Acronis

WHITE PAPER

Confronto tra gestione distribuita e centralizzata della Cyber Protection per le aziende con più sedi

Aumenta la resilienza digitale della tua azienda con la gestione distribuita della Cyber Security e della protezione dei dati

Per garantire l'operatività dei sistemi e l'integrità dei dati, le aziende di ogni dimensione devono fronteggiare minacce di ogni tipo, dagli attacchi informatici assistiti dall'AI agli errori umani, dai guasti hardware ai problemi software. Mentre molte aziende scelgono di centralizzare le operazioni IT e la gestione della Cyber Security, in altri scenari cedere parte di queste incombenze ai team che si occupano di IT e di sicurezza informatica e che operano da posizioni remote può promuovere la resilienza digitale.

In questo white paper esamineremo gli scenari in cui un'azienda, delegando parte del controllo ai team ubicati in posizioni decentrate o remote, può ottenere tempi di operatività più elevati, prevenire in modo più efficace la perdita di dati e ridurre i costi di gestione e protezione dell'infrastruttura IT e dei dati. Il documento valuta i pro e i contro dell'approccio e valuta come le aziende possono soddisfare i propri obiettivi di conformità e governance senza gestire in maniera totalmente centralizzata le operazioni IT e la Cyber Security.

Molte aziende operano su più sedi

Circa un quarto delle aziende statunitensi ha sedi dislocate in diverse ubicazioni. L'Unione Europea (UE) non fornisce dati specifici sulle attività commerciali in base al numero di sedi, ma la forte prevalenza di attività di vendita al dettaglio, ospitalità, sanità, servizi finanziari e altro, segmenti caratterizzati dalla presenza di numerose sedi, suggerisce che le attività con filiali dislocate rappresentino una componente significativa anche nell'economia dell'UE. Per le grandi enterprise la probabilità di avere più sedi (uffici regionali, impianti di produzione, magazzini e centri di distribuzione) è ancora più elevata.

Anche le aziende che si espandono in altri settori di attività e aree geografiche tramite fusioni e acquisizioni, avranno numerose sedi fisicamente distanti dal personale IT e di Cyber Security presente nella sede centrale.

Esempi di aziende distribuite

Il settore della vendita al dettaglio offre un valido esempio di attività altamente distribuita. Un tipico retailer prevede sedi centrali globali e regionali, magazzini di distribuzione ed esercizi fisici per i consumatori. Molte altre aziende non appartenenti al comparto retail sono organizzate fisicamente nello stesso modo, ovvero con punti vendita o uffici dislocati geograficamente, come nei seguenti esempi:

- Erogazione di servizi sanitari, come servizi oculistici, studi di medicina di base, cliniche odontoiatriche, strutture di pronto soccorso, farmacie e cliniche veterinarie.
- Aziende di servizi bancari, assicurativi e finanziari al dettaglio, orientate al consumatore, con numerose filiali.

- Aziende di spedizione/ricezione, trasporto e logistica con numerosi centri di distribuzione e punti vendita al dettaglio per spedizioni e altri servizi aziendali.
- Aziende nel settore del gaming con più sedi: casinò, sale bingo, sale scommesse, sale pachinko e strutture simili.
- Servizi di assistenza stradale, che spesso combinano vendita di carburante, servizi di ricarica per veicoli elettrici, vendita al dettaglio di generi alimentari e istorazione veloce.
- Imprese organizzate secondo strutture federate, in cui un team centralizzato può supervisionare le operazioni IT, la sicurezza informatica e la conformità dell'intera azienda; le singole strutture dispongono tuttavia di budget individuali, responsabilità sull'assunzione del personale e autonomia locale per gestire l'infrastruttura IT dell'unità aziendale.

Le sfide della gestione centralizzata dell'IT e della Cyber Security

In genere, un'azienda con più sedi presenta una combinazione eterogenea di hardware, sistemi di virtualizzazione e operativi, e di applicazioni, come i sistemi di inventario o dei punti vendita forniti da svariati vendor di tecnologie. Il mix di infrastruttura tecnologica e versioni software può variare notevolmente da una sede all'altra. La necessità di preservare le applicazioni legacy, i software personalizzati e i computer utilizzati per controllare la stabilità degli ambienti tecnologici può impedire la standardizzazione dell'IT in tutta l'azienda, con la conseguente proliferazione di strumenti IT e di Cyber Security.

Il personale della sede centrale avrà difficoltà a maturare l'esperienza necessaria per gestire, proteggere e supportare la pletora di strumenti, applicazioni e dati dell'intera organizzazione. Intanto, la complessità e la diversità delle applicazioni, nonché gli strumenti necessari per gestirle e proteggerle, continuano a crescere.

Per ridurre al minimo l'esposizione alle minacce informatiche, alcune sedi remote con requisiti di sicurezza elevati, ad esempio gli ambienti di produzione in fabbrica, potrebbero dover essere "air-gap", ovvero isolati fisicamente dalla rete aziendale e dalla rete Internet pubblica. Questa condizione può complicare ai team della sede centrale la diagnosi e la risoluzione dei problemi tramite desktop remoto o altri strumenti connessi alla rete, imponendo trasferimenti fisici verso la sede remota per le attività di assistenza.

Per i luoghi difficili da raggiungere, come raffinerie in ambienti desertici, piattaforme petrolifere offshore, impianti minerari e altri siti lontani dagli snodi di trasporto aereo e terrestre, questa condizione può imporre all'azienda un notevole impegno in termini di costi e tempo.

La gestione della protezione e della sicurezza dei dati di una grande azienda con un'unica sede è meno complessa e impegnativa rispetto alla protezione dello stesso numero di applicazioni ed endpoint, distribuiti però su più sedi geograficamente dislocate. Se i dati di backup non sono isolati in base alla posizione, il ripristino dal backup in una sede può incidere negativamente sulle prestazioni in tutte le altre.

Nelle diverse aree geografiche e località remote, la connettività WAN e la velocità di rete possono subire notevoli variazioni, rendendo imprevedibili e potenzialmente troppo lunghi i tempi previsti per soddisfare gli obiettivi di ripristino.

La gestione delle sedi remote può imporre al personale IT l'accesso separato e ripetuto ai repository dei dati e alle console di gestione della sicurezza locali, un processo che può risultare inefficiente, lento e soggetto a errori. Molti strumenti tradizionali di backup, disaster recovery e sicurezza sono specifici per i particolari ambienti applicativi, il che complica ulteriormente la standardizzazione su strumenti comuni a tutta l'azienda.

La conseguente proliferazione degli strumenti per l'operatività IT e la sicurezza è costosa e aumenta i costi di onboarding e formazione del personale di supporto, un problema di grande rilevanza in un mondo in cui i costi del personale IT e della Cyber Security non accennano a diminuire.

Le sfide della gestione centralizzata della conformità

I requisiti di conformità variano significativamente da nazione a nazione e, in alcuni casi, in ambito regionale, provinciale e comunale. Le aziende che operano negli Stati Uniti, ad esempio, potrebbero dover rispettare le normative sulla privacy applicate dal governo federale, da diversi stati americani e da alcune singole città.

Anche la conformità alle normative sulla sovranità dei dati rappresenta una nuova sfida. Tali normative limitano le ubicazioni fisiche, i data center e le reti in cui i dati sensibili possono transitare o essere archiviati, partendo dal presupposto che alcuni governi nazionali violeranno la riservatezza dei dati con controlli arbitrari. Nelle aziende con più sedi, il rispetto di questi requisiti è complesso da gestire e può influire negativamente sulle prestazioni delle applicazioni.

Tenere traccia dei dati che devono essere protetti, su quali dispositivi, degli elementi dell'infrastruttura IT certificati come conformi in base ai vari standard di sicurezza e normativi e dei dipendenti autorizzati ad accedere a tali dati è un compito gravoso, che può creare confusione e falle nella conformità. Queste complessità emergono in un momento in cui la maggior parte delle aziende dispone di budget invariati o in calo da destinare a personale IT e sicurezza informatica, mentre il numero di applicazioni e il volume di dati che devono gestire e proteggere continua a crescere.

Oggi le autorità di regolamentazione applicano sanzioni importanti per promuovere l'aderenza alle normative. Ad esempio, l'UE impone sistematicamente sanzioni che vanno dal 2 al 4% del fatturato annuo aziendale in caso di ripetuti inadempimenti nella protezione dei dati dei consumatori.

Ciò comporta problemi importanti per alcune aziende distribuite e con più sedi, tra cui difficoltà con la rete e nel reperire servizi di hosting per applicazioni e storage di terze parti conformi e sicuri, dotati di funzionalità come il controllo avanzato degli accessi e lo storage immutabile.

Acronis risolve le sfide di gestione e protezione delle aziende distribuite

Integrando in un'unica piattaforma centralizzata gestione remota, backup, disaster recovery e sicurezza, Acronis Cyber Protect risolve le sfide legate alla distribuzione delle soluzioni di sicurezza e protezione dei dati negli ambienti distribuiti. Le singole sedi remote possono essere configurate e gestite separatamente dal personale locale tramite una console dedicata alla specifica sede, installata in locale o in hosting su cloud.

È possibile personalizzare i piani di protezione dei dati e la pianificazione dei backup per ogni sede, oppure adottare piani e pianificazioni standardizzati per più di una sede. La protezione dei dati e la sicurezza di tutte le risorse locali possono essere gestite da un'unica console, senza dover passare da una schermata o da un'applicazione all'altra.

Tutte le funzioni di sicurezza e protezione dei dati sono gestite con un singolo agente installato su ogni endpoint. La crittografia completa dei dati e il trasferimento protetto con protocollo TLS (Transport Layer Security) garantiscono la sicurezza dei dati durante il transito. Inoltre, compressione e deduplicazione dei dati e limitazione della larghezza di banda sono gestite automaticamente, per ottimizzare il traffico con qualsiasi velocità di connessione ragionevole, garantendo un impatto minimo sulle operazioni attive.

Al contempo, i team che si occupano dell'IT e della Cyber Security presso la sede centrale possono monitorare le sedi remote tramite un dashboard centralizzato, per valutare il rischio informatico complessivo, lo stato della protezione dei dati e la conformità dell'intera organizzazione, come mostrato nella Figura 1.

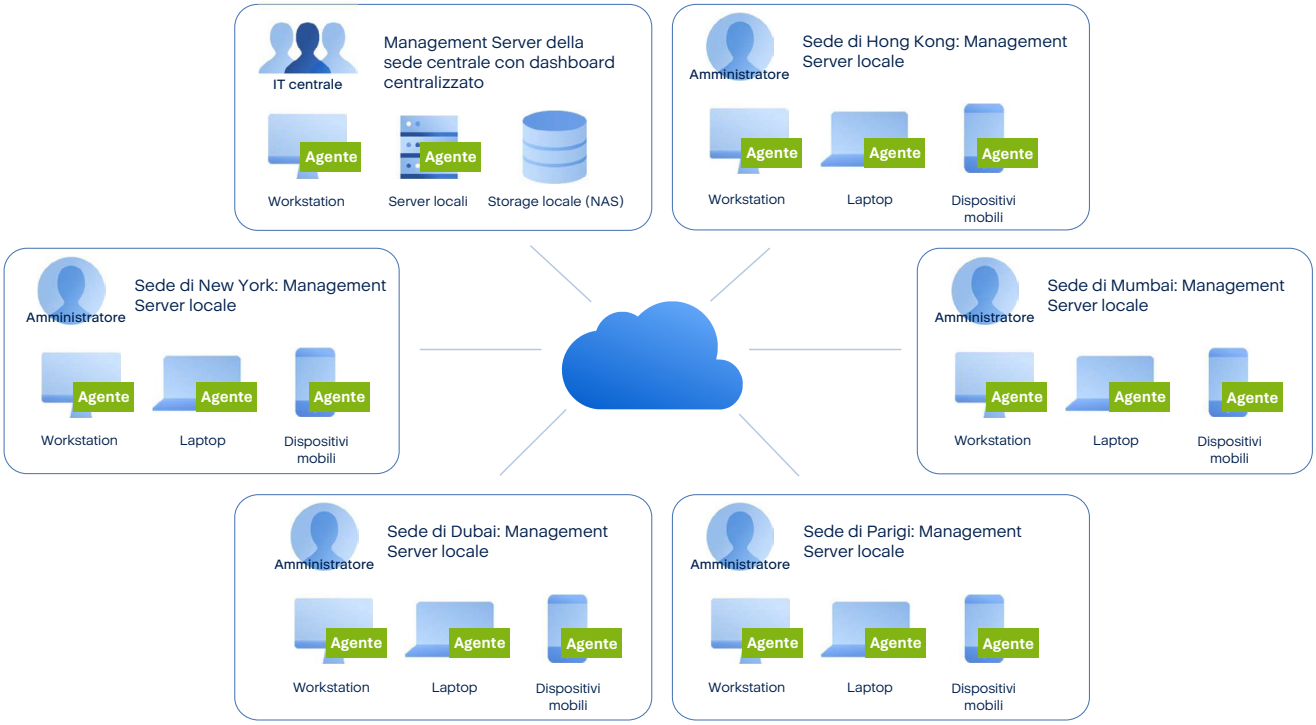

Figura 1. Gestione della Cyber Security e delle operazioni IT su più sedi, con controllo locale e monitoraggio centralizzato

Vantaggi chiave di Acronis Cyber Protect

- Isola l'archiviazione e la sicurezza dei dati di ogni posizione.
- Riduce o elimina i problemi di compatibilità della Cyber Security in termini di hardware, software e virtualizzazione.
- Risolve i problemi di sovranità dei dati e agevola il rispetto della conformità normativa.
- Risolve i problemi relativi alle diverse configurazioni e connessioni di rete.
- Riduce o elimina la necessità di più ambienti di hosting per la protezione dei dati.
- Genera costi omogenei e prevedibili per tutte le sedi fisiche.
- Semplifica il deployment dello storage con ridondanza geografica.
- Consente il monitoraggio centralizzato per la valutazione del rischio informatico, dello stato della protezione dei dati e della conformità a livello aziendale.

Le soluzioni Acronis si basano su immagini e file e utilizzano un agente multipiattaforma compatibile con la maggior parte degli ambienti informatici utilizzati in ambito commerciale e manifatturiero. Inoltre, le soluzioni Acronis proteggono anche le piattaforme di posta elettronica e collaborazione basate su cloud, come Microsoft 365 e Google Workspace, e quelle locali, ad esempio Microsoft Exchange in sede.

Ambienti supportati da Acronis

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 (RHV) 4.0, 4.1

Red Hat Virtualization (oVirt) 4.2, 4.3, 4.4

Virtuozzo 7.0.14 – 6.0.1.0

Virtuozzo Infrastructure Platform 3.5

Oracle Linux Virtualization Manager (Oracle LVM) 4.3

Nutanix Acropolis Hypervisor (AHV) 20160925x – 20180425x

Virtuozzo Hyper Server 7.5

Virtuozzo Hybrid Infrastructure 4.3 – 3.5

Sovranità dei dati e conformità per ambienti distribuiti

Acronis gestisce una rete di data center globale e indipendente, presente in tutto il mondo industrializzato; offre alle aziende distribuite grande flessibilità per l'archiviazione sicura dei dati, con l'obiettivo di ottimizzare le prestazioni della protezione dei dati e supportare le normative di conformità relative alla sovranità dei dati. Le singole sedi remote possono gestire la protezione e la sicurezza dei dati in base alla posizione e conservare i propri server, endpoint e dati delle soluzioni di e-mail e collaborazione dove necessario per il rispetto della conformità.

Integrando gestione degli endpoint, protezione dei dati e Cyber Security in un'unica piattaforma con console locali, è possibile ridurre i costi delle operazioni IT fino al 60%. Ulteriori risparmi sono possibili grazie alla riduzione delle spese associate alla formazione del personale e alla manutenzione di molteplici strumenti IT e di sicurezza informatica, nonché dei costi delle applicazioni di storage e transito dei dati di terze parti, in conformità alle normative dei singoli paesi.

L'implementazione e la manutenzione delle soluzioni di sicurezza, backup e disaster recovery sono sfide particolarmente complesse per le aziende distribuite e con più sedi. A queste si aggiungono la gestione delle soluzioni in più sedi, la gestione e la manutenzione dei servizi su innumerevoli combinazioni di tecnologie hardware e software, la garanzia di conformità alle normative sulla privacy e sulla sovranità dei dati e la distribuzione di questi servizi in ambienti con risorse e budget limitati. Se le aziende si espandono oltre i confini nazionali, queste sfide risulteranno amplificate.

Vantaggi della gestione su più sedi

Console locali per posizioni remote con agenti indipendenti

- Unica console in locale o con hosting su cloud per ogni sede, reparto, unità aziendale o marchio.
- Limitazione della larghezza di banda, compressione e deduplicazione dei dati, sempre incrementali, con trasporto facoltativo del disco fisico.
- Agente alla fonte con crittografia dei dati e trasferimento sicuro tramite TLS; non è necessario utilizzare la rete aziendale.

Dashboard centralizzato presso la sede centrale per il monitoraggio di tutte le console Acronis dei siti remoti

- Monitoraggio individuale o collettivo di tutte le console Acronis dei siti remoti.
- Visione unificata di tutti i dispositivi, gli avvisi e le attività del sito remoto.
- Download dei dati dai widget della console Acronis del sito remoto.
- Drill-down su dispositivi specifici di qualsiasi console Acronis remota.

Consolidamento di più strumenti

Singolo agente e singola console per gestire:

- Backup e disaster recovery.
- Sicurezza dell'e-mail e degli endpoint con tecnologia EDR (Endpoint Detection and Response).
- Applicazione di patch, inventario, assistenza remota, scripting e monitoraggio.

Workload protetti

- Server, VM, VM cloud e workstation.
- Desktop, laptop e dispositivi mobili.
- Windows (fino al 2003/XP), Mac, Linux.
- Microsoft 365 e Google Workspace.

Conformità migliorata alle normative locali

Oltre 50 data center in tutto il mondo.

- 11 data center in Europa.
- 2 data center in Germania.

Dati crittografati all'origine tramite AES-265 con password aziendali.

Dati in transito crittografati tramite SSL/TLS.

Storage immutabile.

Autenticazione a più fattori.

Accesso basato sui ruoli.

Certificazioni di conformità globali.

Riduzione dei costi e della complessità dei fornitori

Scegliere una soluzione Acronis permette di risparmiare fino al 60% rispetto all'utilizzo di molteplici strumenti di più fornitori.

Riduzione di vincoli delle risorse

Unica console, unica gestione.

Intelligenza artificiale e machine learning (ML) a supporto delle attività quotidiane.

- Monitoraggio dei dispositivi e correzioni automatiche.
- Indagine e risoluzione degli incidenti di sicurezza basate su AI.
- Backup automatico e test del disaster recovery.
- Libreria di script automatizzati per le attività di manutenzione.

Considerazioni finali

Sebbene la maggior parte delle aziende si avvalga di team centralizzati per gestire le operazioni IT e la Cyber Security, per altre la delega di alcune funzioni di gestione dell'IT e della sicurezza ai team che operano nelle sedi regionali e/o remote può promuovere la resilienza digitale.

La gestione distribuita delle misure di difesa aziendale contro le minacce informatiche e altre cause di inattività e perdita di dati, e la capacità di ripristinare rapidamente i dati e l'operatività in caso di emergenza può ridurre i rischi aziendali in modo più efficace rispetto al controllo centralizzato.

Nei contesti distribuiti su più sedi con gestione locale, i team regionali e remoti devono disporre di strumenti che integrino nativamente Cyber Security, protezione dei dati e gestione degli endpoint. Il monitoraggio centralizzato delle console utilizzate nelle sedi regionali e remote facilita ai team che operano dalla sede centrale la verifica e l'applicazione degli standard aziendali relativi a governance e conformità degli ambienti IT.

La combinazione di monitoraggio centralizzato e gestione distribuita delle operazioni IT e della Cyber Security permette di ottimizzare la reattività del supporto (in particolare per gli ambienti air-gap o le strutture molto remote), migliorando la conformità alle normative regionali in materia di sicurezza e IT e riducendo i rischi complessivi per l'azienda.

Per saperne di più

Non esitare a contattare Acronis qui per richiedere una consulenza gratuita con un esperto delle soluzioni Acronis che ti aiuterà a valutare se una topologia di controllo distribuita e con monitoraggio centralizzato per la gestione delle operazioni IT e della Cyber Security è adatta alla tua azienda.

Richiedi una versione di prova gratuita valida 30 giorni di Acronis Cyber Protect qui.

Informazioni su Acronis

Acronis, leader globale nella Cyber Protection, fornisce soluzioni che integrano nativamente funzioni di Cyber Security, protezione dei dati e gestione degli endpoint, progettate per i Managed Service Provider (MSP), le piccole e medie imprese (PMI) e i team IT aziendali. Altamente efficienti, le soluzioni Acronis consentono di identificare, prevenire, rilevare, rispondere e correggere le minacce informatiche più recenti e di avviare il ripristino con minime interruzioni, garantendo integrità dei dati e continuità operativa. Acronis offre la soluzione di sicurezza più completa sul mercato per gli MSP, grazie alla sua capacità unica di soddisfare le esigenze di ambienti IT diversi e distribuiti.

Acronis è una società svizzera fondata a Singapore nel 2003, con 45 sedi in tutto il mondo. Acronis Cyber Protect Cloud è disponibile in 26 lingue e in più di 150 paesi, ed è utilizzata da oltre 20.000 Service Provider per proteggere più di 750.000 aziende. Scopri di più su www.acronis.com.

Acronis

Scopri di più su
www.acronis.com