
Operazioni petrolio e gas	Server di monitoraggio delle pipeline, sistemi di rilevamento perdite, sistemi DCS/SCADA di raffineria, PC di controllo per turbomacchine, sistemi di misura fiscale.	Configurazioni di processo, dati di monitoraggio, file di calibrazione/taratura, registrazioni operative.
Ingegneria e digitalizzazione	PC di ingegneria, workstation CAD/CAM, sistemi di simulazione, server di gestione delle risorse, piattaforme digital twin.	File, disegni e modelli dei progetti di ingegneria, documentazione, repository di configurazione, dati di progetto coperti da proprietà intellettuale.
Sistemi OT DMZ e di supporto	Jump host, server di acquisizione dati, server di autenticazione/sicurezza, sistemi intermedi OT/IT.	Configurazioni dei gateway di accesso, registri, immagini di sistema, dati di policy/configurazione.



*List of protected systems not exhaustive

Visibilità SIEM e SOC: l'integrazione SIEM in locale di Acronis inoltra gli avvisi e gli eventi relativi a backup, sicurezza e RMM ai sistemi SIEM di terzi tramite syslog o esportazione di file, aiutando così i team OT e della sicurezza a centralizzare il monitoraggio e la visibilità sugli incidenti negli ambienti protetti.

In che modo Acronis protegge i sistemi OT

Backup ottimizzato per sistemi OT: backup completo dell'immagine e di file a basso impatto, adatto ai sistemi OT in funzione; non richiede interruzioni operative pianificate nella maggior parte delle implementazioni.

Progettato per siti segmentati e air-gapped: supporta il funzionamento offline e lo storage locale (SAN/NAS/aree di storage dedicate) e può essere distribuito in linea con la segmentazione della rete OT e la connettività limitata.

Ripristino sicuro e verificato: convalida del backup e controlli di integrità, oltre alla scansione facoltativa del malware nei punti di ripristino, per evitare di ripristinare sistemi compromessi.

Ripristino rapido gestito dall'operatore: flussi di lavoro di ripristino guidati e semplificati per i siti con personale IT limitato, che consentono ai team locali di ripristinare i sistemi quando l'accesso remoto non è disponibile.

Ripristino indipendente dall'hardware: ripristino su hardware nuovo o diverso (inclusi P2P, P2V e V2P)* per mantenere l'operatività quando i PC industriali originali sono obsoleti o non disponibili.

Supporto per sistemi OT safety-critical e SIS

Nelle operazioni del settore del petrolio, del gas e dell'energia, la priorità è chiara: la sicurezza al primo posto. I sistemi strumentati di sicurezza (SIS), tra cui le piattaforme come Triconex, DeltaV SIS e Honeywell Safety Manager, dipendono da sistemi basati su PC: workstation di ingegneria, repository di configurazione, sistemi di manutenzione, sistemi di documentazione, interfacce di sistemi historian e server di supporto che garantiscono la sicurezza delle operazioni.

Acronis Cyber Protect per OT è incentrato sulla protezione e sul ripristino di questi sistemi di supporto basati su PC. Facilitando il ripristino a uno stato convalidato e sicuro dopo guasti hardware, compromissioni, attacchi ransomware o interruzioni operative, Acronis supporta la resilienza digitale degli ambienti OT safety-critical, mantenendo al contempo una netta distinzione tra resilienza digitale e sicurezza funzionale.

Con Acronis, proteggi qualsiasi sistema OT basato su PC, da XP fino ai più recenti

Acronis supporta i vecchi sistemi operativi per PC che altri fornitori hanno abbandonato:

Windows

- Windows Server 2003 SP1, R2 e successivi, 2008/2008 R2, 2012/2012 R2, 2016, 2019, 2022 (tutte le opzioni di installazione eccetto Nano)
- Windows Small Business Server 2003/2003 R2, 2008, 2011
- Windows Home Server 2011
- Windows MultiPoint Server 2010, 2011, 2012
- Windows Storage Server 2003, 2008/2008 R2, 2012/2012 R2, 2016
- Windows XP Professional SP1, SP2, SP3
- Windows 7, 8/8.1, 10 (eccetto RT), 11 (tutte le edizioni)

Linux

- Kernel da 2.6.9 a 5.19
- RHEL 4.x, 5.x, 6.x, 7.x, 8.x*, 9.0*, 9.1*, 9.2*, 9.3*
- Ubuntu 9.10 - 23.04
- Fedora 11 - 31
- SUSE Linux Enterprise Server 10, 11, 12, 15
- Debian 4.x, 5.x, 6.x, 7.0, 7.2, 7.4-7.7, 8.0-8.8, 8.11, 9.0- 9.8, 10.x, 11.x
- CentOS 5.x, 6.x, 7.x, 8.x*
- Stream 8*, 9*
- Oracle Linux 5.x, 6.x, 7.x, 8.x*, 9.0*, 9.1*, 9.2*, 9.3*
- CloudLinux 5.x, 6.x, 7.x, 8.x*
- ClearOS 5.x, 6.x, 7.x
- AlmaLinux 8.x*, 9.0*, 9.1*, 9.2*, 9.3*
- Rocky Linux 8.x*, 9.0*, 9.1*, 9.2*, 9.3*
- ALT Linux 7.0

* P2P, P2V e V2P indicano che il sistema può essere ripristinato da ambiente fisico ad ambiente fisico, da fisico a virtuale o da virtuale a fisico, garantendo sempre la possibilità di ripristino anche quando il PC industriale o il suo hardware identico all'originale non sono più disponibili.

Principali scenari operativi

Guasto del sistema OT	Incidente ransomware o malware	Patch o aggiornamento del fornitore non riusciti	Perdita delle postazioni di ingegneria	Interruzione in un sito remoto o offshore
Guasto del disco o della scheda madre del PC industriale. Ripristino rapido dell'intero sistema per tornare operativi senza dover ricostruire i sistemi da zero.	Isolamento dei sistemi interessati e ripristino di backup puliti e convalidati per tornare a uno stato operativo noto e affidabile, riducendo il rischio di reinfezione.	Esecuzione del rollback all'ultimo stato operativo noto e affidabile, dopo che una modifica ha causato instabilità o comportamenti non sicuri.	Ripristinare i PC di ingegneria e i repository di progetto per non perdere settimane nella riconfigurazione e supportare un controllo delle modifiche sicuro.	Ripristino in locale senza dipendere da Internet o da VPN per sottostazioni, stazioni di compressione, impianti di perforazione e siti di produzione remoti.

Percorsi di ripristino in base alla tipologia di guasto

Acronis Cyber Protect per OT offre molteplici opzioni di ripristino, permettendo ai team di selezionare il percorso più sicuro e veloce in base alla tipologia di guasto, ai vincoli del sito e alle priorità operative.

Tipologia di guasto	Percorso di ripristino consigliato	Funzionalità abilitate da Acronis	Ruoli coinvolti
Eliminazione o compromissione accidentale di un numero limitato di file.	Ripristino granulare (ripristino di file/cartelle).	Ripristino dei soli file necessari (ad esempio artefatti di progetto, file di configurazione, report) senza ricostruire l'intero sistema. Contenimento dell'impatto sull'operatività, evitando modifiche non necessarie alla workstation o al server OT.	Ingegnere dei controlli/dell'automazione oppure ingegnere OT/ICS.
Guasto parziale dell'applicazione o configurazione errata (il sistema si avvia ancora).	Esecuzione del rollback all'ultimo stato noto e affidabile (punto di ripristino).	Ripristino del sistema a un punto convalidato dopo una patch o un aggiornamento del fornitore non riusciti o un errore di configurazione. Aiuta a riportare lo stack di applicazioni OT a una condizione operativa prevedibile.	Ingegnere dei controlli/dell'automazione oppure ingegnere OT/ICS.
Il sistema non si avvia (guasto del disco, SO danneggiato, conseguenze di un attacco ransomware).	Ripristino bare-metal (supporto di ripristino avviabile: Linux o WinRE).	Avvio del dispositivo con il supporto di ripristino Acronis e ripristino dell'immagine completa (SO, applicazioni, driver e dati) per riportare il sistema a uno stato operativo noto e affidabile senza reinstallazione manuale.	Ingegnere OT/ICS o tecnico di sito qualificato.
Guasto hardware senza disponibilità del ricambio identico.	Ripristino su hardware diverso (Universal Restore).	Ripristino dell'immagine di sistema sull'hardware sostitutivo e integrazione dei driver critici richiesti per l'avvio (ad esempio controller di storage/chipset) per riportare online gli stack OT legacy e specifici del fornitore quando i PC industriali originali sono obsoleti o non disponibili.	Ingegnere OT/ICS o tecnico di sito (IT facoltativo).
Interruzione in un sito remoto (accesso IT limitato o assente).	Ripristino gestito dall'operatore (ripristino con un clic).	Flussi di lavoro di ripristino guidati e semplificati che consentono al personale non IT di ripristinare i sistemi OT in locale e in sicurezza, riducendo le interruzioni operative quando i tempi di viaggio per gli interventi o i vincoli all'accesso remoto ritardano il ripristino.	Operatore/capoturno oppure tecnico sul campo/di sottostazione.
Incidente ransomware o malware (rischio di reinfezione durante il ripristino).	Ripristino più sicuro (scansione/convalida dei punti di ripristino prima del ripristino).	Convalida dei backup e scansione dei punti di ripristino alla ricerca di malware prima del ripristino, per ridurre il rischio di ripristinare immagini compromesse. Supporta un flusso di lavoro di ripristino più sicuro quando si riportano le operazioni OT a uno stato noto e affidabile.	Ingegnere OT/ICS con responsabile della sicurezza OT.

Tipologia di guasto	Percorso di ripristino consigliato	Funzionalità abilitate da Acronis	Ruoli coinvolti
I workload OT virtualizzati richiedono un ritorno all'operatività più rapido (dove la virtualizzazione è consentita).	Ripristino rapido con macchine virtuali in standby.	Dove la virtualizzazione è consentita, il ripristino dei workload OT come macchine virtuali riduce i tempi di ripristino del servizio e consente di completare la convalida senza ritardare i tempi di operatività.	Ingegnere di piattaforma/ virtualizzazione OT (condiviso da OT/IT).
Le attività di audit, manutenzione e garanzia di resilienza richiedono prove della recuperabilità.	Recuperabilità verificata (convalida del backup e controlli di avviabilità).	Convalida della recuperabilità dei backup con controlli di integrità e verifica dell'avviabilità. Garanzia operativa della ripristinabilità dei sistemi OT critici nel rispetto degli obiettivi di ripristino richiesti.	Ingegnere OT/ICS con competenze in sicurezza OT/conformità.

Selezionando il percorso di ripristino che meglio corrisponde alla tipologia di guasto, i team OT possono ridurre l'interruzione operativa, evitare modifiche non necessarie ai sistemi e riportare le operazioni a uno stato convalidato allineato alle procedure del sito e alle policy di controllo delle modifiche.

Conformità e allineamento normativo

Acronis Cyber Protect per OT permette di soddisfare le aspettative in merito alla preparazione al ripristino e alla capacità di fornire prove per gli audit e garanzia dei fornitori oggi ampiamente richieste nei programmi di cyber security energetica e industriale. Ciò include l'allineamento ai principi di preparazione al ripristino della norma IEC 62443 e alle normative regionali, come NIS 2, ai requisiti di resilienza OT delle normative sulle infrastrutture critiche e alla pianificazione e ai test di ripristino specifici del settore, nonché alle aspettative in materia di garanzia dei fornitori e sviluppo sicuro, aspetti sempre più rilevanti per gli OEM nell'ambito del Cyber Resilience Act (CRA) dell'Unione europea.

GDPR NIS2 NIST IEC NERC CIP CRA

Funzionalità di conformità della piattaforma Acronis Cyber Protect

Prove di ripristino verificate.

Backup crittografati con controlli di conservazione.

Processi di ripristino controllati.

Pratiche SSDLC a supporto delle valutazioni di garanzia del fornitore.

IEC 62443-4-1 CERTIFIED

Certificazione IEC 62443-4-1 Acronis

La certificazione IEC 62443-4-1 conferma che Acronis applica pratiche di sviluppo sicuro dei prodotti (SSDLC) allineate alle aspettative del settore. Per le organizzazioni del settore petrolifero e del gas, dell'energia e dell'elettricità, ciò consolida la garanzia dei fornitori, riduce i rischi della supply chain e supporta la fiducia nelle soluzioni di resilienza OT.

Riepilogo

Acronis Cyber Protect consente alle organizzazioni del settore petrolifero e del gas, dell'energia e dell'elettricità di ripristinare i sistemi OT critici in modo sicuro, prevedibile e rapido senza causare interruzioni operative, supportando al contempo le crescenti esigenze di cyber security e di preparazione al ripristino del settore.

Acronis

Per saperne di più, visita acronis.com