SBT Small Biz Thoughts
di Karl W. Palachuk

IL MODO PIÙ RAPIDO PER MIGLIORARE LA PRODUTTIVITÀ DELLE ATTIVITÀ IT, DELL'HELP DESK E DEL TEAM MSP

E-book commissionato da **Acronis**

SOMMARIO

IL MODO PIÙ RAPIDO PER MIGLIORARE LA PRODUTTIVITÀ DELLE ATTIVITÀ IT, DELL'HELP DESK E DEL TEAM MSP

di Karl W. Palachuk

Nel dicembre del 2019 Boeing ha lanciato nello spazio la capsula Starliner, che avrebbe dovuto agganciarsi alla Stazione Spaziale Internazionale, in una missione teoricamente semplice: lancio della navicella, attracco alla Stazione Spaziale, rientro sulla Terra.

Cinquantacinque minuti dopo il lancio, la NASA comunicava che la Starliner era entrata in un'orbita non nominale, ovvero, in un linguaggio meno tecnico, si trovava nell'orbita sbagliata e avrebbe mancato l'aggancio alla Stazione Spaziale Internazionale. Mancato! A bordo della capsula, fortunatamente, non c'era alcun equipaggio.

In un contesto di assoluta precisione come quello delle rotte spaziali, come è stato possibile "mancare" il bersaglio? La risposta è semplice: un inconveniente causato dalla mancata comunicazione tra due diversi sistemi software. Un orologio di bordo era impostato sull'ora sbagliata e perciò la capsula non arrivò nel posto giusto al momento giusto. Tutte le migliori intenzioni di comunicare in modo aperto e trasparente non sono bastate.

Riflettiamo: NASA, SpaceX e Boeing si erano impegnate a collaborare in un contesto di cooperazione e trasparenza. Tutti i partner avevano buone intenzioni, puntavano agli stessi obiettivi e guardavano nella stessa direzione alla ricerca di risultati condivisi.

L'intera operazione è costata a Boeing circa 1,5 miliardi di dollari. E hanno mancato l'obiettivo.

La lezione da trarre riguarda la relazione tra complessità, interconnessioni e utilizzo efficiente del software. Le cose possono andare storte anche quando i partner definiscono insieme le specifiche di progettazione e collaborano con piattaforme aperte e ben documentate.

Immaginiamo invece un contesto in cui gli sviluppatori non sono partner ma concorrenti, e ognuno indica le proprie specifiche di connessione tramite API (Application Programming Interface, interfacce di programmazione delle applicazioni), senza mai comunicare direttamente con gli altri.

Il risultato è prevedibile: molte complicazioni, poca linearità e alta probabilità di riscontrare problemi.

IL BUONO, IL BRUTTO E IL CATTIVO... DELLE API

Il settore della tecnologia avanza a grande velocità. Mentre negli altri settori emerge una nuova tipologia di business più o meno ogni 10 anni, nell'IT emerge una nuova generazione tecnologica ogni 18-24 mesi. Se non avete cambiato modalità operativa negli ultimi 5 anni, siete senz'altro rimasti indietro.

Siamo nel 2021, in un'epoca dominata dalle API. Al loro avvento, all'inizio del secolo, rappresentavano una modalità per facilitare la collaborazione tra le applicazioni, lo scambio di informazioni e l'automazione dei processi.

Consentendo a numerosi strumenti diversi di lavorare insieme, le API hanno offerto un'opportunità di valore a molti Managed Service Provider. Al maggior numero di middleware API acquistati corrispondeva naturalmente un costo di erogazione dei servizi più alto. Quel middleware era a volte molto costoso e spesso anche improvvisato, però funzionava.

Quella che inizialmente sembrava una nuova strategia straordinaria era diventata una sorta di kit "crea il tuo software Frankenstein".

Ma arriviamo al giorno d'oggi. Le API sono una tecnologia ormai consolidata, ma anche nelle migliori condizioni e con la programmazione più avanzata, le connessioni API non sono semplici da gestire. Se la connessione coinvolge i software di due aziende diverse, una modifica unilaterale può rendere inoperative alcune funzionalità. Se poi tra le due applicazioni si inserisce un'altra connessione, le cose si fanno ancora più complicate.

Ogni connessione richiede almeno un livello di gestione e rappresenta una potenziale falla nella sicurezza che deve essere monitorata. Oggi il ransomware è un grosso affare e i criminali informatici hanno scoperto che i Service Provider IT sono una fonte inesauribile alla quale attingere per sottrarre dati e iniettare codice. Come per qualsiasi altro attacco, possono scegliere un punto d'accesso qualsiasi e infiltrarsi, il che significa che è necessario organizzare le difese a 360°.

Il segreto ben custodito delle attività di sviluppo software è che la manutenzione e il supporto finiscono puntualmente per costare più del software stesso. (La fonte di questa informazione è sicura: siamo Service Provider IT e fornire supporto è il nostro lavoro.) In più, ogni set di connessioni in più richiede ulteriori interventi di monitoraggio, manutenzione e supporto.

IL COSTO REALE DELLA PROLIFERAZIONE DEI TOOL

Oltre al costo dei tanti vendor per le loro varie soluzioni, la proliferazione dei tool incide sui costi di formazione, integrazione e gestione. Uno studio di Gartner evidenzia come questa complessità sia causa di maggiori spese su più fronti. Il "brutto" delle API è, in sostanza, la loro poca efficienza nel connettere software diversi. Ogni connessione aggiunge complessità, documentazione, formazione e richiede due o più connessioni aggiuntive che vanno poi gestite.

Il lavoro dedicato alla manutenzione di un sistema complesso e interconnesso ha un impatto diretto sulla produttività generale. Ogni ora dedicata alla gestione dei sistemi è un'ora sottratta all'assistenza degli utenti finali.

Un recente studio di Forrester Research evidenzia che l'uso di strumenti legacy costituisce una delle principali barriere alla modernizzazione e alla trasformazione digitale. Dallo studio emerge che l'86% delle aziende utilizza almeno uno strumento legacy, e che solo il 12% utilizza tool di monitoraggio integrati e innovativi.

Affidarsi a questa varietà di strumenti obsoleti e con scarse capacità di connessione incide sui costi di supporto dell'ambiente, rallenta l'erogazione dei servizi e aumenta il rischio di sicurezza (aspetti che approfondiremo più avanti). Un costo ulteriore è quello dell'integrazione: quasi metà (46%) delle aziende intervistate riferisce di "dedicare troppo tempo e denaro alla gestione e all'integrazione dei diversi protocolli di sicurezza di ogni strumento".

Infine, è inevitabile che con l'uso di più strumenti alcune funzionalità si sovrappongano. In altre parole, la stessa funzionalità viene pagata due o tre volte. In ciascun caso, almeno uno dei tool non usa tutte le proprie funzionalità integrate poiché si avvale di una funzionalità simile di un altro strumento. La sovrapposizione delle funzioni porta al sottoutilizzo della maggior parte dei tool, a causa della complessità, della carenza di risorse e del carico associato alla gestione di più strumenti.

> In breve, la maggior parte delle aziende utilizza una serie di strumenti non progettati per essere connessi e investe denaro in funzioni duplicate, che aumentano i costi della manutenzione e delle licenze iniziali. L'intera operazione richiede, per ogni soluzione aggiunta, un ulteriore carico di formazione, monitoraggio e documentazione.
>
> Ma non deve essere per forza così.

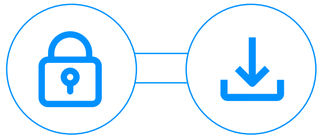
UNA SOLUZIONE PERFETTAMENTE INTEGRATA

Dalle prime API macchinose, abbiamo fatto tanta strada. Sempre di più, i reparti IT scelgono opzioni software integrate a livello progettuale e non "collage" messi insieme a posteriori. Ci stiamo così lasciando alle spalle il panorama dominato dalle connessioni API.

La complessità è un fattore importante nello sviluppo e nella manutenzione del software. Come è facile immaginare, causa un aumento dei costi di manutenzione, sicurezza e assistenza.

Esempio 1

Due soluzioni software e un connettore prevedono la collaborazione di uno, due o tre partner diversi. Ognuno di loro può apportare una modifica al programma che interrompe la connessione o crea una vulnerabilità che potrebbe essere sfruttata dagli hacker.



Esempio 2

Tre soluzioni software e due connettori prevedono la collaborazione di uno, due, tre, quattro o cinque partner diversi. Anche in questo caso, ognuno di loro può apportare una modifica che interrompe la connessione o crea una vulnerabilità che potrebbe essere sfruttata dagli hacker.

Esempio 3

Diamo un'occhiata al mercato emergente delle applicazioni di sicurezza "integrate". Sono state concepite per lavorare insieme, sono state realizzate dallo stesso team, collaborano per definizione.

Come abbiamo visto, in presenza di sistemi diversi per il backup, la protezione dal malware, il supporto per desktop remoto e la gestione, si avranno anche molteplici connessioni, che rappresentano punti deboli e potenziali vettori d'attacco per l'ambiente informatico. Illustriamo meglio il concetto.

Ipotizziamo di voler connettere due applicazioni e i relativi servizi, ad esempio backup e antivirus. Il risultato finale dipende da diversi fattori. Le applicazioni sono realizzate dalla stessa azienda? Sono state concepite per lavorare insieme? Se esiste una connessione tra i due sistemi, è stata scritta da una delle aziende produttrici o da una terza parte?

Con la progressiva riduzione della complessità del software, emergono una serie di vantaggi: più efficienza, meno manutenzione, aumento della produttività e maggiore sicurezza. I costi si abbattono dal principio, in quanto non occorre acquistare middleware di terze parti per far funzionare in modo fluido l'intero stack applicativo, né dedicare tempo alla gestione delle applicazioni aggiuntive.

I Service Provider IT riscontrano un problema emergente, che possiamo definire "stress da vendor" ed è causato dal numero eccessivo di fatture inviate dalle tante aziende che devono contribuire a far funzionare i sistemi come dovrebbero.

C'è un'azienda che ha affrontato e risolto questo problema. Acronis ha creato uno stack di prodotti che si integrano alla perfezione l'uno con l'altro. Progettato partendo da zero, Acronis Cyber Protect ottimizza l'efficienza riducendo la complessità e il costo totale di proprietà. Il principio è illustrato da Lauren Beliveau, Acronis Product Marketing Manager, che afferma: "Non abbiamo realizzato un gruppo di prodotti, ma uno stack di soluzioni".

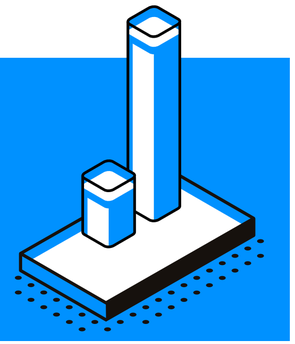
Non si tratta solo di un problema teorico. In ambito di sicurezza, il vecchio mix di strumenti legacy costituisce una seria minaccia che esige ulteriori attività di monitoraggio. Ogni connessione, patch o aggiornamento costituisce una potenziale vulnerabilità. E non basta applicare le patch: bisogna anche monitorarle per verificare che non abbiano introdotto problemi. Talvolta è necessario disinstallarle e poi riapplicarle, perché sono emerse delle vulnerabilità.

Purtroppo, in molti casi si aspetta prima di applicare le patch, per assicurarsi che non introducano ulteriori problemi, incompatibilità o punti deboli. Questa strategia espone le applicazioni alle vulnerabilità note, per periodi di tempo anche lunghi.

Infine, le applicazioni poco integrate di vendor diversi potrebbero non essere in grado di condividere dati, avvisi, automazione, documentazione, interfacce utente, agenti e altri aspetti. A ogni punto debole di una connessione corrisponde un punto debole nella sicurezza, il cui costo è oggi troppo elevato per essere ignorato.

Acronis Cyber Protect include una funzionalità antivirus che riconosce la presenza di un backup e lo analizza. È una soluzione completamente integrata in cui il backup e l'antivirus lavorano insieme in modo efficiente. Per garantire la pulizia dei dati, i backup vengono analizzati automaticamente alla ricerca di minacce quali virus, malware e ransomware. Le patch vengono applicate ai backup e ai sistemi in funzione, in modo ottimizzato. Senza il minimo attrito.

La progressiva riduzione della complessità del software genera più efficienza, meno manutenzione, aumento della produttività e maggiore sicurezza.



QUANTO CONTA LA MATURITÀ DELL'AZIENDA

Un fattore raramente considerato è la maturità dell'azienda che realizza gli strumenti. Come accade alle persone, anche le aziende si trasformano e crescono attraversando diverse fasi. Inizialmente, propongono un prodotto "acerbo", con un'unica finalità, ad esempio un antivirus. Nel tempo, il prodotto diventa completamente funzionale. Nel passaggio da startup ad azienda consolidata, l'azienda si concentra sul lancio del prodotto sul mercato, con l'intento di produrre un profitto.

Le startup ormai consolidate puntano ad aggiungere funzionalità e connettività, adottando le onnipresenti API con l'obiettivo di comunicare con qualsiasi prodotto. È forse la fase meno lineare, perché in genere il prodotto funziona ma le API non sono perfezionate e tutto è in continua evoluzione. Se l'azienda ha successo, gli utenti iniziano a chiedere più funzionalità. Inizia quindi la fase successiva, ovvero l'ampliamento della clientela.

A questo punto, l'azienda si concentra sui nuovi clienti ma anche sulla creazione o acquisizione di nuove funzionalità. La strategia è quella di aumentare la clientela offrendo prodotti più sofisticati e collaborando con più competitor. L'obiettivo finale è ampliare la quota di mercato rispondendo alle esigenze dei clienti e utilizzando al meglio gli strumenti disponibili. È una fase di espansione a cui corrispondono spesso grandi cambiamenti interni e la necessità di tenere il passo con le API in evoluzione a più livelli: internamente, tra i prodotti acquistati e integrati, e tra i prodotti proprietari e quelli dei concorrenti.

La fase successiva è quella dell'espansione finanziaria, attuata tramite capital venture o altri meccanismi di finanziamento. È il momento in cui all'azienda serve denaro per ingrandirsi, ma anche quello in cui si riduce la tempestività di risposta ai clienti. Quando i dirigenti spostano l'attenzione dalle funzioni alle finanze, il fatturato diventa più importante della correzione dei problemi o dell'aggiunta di funzionalità.

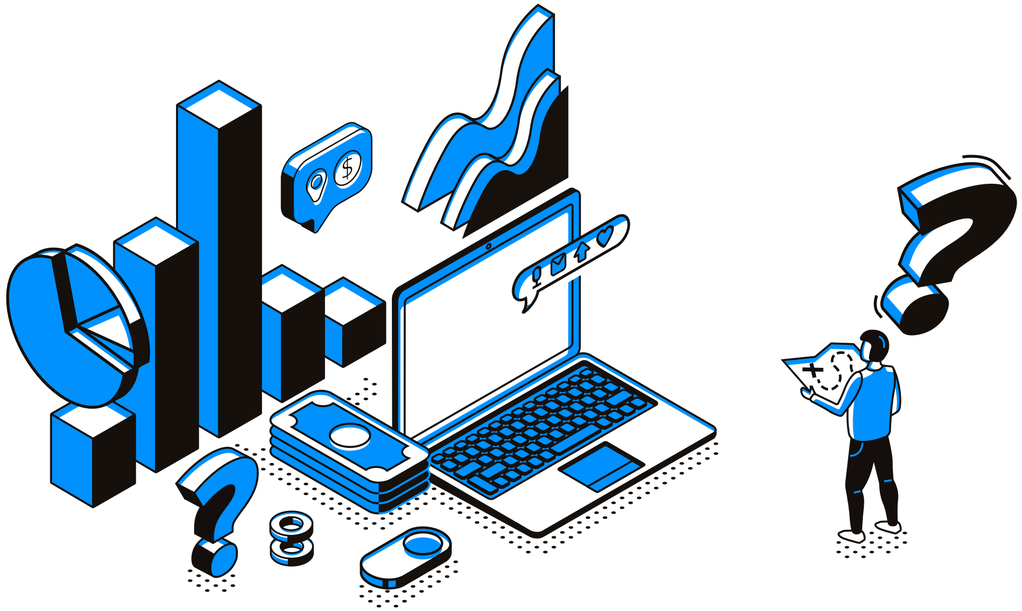
Lo abbiamo osservato nelle fusioni degli ultimi anni: un vendor prima altamente reattivo smette di risolvere le problematiche, mettendo in difficoltà i professionisti IT che si affidano a quel software. In questa fase il fatturato è l'unico obiettivo dell'azienda, mentre le attività di sviluppo, anche quelle che prevedono la risoluzione dei problemi software, si contraggono.

Sono poche le aziende che vivono abbastanza a lungo da acquisire una completa maturità, necessaria per sviluppare strumenti integrati e ottimizzati e offrire il necessario supporto ai programmatori perché aggiungano nuove funzionalità

senza causare incompatibilità o nuovi problemi. Oltre agli ostacoli tecnici, le aziende consolidate affrontano investimenti di lungo periodo, per finanziare lo sviluppo continuo, sostenere il fatturato e supportare i clienti.

Per assecondare l'accelerazione dei cambiamenti tecnologici, è indispensabile aggiungere funzioni nuove per fronteggiare le nuove sfide. Questo principio è valido per la Cyber Security più che per qualsiasi altro settore. 10 anni fa, i virus erano una seccatura e rallentavano l'operatività aziendale. Oggi, al costo dell'inattività si sommano i milioni di dollari destinati ai riscatti.

Le aziende poco consolidate e quelle in fase di fusione e acquisizione sono spesso vincolate a prodotti obsoleti. Molto spesso non hanno tempo, denaro o capacità interne per stare al passo con un panorama della sicurezza in costante trasformazione.



Nel migliore dei casi distribuiscono soluzioni vecchie. Nel peggiore, le loro soluzioni non si integrano con gli strumenti più innovativi.

La complessità degli strumenti è direttamente proporzionale al rallentamento dell'efficienza. Oltre a risolvere le problematiche date dalla molteplicità di API, occorre gestire le attività interne del software a vari livelli di maturità e il supporto fornito da aziende a vari livelli di maturità per le loro API e la relativa documentazione.

L'obiettivo è creare lo stack perfetto. A volte, significa selezionare le migliori opzioni disponibili, anche se realizzate da vendor diversi. Quando possibile, si acquista un unico stack al fine di aumentare efficienza, sicurezza e profitto.

> Acronis Cyber Protect rappresenta il meglio dei due mondi. Ampiamente riconosciuta come leader nella protezione dati e nel ripristino, Acronis ha realizzato un'intera raccolta di soluzioni di altissima qualità per proteggere dati, applicazioni e sistemi, e per eliminare tutte le complessità del middleware.
>
> Acronis Cyber Protect include alcune tra le funzionalità più copiate dai competitor, tra cui l'applicazione delle patch alle immagini di backup, in modo che le procedure di ripristino non possano ristabilire il livello di sicurezza compromesso dei sistemi client.

Il momento è difficile: ransomware, cause da milioni di dollari e un gran numero di normative e disposizioni di legge. Non c'è tempo né denaro da investire in strumenti di sicurezza diversi, nella speranza che funzionino bene insieme. Servono invece soluzioni che garantiscano funzionalità e sicurezza all'avanguardia, e che riducano al contempo la complessità, la manutenzione e i costi a queste associati.

È il momento di passare all'unico stack di sicurezza concepito specificamente per garantire un'integrazione perfetta.

CONCLUSIONI

Non possiamo più considerare la sicurezza come una funzionalità aggiunta ad altri servizi. In questo decennio, i consulenti tecnologici dovranno affidarsi a soluzioni complete, solide e comprovate, che garantiscano una sicurezza ineguagliabile e permettano ai clienti di dedicarsi ad altro.

La complessità limita l'efficienza e la produttività e aumenta i costi di manutenzione, documentazione e formazione. Più componenti richiedono più connettori. Uno stack completamente integrato, concepito sin dal principio per funzionare senza il minimo attrito, ottimizza la sicurezza e riduce la complessità e i costi a questa associati.

Utilizzeremo le API ancora a lungo, ma scegliendo lo stack totalmente integrato di Acronis, leader nella Cyber Security e nella protezione dei dati, potrete essere produttivi anche gestendo sistemi complessi e interconnessi.

Le connessioni sono un buon punto di partenza, ma l'integrazione "by design" è la destinazione perfetta.

FONTI

https://www.msn.com/en-us/news/technology/boeings-software-troubles-show-an-engineering-culture-clash/ar-BB16xEdq

https://www.forbes.com/sites/jonathanocallaghan/2019/12/20/boeing-starliner-spacecraft-launches-to-the-international-space-station-heralding-a-new-era-for-american-human-spaceflight/

If This Then That
https://ifttt.com/

Zapier
https://zapier.com/

Programmable Web
https://www.programmableweb.com/

Salesforce.com
www.salesforce.com

Harvard Business Review, "The Strategic Value of APIs".
https://hbr.org/2015/01/the-strategic-value-of-apis

"Gartner Says Organizations Can Cut Software Costs by 30 Percent Using Three Best Practices".
https://www.gartner.com/en/newsroom/press-releases/2016-07-19-gartner-says-organizations-can-cut-software-costs-by-30-percent-using-three-best-practices

Forrester Research, "Prevalence Of Legacy Tools Paralyzes Enterprises' Ability To Innovate".
https://sciencelogic.com/wp-content/uploads/sciencelogic-os.pdf

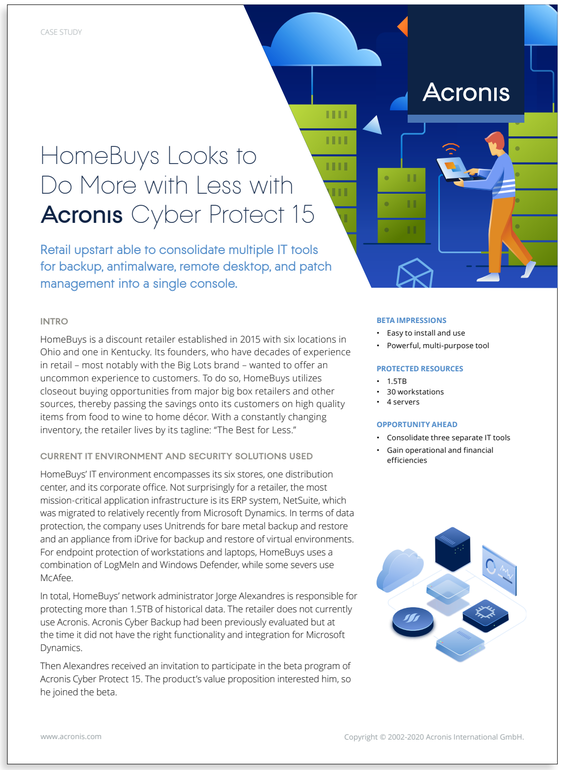
"Struggling With Toolchain Sprawl? You're Not Alone."
https://dzone.com/articles/toolchain-sprawl-youre-not-alone

INFORMAZIONI SULL'AUTORE

Karl W. Palachuk ha creato e venduto due società di servizi gestiti a Sacramento, in California. Fondatore e presidente del Sacramento SMB IT Professionals Group, è anche autore di numerosi libri, tra cui "The Network Documentation Workbook" e "Managed Services in a Month".

Da oltre 15 anni, Karl è un relatore molto richiesto in conferenze e seminari in tutto il mondo. Oltre a essere Microsoft Certified Systems Engineer, ha conseguito la laurea presso la Gonzaga University e un Master presso la University of Michigan. È anche Microsoft Small Business Specialist e uno dei membri fondatori dello Small Business Specialist Advisory Panel di Microsoft.

RISORSE AGGIUNTIVE



CASE STUDY

Acronis

HomeBuys Looks to Do More with Less with **Acronis** Cyber Protect 15

Retail upstart able to consolidate multiple IT tools for backup, antimalware, remote desktop, and patch management into a single console.

INTRO

HomeBuys is a discount retailer established in 2015 with six locations in Ohio and one in Kentucky. Its founders, who have decades of experience in retail – most notably with the Big Lots brand – wanted to offer an uncommon experience to customers. To do so, HomeBuys utilizes closeout buying opportunities from major big box retailers and other sources, thereby passing the savings onto its customers on high quality items from food to wine to home décor. With a constantly changing inventory, the retailer lives by its tagline: "The Best for Less."

CURRENT IT ENVIRONMENT AND SECURITY SOLUTIONS USED

HomeBuys' IT environment encompasses its six stores, one distribution center, and its corporate office. Not surprisingly for a retailer, the most mission-critical application infrastructure is its ERP system, NetSuite, which was migrated to relatively recently from Microsoft Dynamics. In terms of data protection, the company uses Unitrends for bare metal backup and restore and an appliance from iDrive for backup and restore of virtual environments. For endpoint protection of workstations and laptops, HomeBuys uses a combination of LogMeIn and Windows Defender, while some severs use McAfee.

In total, HomeBuys' network administrator Jorge Alexandres is responsible for protecting more than 1.5TB of historical data. The retailer does not currently use Acronis. Acronis Cyber Backup had been previously evaluated but at the time it did not have the right functionality and integration for Microsoft Dynamics.

Then Alexandres received an invitation to participate in the beta program of Acronis Cyber Protect 15. The product's value proposition interested him, so he joined the beta.

BETA IMPRESSIONS

- Easy to install and use
- Powerful, multi-purpose tool

PROTECTED RESOURCES

- 1.5TB
- 30 workstations
- 4 servers

OPPORTUNITY AHEAD

- Consolidate three separate IT tools
- Gain operational and financial efficiencies

www.acronis.com

Copyright © 2002-2020 Acronis International GmbH.

Blog di Acronis: le opinioni più recenti e aggiornate dai leader globali della Cyber Protection.

Canale YouTube di Acronis: video su scenari di utilizzo, demo, analisi delle minacce e news sull'azienda.

Acronis Resource Center: punto di riferimento centrale dove trovare whitepaper, e-book, articoli dettagliati, tutorial, infografiche e altro sulla Cyber Protection.

Eventi Acronis: serie di eventi, webinar, interviste ecc., con tutte le informazioni per partecipare.

INFORMAZIONI SU ACRONIS

Acronis coniuga protezione dati e Cyber Security per offrire una Cyber Protection integrata e automatizzata in grado di risolvere i problemi di salvaguardia, accessibilità, privacy, autenticità e sicurezza (SAPAS) del mondo digitale di oggi. Grazie a modelli di deployment flessibili che si adattano alle esigenze dei Service Provider e dei professionisti IT, Acronis garantisce una Cyber Protection di livello superiore per dati, applicazioni e sistemi con soluzioni innovative di nuova generazione per antivirus, backup, disaster recovery e protezione degli endpoint. Con le sue pluripremiate tecnologie antimalware basate su IA e di autenticazione dei dati basate su blockchain, Acronis protegge qualsiasi tipo di ambiente – cloud, ibrido o in sede – a un costo contenuto e senza sorprese.

Fondata a Singapore nel 2003 e costituita in Svizzera nel 2008, Acronis conta oggi più di 1.500 dipendenti in 33 uffici distribuiti in 18 paesi. Alle sue soluzioni si affidano più di 5,5 milioni di utenti privati e più di 500.000 aziende, fra cui la totalità di quelle presenti nella classifica Fortune 1000 e team di sport professionistici ai massimi livelli. I prodotti Acronis sono disponibili presso 50.000 partner e Service Provider in oltre 150 paesi in più di 40 lingue.

SBT SMALL BIZ THOUGHTS

di Karl W. Palachuk

SmallBizThoughts.com

E-book commissionato da **Acronis**

acronis.com