Mantenere l'operatività negli ambienti di tecnologia operativa (OT)

I costi elevati dell'interruzione operativa dei sistemi OT

I sistemi di tecnologia operativa (OT) sono un elemento cruciale per la continuità operativa della produzione e per la redditività aziendale. Quando si "guastano", possono far crollare con sé linee di assemblaggio, gasdotti, reti di servizi pubblici e l'intera catena di fornitura. I costi delle interruzioni derivanti possono variare da decine a centinaia di migliaia di dollari all'ora. Un'indagine condotta da ABB ha rilevato che il 69% delle aziende di recente ha subito un'interruzione operativa al mese, con un costo di 150.000 dollari all'ora per le aziende[1]. Altre possibili conseguenze delle interruzioni operative OT:

- Costi delle opportunità di vendita dovuti ad ordini non soddisfatti e tempi di consegna più lunghi.
- Aumento dei costi diretti del lavoro per quantità di beni prodotti.
- Danni alla reputazione del brand e alle relazioni con i clienti dovuti a consegne lente o non effettuate.
- Diminuzione della capitalizzazione di mercato per la perdita di fiducia degli investitori nelle capacità dell'azienda di mantenere una produzione omogenea.
- Multe per il mancato rispetto degli accordi sui livelli di servizio e di altri obblighi contrattuali.
- Multa e sanzioni penali per mancata conformità ai requisiti normativi in materia di resilienza digitale.

Di conseguenza, la posta in gioco è molto alta nella difesa dei sistemi OT contro attacchi informatici, disastri naturali, guasti hardware, malfunzionamenti del software e errori umani, nonché per il ripristino rapido in caso di malfunzionamenti.

Molti settori fanno ampio uso dell'automazione per i processi di produzione in tempo reale, compresi i settori automobilistico, energetico, farmaceutico e della logistica. Molte di queste tecnologie di automazione sono controllate, configurate e monitorate da PC, con sistema operativo Windows o Linux, che rientrano nell'ambito delle tecnologie operative (OT), dei sistemi di controllo industriale (ICS) e delle infrastrutture cyber-fisiche. Le applicazioni OT più comuni includono i sistemi SCADA (supervisory control and data acquisition), i sistemi di controllo distribuiti (DCS), le interfacce uomo-macchina (HMI) e i sistemi di memorizzazione delle operazioni che acquisiscono i dati dei processi in tempo

[1] ABB. "Il valore dell'affidabilità: rapporto ABB 2023."

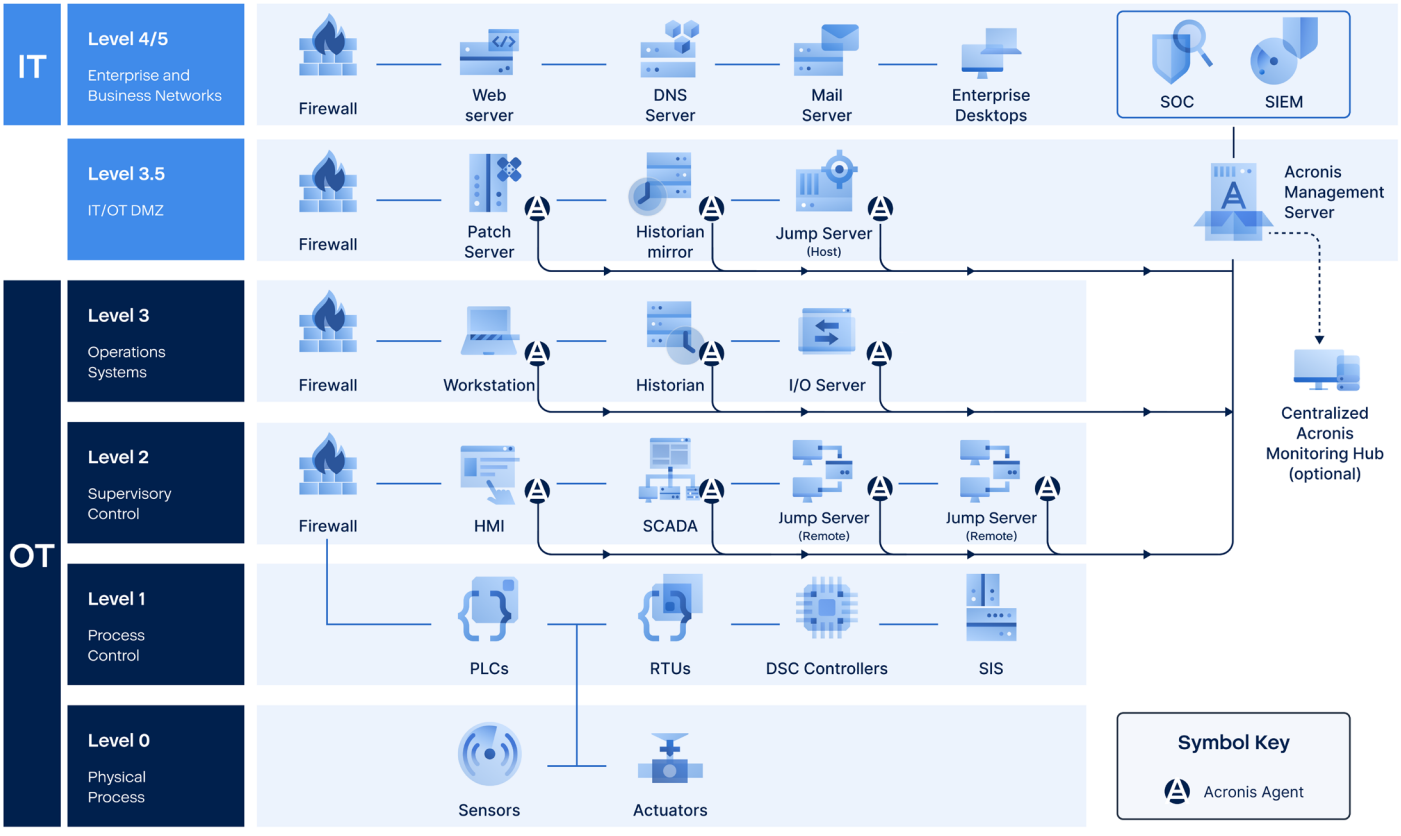
Le sfide per il mantenimento dell'operatività dei sistemi OT

L'esigenza di ridurre al minimo le interruzioni operative dei sistemi OT è amplificata dal fatto che gli ambienti OT presentano caratteristiche uniche, e sono più difficili da mantenere in esercizio rispetto ai tradizionali sistemi IT back-office e front-office:

- Molti sistemi OT girano su hardware e sistemi operativi (OS) datati, alcuni risalenti all'epoca di Windows XP. Aggiornare con versioni nuove di hardware e sistema operativo è rischioso e potrebbe danneggiare o limitare la funzionalità delle applicazioni OT.
- Inoltre, l'età di questi sistemi rende difficile o impossibile dotarli di misure di Cyber Security aggiornate, come il rilevamento e risposta sugli endpoint (EDR).
- Spesso, quando un fornitore di sistemi operativi annuncia la fine del supporto per una data versione del suo prodotto (ad esempio, come Microsoft per Windows XP nell'aprile 2014), entro cinque anni, ma anche prima, anche i fornitori di soluzioni di backup smettono di supportarla. Senza il giusto supporto di un fornitore di backup, gli ingegneri OT sono costretti a fare affidamento su processi di backup lenti, manuali e soggetti a errori, che per essere eseguiti richiedono interruzioni operative programmate e costose.
- Le strutture in cui si trovano i sistemi OT hanno raramente un supporto IT locale e sono spesso distanti dai team IT centralizzati. Inoltre, gli ambienti OT sono spesso isolati per ridurre i rischi per la Cyber Security il che impedisce all'IT di utilizzare strumenti di monitoraggio e gestione remoti. L'invio fisico del personale IT presso le sedi di produzione può essere lento e costoso e prolunga i tempi di inattività.

Acronis soddisfa le esigenze di resilienza digitale specifiche degli ambienti OT

La piattaforma Acronis Cyber Protect è ampiamente utilizzata nel settore manifatturiero e industriale per proteggere una varietà di sistemi OT, tra cui (ma non solo) quelli illustrati nel Modello Purdue mostrato in Figura 1



*List of protected systems not exhaustive

Figura 1: Esempi di sistemi OT protetti da Acronis, secondo il modello Purdue

Acronis Cyber Protect offre backup e ripristino per i sistemi OT con funzionalità essenziali in ambienti di produzione che richiedono un'operatività estremamente elevata, tra cui:

- La possibilità di installare l'agente di Acronis Cyber Protect e di eseguire i backup senza mai mettere offline il sistema OT o riavviarlo.
- Esecuzione del backup rapida, affidabile e completamente automatica, che non sovraccarica il sistema OT per elaborazione e archiviazione dei backup.
- La possibilità di standardizzare (o personalizzare) i backup su più sistemi e siti, grazie ai piani di protezione dei dati.
- Funzioni di Cyber Security opzionali che utilizzano lo stesso agente Acronis, tra cui EDR, anti-malware e anti-ransomware.

Acronis protegge anche i sistemi OT più datati

Acronis rafforza la stabilità degli ambienti OT proteggendo ogni sistema operativo, dall'era di XP fino ad oggi (compresi i sistemi operativi da tempo abbandonati da altri fornitori). Questo garantisce un ripristino rapido e affidabile anche dei sistemi più obsoleti, con la possibilità di replicare un sistema su nuovo hardware PC tramite un processo chiamato ripristino bare-metal, se necessario. Questa funzionalità installa automaticamente i nuovi driver necessari per garantire che il sistema operativo e le applicazioni OT funzionino correttamente sul nuovo hardware. La figura 2 mostra la gamma di supporto Acronis per i sistemi operativi e gli hypervisor a partire dall'era XP fino ad oggi, evidenziando le versioni di Windows e Linux più comunemente utilizzate negli ambienti OT:

Copertura ottimale per i più diffusi sistemi operativi e hypervisor

Windows

- Windows Server 2003 SP1/2003 R2 e successivi, 2008, 2008 R2, 2012/2012 R2, 2016, 2019, 2022 (tutte le opzioni di installazione eccetto Nano Server)
- 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, 11 (tutte le edizioni), 10, - tutte le edizioni, eccetto Windows RT

Microsoft SQL Server
2022, 2019, 2017, 2016, 2014, 2012, 2008 R2, 2008, 2005

Microsoft Exchange Server
2019, 2016, 2013, 2010, 2007

Hypervisor

VMware vSphere
4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0, 8.0

Microsoft Hyper-V Server
2022, 2019, 2016, 2012/2012 R2, 2008/2008 R2

Citrix XenServer/Citrix Hypervisor
8.2 - 4.1.5

Linux KVM
8 - 7.6

Scale Computing Hypercore
8.8, 8.9, 9.0

Red Hat Enterprise Virtualization (RHEV)
3.6-2.2

Red Hat Virtualization
4.0, 4.1, 4.2, 4.3, 4.4

Virtuozzo
7.0.14 - 6.0.10

Infrastruttura Piattaforma Virtuozzo
3.5

Nutanix Acropolis Hypervisor (AHV)
Da 20160925.x a 20180425.x

MacOS

- **OS X** Mavericks 10.9, Yosemite 10.10, El Capitan 10.11
- **macOS** Sierra 10.12, High Sierra 10.13, Mojave 10.14, Catalina 10.15, Big Sur 11, Monterey 12, Ventura 13, Sonoma 14

Linux: kernel 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

Figura 2: Supporto Acronis per sistemi operativi e hypervisor

Acronis consente il ripristino dei sistemi OT senza l'intervento dell'IT

Acronis offre una funzionalità unica chiamata Ripristino con un clic, che è fondamentale negli ambienti OT privi di personale IT in loco e/o con isolamento di rete, che impedisce l'uso di strumenti di gestione remota da parte del personale IT centralizzato. Il Ripristino con un clic di Acronis consente a qualsiasi operatore locale, indipendentemente dal suo livello di competenza IT, di ripristinare con pochi passaggi un sistema OT guasto da un backup locale. I costosi fermi produzione dovuti ai guasti dei sistemi OT, che potrebbero richiedere ore o giorni per essere risolti, compreso anche il tempo necessario per avere personale IT sul posto, possono essere ridotti a pochi minuti. La funzionalità consente di recuperare i sistemi OT da un backup su disco locale o da Acronis Cloud, e di proteggere i backup con crittografia Bitlocker e password di ripristino.

La protezione dei sistemi OT di Acronis è utilizzata dai principali fornitori di automazione

I principali fornitori di OT e ICS, tra cui ABB, Siemens, Honeywell e molti altri, utilizzano Acronis Cyber Protect come soluzione di backup per i propri clienti, in soluzioni white label o di co-branding. Nessun altro fornitore di soluzioni di protezione dei dati gode di una gamma di partnership e di approvazioni simile a quella di Acronis.

Acronis è riconosciuta come leader di resilienza digitale per l'OT

Aziende leader nel settore della ricerca tecnologica, come Forrester Research, TAG Infosphere e Omdia, considerano Acronis un'azienda di punta nella protezione dei sistemi OT.

Report di TAG Infosphere LEGGI

Report Omdia LEGGI

Conclusioni

Acronis Cyber Protect viene utilizzato per proteggere i sistemi OT in ambienti di produzione industriale e manifatturiera in tutto il mondo. La sua combinazione unica di protezione dei dati per i sistemi operativi – dall'era di XP a oggi, il ripristino con un solo clic per i sistemi OT da parte di personale non IT, e l'adozione da parte dei principali fornitori di automazione, hanno contribuito al riconoscimento da parte della comunità degli analisti come leader della resilienza digitale OT.

APPROFONDIMENTI

Scopri di più su Acronis Cyber Protect per OT

- Soluzioni di produzione Acronis
- Infografica: mantenere l'operatività OT grazie al ripristino con un solo clic
- Case study: prodotti downstream di Tata Steel
- Case study: ABB
- Case study: Johnson Electric
- Case study: BDR Pharma
- Fai una prova gratuita con Acronis Cyber Protect
- Parla con uno specialista di resilienza digitale OT

Acronis

Per maggiori informazioni vai su www.acronis.com