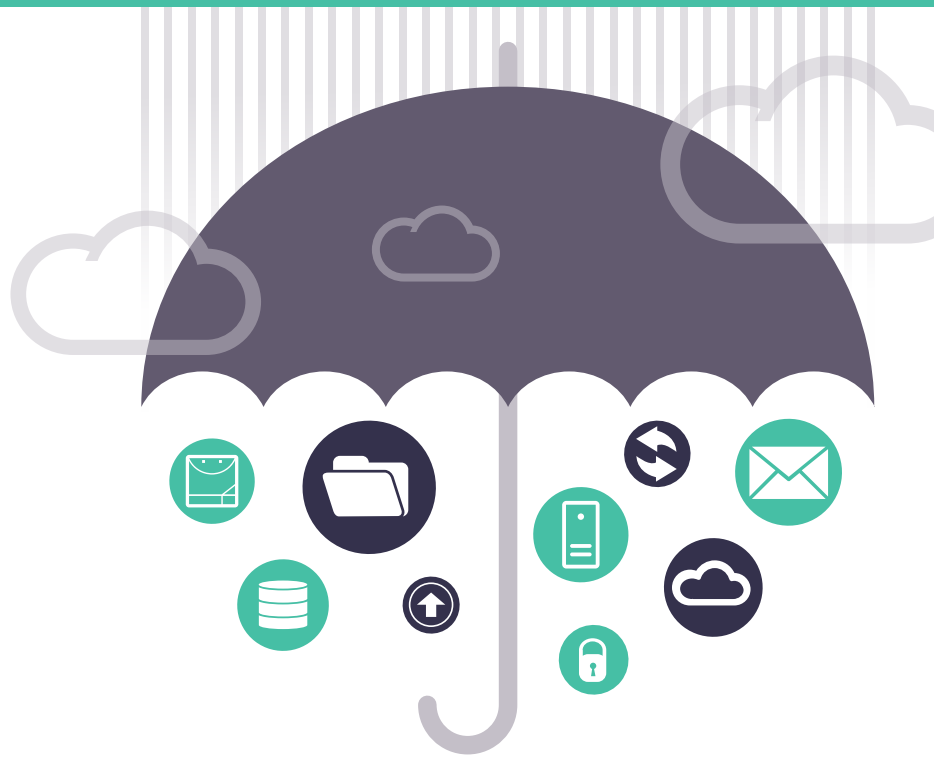
arcserve®



Tutto ciò che occorre sapere oggi sull'architettura di protezione dei dati di prossima generazione

Non è necessario ribadire l'importanza di un sistema di protezione dei dati efficace ed efficiente. Sapete già che la capacità di garantire non solo la protezione, ma anche il ripristino rapido da interruzioni di sistema e perdite di dati, è un elemento essenziale per la sopravvivenza dell'azienda.

Nonostante questo, l'architettura di protezione dei dati può essere ancora il vostro tallone d'Achille.

A volte il problema è la vulnerabilità dell'hardware e dell'infrastruttura di elaborazione e networking, che non offrono una base sufficientemente solida. In altri casi è la presenza di silos di protezione non flessibili a minare l'efficacia e l'efficienza del piano. Infine, l'infrastruttura può essere esposta a piccoli e grandi eventi di perdita di dati.

È essenziale identificare tutto ciò che può andare storto e proteggersi da ogni eventualità.

La buona notizia è che il settore delle architetture per la protezione dei dati è in grande fermento. La tecnologia si sta evolvendo a un ritmo esponenziale e oggi consente di migliorare l'efficienza operativa, soddisfare al meglio le esigenze degli utenti finali e offrire funzionalità più robuste di protezione, deduplica e ripristino dei dati.

Dunque, cosa occorre sapere sulla direzione in cui ci stiamo muovendo?

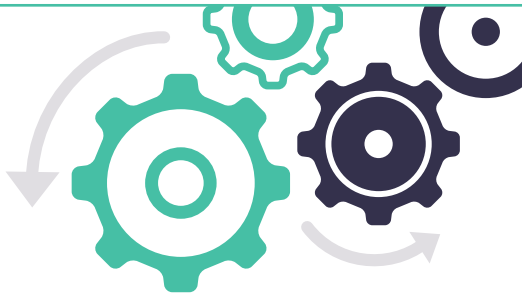
Questo documento illustra i fattori alla base della rapida evoluzione delle architetture di protezione dei dati, le tendenze da tenere d'occhio, ciò che possiamo aspettarci dalle architetture di prossima generazione e il panorama attuale del mercato.

Non c'è motivo di allarmarsi. Ci sono grandi trasformazioni in corso, ma qui troverete un resoconto dei fatti essenziali.

Sommario

Capitolo 1:

I fattori alla base della modifica delle architetture esistenti



Per restare competitivi sul mercato, oggi i vendor di soluzioni di protezione dei dati come Arcserve devono innovare costantemente la propria offerta, per aiutare i clienti a gestire un livello di complessità esponenzialmente superiore rispetto al passato.

Qual è la richiesta del mercato?

Fino a pochissimo tempo fa non esisteva una singola soluzione per la protezione, la deduplica e il ripristino dei dati. I reparti IT erano costretti a utilizzare più soluzioni puntuali fornite da vendor diversi, creando così ambienti intrinsecamente più complessi e impegnativi da gestire.

Questo ha certamente creato infrastrutture di protezione dati incoerenti.

Consideriamo ora l'ampia adozione della virtualizzazione e delle applicazioni di business multilivello, caratterizzate da schemi di protezione dei dati estremamente complessi. È abbastanza da far girare la testa a chiunque.

E c'è di più: gli eventi di perdita di dati oggi diventano di dominio pubblico.

Nel contesto odierno, gli eventi altamente pubblicizzati di danneggiamento dei dati hanno un enorme impatto sulla redditività del business e sulla fiducia dei consumatori. Di conseguenza

i reparti IT sono forzati a dimostrare l'aderenza

a rigorosi requisiti di conformità e controllo dei dati a dirigenti, commissioni ed investitori, senza però disporre di una prevedibilità coerente rispetto al ripristino, né della capacità di misurare gli indicatori prestazionali chiave che sarebbero tenuti a comunicare.

Come se tutto ciò non bastasse, i reparti IT devono anche far fronte alla scarsità di risorse.

Può sembrare una sfida insormontabile. **Non lo è.**

È in atto un profondo cambiamento.

L'IT di oggi si basa sull'interdipendenza dei sistemi e delle applicazioni nell'ambito della delivery del servizio.

I vendor che hanno identificato questa opportunità di trasformazione del mercato stanno rivedendo le proprie best practice di protezione dei dati e apportando ai prodotti le modifiche essenziali necessarie per allinearli ad esse. I loro prodotti

di nuova generazione offriranno ai clienti misurabilità, facilità d'uso e capacità di ripristino superiori.

Quali sono le tendenze attuali e future da tenere sotto controllo?

Capitolo 2:

Tendenza da tenere d'occhio: appliance di protezione dei dati appositamente progettate

Il metodo tradizionale di acquisto, installazione e configurazione del software di backup sui server interni sta per tramontare a favore di una nuova tendenza, che promette un approccio più semplice e diretto alla protezione dei dati.

Si tratta delle appliance fisiche appositamente progettate, preconfigurate per l'esecuzione di software per la protezione dei dati e il ripristino.

Oggi, queste appliance fisiche sono molto richieste.

> Non solo il 64% delle aziende utilizza già PBBA (Purpose Built Backup Appliance) nel proprio ambiente, ma un altro 29% prevede o è interessata a farlo nel prossimo futuro.
>
> – Jason Buffington, Senior Analyst, Enterprise Strategy Group

Cosa rende le appliance fisiche così appetibili?

In una sola parola: **la semplicità**.

Queste soluzioni chiavi in mano semplificano

la determinazione del prezzo, l'acquisto, la configurazione e il deployment dell'architettura di protezione dei dati. Per le aziende di piccole e medie dimensioni, questo si traduce nella capacità di usufruire di funzionalità di protezione dei dati di fascia enterprise subito operative, senza bisogno di investire cifre enormi nel settore IT.

Questo ha enormemente accelerato l'acquisizione e il deployment di infrastrutture di protezione dei dati. Secondo i dati pubblicati da IDC*, infatti, nel 2014 le aziende hanno speso 3,26 miliardi di dollari in PBBA.

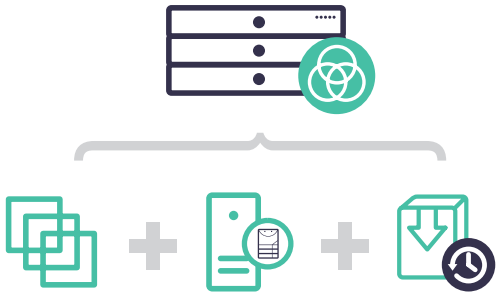
*International Data Corporation (20 marzo 2015). Worldwide Purpose-Built Backup Appliance (PBBA) Market Revenue Breaks the $1 Billion Mark in the Fourth Quarter, According to IDC [Comunicato stampa]. Il documento è disponibile qui.

L'evoluzione delle appliance fisiche di protezione dei dati

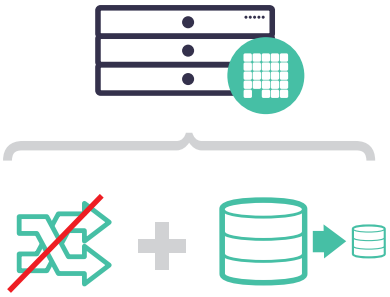
Fino a poco tempo fa, acquistando un'appliance di backup appositamente progettata (PBBA, Purpose Built Backup Appliance), si riceveva una soluzione in bundle con software e hardware modificati allo scopo, dunque un riadattamento privo di eleganza e carente in termini di efficienza e semplicità di utilizzo.

Oggi il mercato si sta orientando verso soluzioni progettate fin dall'inizio per l'uso di appliance fisiche.

Tali appliance includono:



Appliance di backup integrate con supporto nativo di più applicazioni e fornite con un software di backup e un server.



Appliance di deduplica basate sulla destinazione oppure lato origine più efficienti, che eliminano i dati duplicati e comprimono quelli rimanenti, riducendo il volume complessivo dei dati da proteggere.

Per ottenere riduzioni dei dati di tale entità, in genere le appliance di deduplica vengono accoppiate ad appliance di backup. Oggi, tuttavia, vengono introdotte sul mercato nuove soluzioni che offrono funzionalità di backup e deduplica integrate in un'unica appliance.

La gamma di appliance fisiche di protezione dei dati include inoltre le appliance di failover e gateway per il cloud, sebbene queste due offerte native per il cloud rappresentino una tendenza emergente a sé stante. Verranno quindi illustrate a parte nel prossimo capitolo.

Capitolo 3:

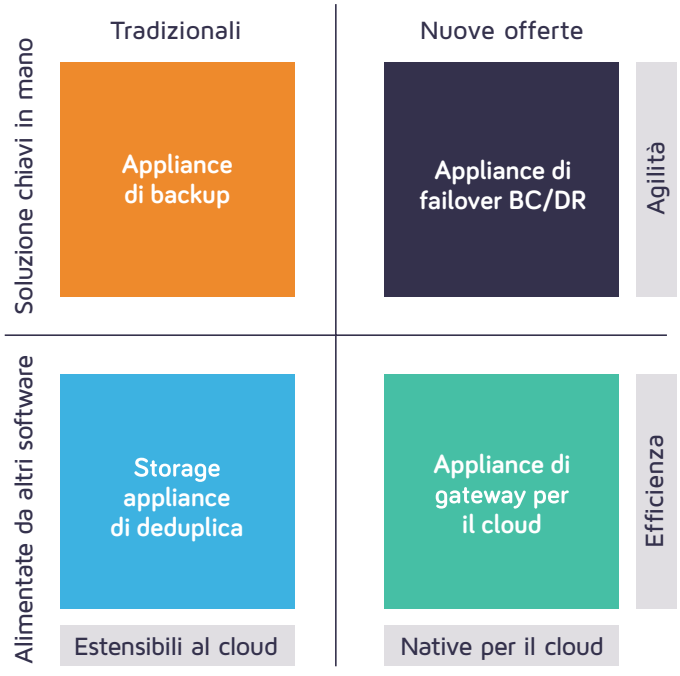
Tendenza da tenere d'occhio: appliance di failover e gateway per il cloud

Quando nel settore IT si parla di appliance di protezione dei dati appositamente progettate, ci si riferisce spesso alle appliance di backup tradizionali, quelle disponibili finora sul mercato.

Tuttavia, la crescita esplosiva dei dati, l'espansione delle funzionalità cloud e l'aspettativa da parte degli utenti di business di disporre di accesso ai dati continuo e da qualsiasi luogo, hanno fatto emergere due nuove categorie native per il cloud, che rappresentano la direzione attuale del mercato.

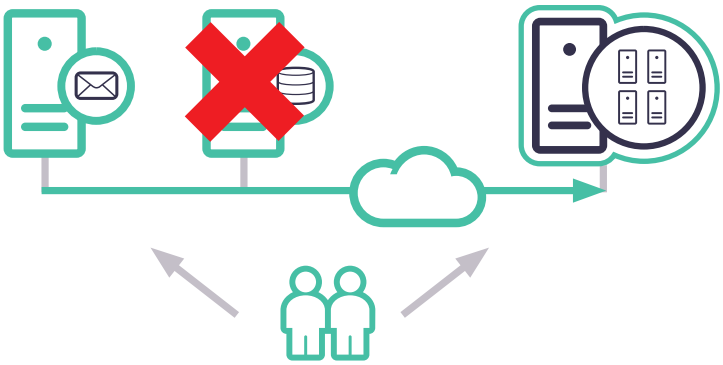
Si tratta delle appliance di failover per il backup e il disaster recovery e delle appliance di gateway per il cloud.

Qual è il valore di queste nuove categorie per l'infrastruttura di protezione dei dati aziendale?



Fonte: "Data Protection Appliances are better than PBBAs", Jason Buffington, Enterprise Strategy Group, 2014

Appliance di failover per backup e disaster recovery



Paragonando il ripristino dei dati a un esercizio di equilibrismo, le appliance di failover per backup e disaster recovery rappresentano la rete di sicurezza.

Queste nuove appliance di failover integrano software e hardware appositamente progettati per la disponibilità elevata.

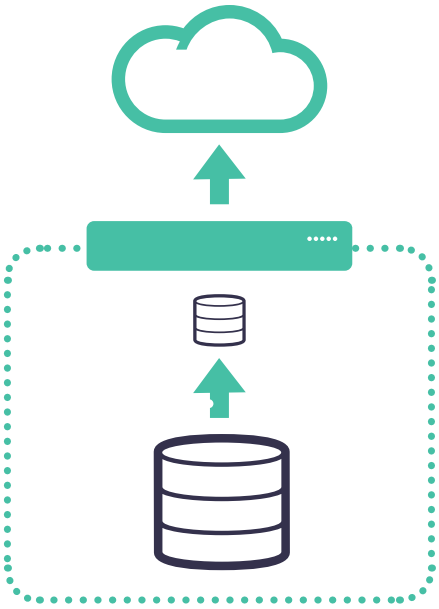
Vengono implementate localmente o in siti secondari, in modo che in caso di perdita di dati o errori di sistema sia possibile attivare rapidamente una macchina virtuale o un servizio all'interno dell'appliance, riducendo sia la perdita di dati che i tempi di inattività.

Ma c'è di più: il backup e il ripristino delle applicazioni business-critical sono così semplici che gli utenti finali non si accorgeranno affatto di essere stati reindirizzati a un sito di disaster recovery.

Queste appliance di failover offrono un elevato grado di automazione del processo di ripristino dei dati, certamente molto utile, e in genere offrono agli amministratori IT e ai provider di servizi gestiti (MSP) un valore maggiore per quanto riguarda gli SLA (Service Level Agreement).

In breve, se il Recovery Point Objective (RPO) è di pochi secondi, questo tipo di ambiente di disaster recovery (o DR), è un'assoluta necessità.

Appliance di gateway per il cloud



Le appliance di gateway per il cloud sono ben più di un'autostrada digitale verso un MSP o un servizio cloud, pubblico o privato. Sono infatti progettate e ottimizzate a livello nativo per la replica dei dati nel cloud.

Qual è il vantaggio?

Anche se i gateway cloud non sono tutti uguali, possono offrire alcune o tutte le caratteristiche seguenti:

- Crittografia integrata, per la massima sicurezza dei dati
- Storage locale, anche se limitato, con accesso istantaneo ai backup recenti memorizzati nella cache locale dell'appliance
- Deduplica, per la riduzione della larghezza di banda necessaria per la replica dei dati sul servizio cloud e i conseguenti notevoli risparmi

Non c'è dubbio: con l'aumento del numero di aziende che spostano i propri dati in ambiente cloud, queste appliance saranno sempre più richieste.

Capitolo 4:

Tendenza da tenere d'occhio: tecnologia di protezione dei dati unificata

L'approccio KISS (Keep it simple, stupid, ovvero rimani sul semplice, stupido) alla progettazione suggerito dalla marina militare degli Stati Uniti ormai negli anni '60 aveva davvero centrato il punto.

Sfortunatamente, si è iniziato ad applicare l'approccio KISS alle tecnologie di protezione dei dati solo di recente. Cosa si intende esattamente per protezione dei dati unificata?

Essenzialmente si intende una soluzione unica e leggera che non solo offre tutte le funzionalità necessarie per gli ambienti sia fisici che virtuali, ma che è stata progettata fin dall'inizio a questo scopo.

Cosa c'è alla base della richiesta di una tecnologia di protezione dei dati unificata?

Fino a pochissimo tempo fa, per la protezione dei dati era necessario un vero e proprio arsenale di prodotti di nicchia che consentissero di gestire la crescita esplosiva dei dati e la consumerizzazione dell'IT, prodotti che non comunicavano tra loro e producevano silos di dati senza alcuna flessibilità.

Per un certo periodo l'accumulo di soluzioni sovrapposte è riuscito a risolvere i problemi delle aziende, ma l'aggiunta di ulteriori soluzioni di nicchia per soddisfare le nuove esigenze e i nuovi livelli di servizio ha generato un mostro incontrollabile.

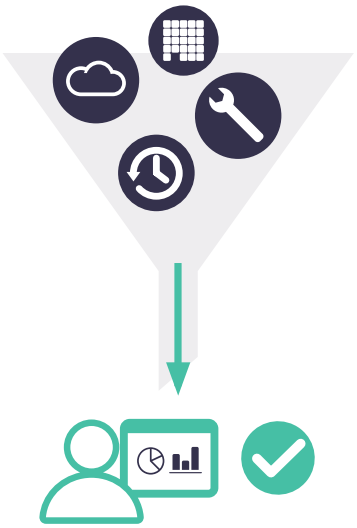
Questa situazione ha posto le piccole e medie aziende di fronte a una particolare sfida.

Le aziende di fascia enterprise possono contare su vaste competenze IT, anche molto specializzate in tecnologie e attività di protezione dei dati, ma le aziende di dimensioni più piccole non dispongono di reparti IT e budget di pari livello.

Devono invece fare affidamento su operatori IT generalisti che, oggi, grazie alla semplicità delle tecnologie di protezione dei dati unificata e a un unico dashboard di gestione, saranno in grado di implementare funzionalità di protezione dei dati di classe enterprise con una base di competenze comune.

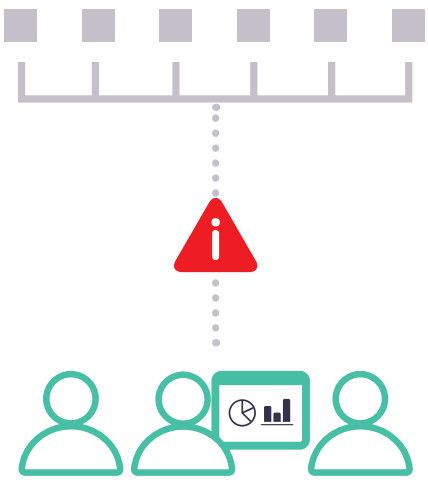
Approcci dei vendor alle tecnologie di protezione dei dati unificata

I principali approcci adottati dai vendor rispetto alla protezione dei dati unificata sono due:



Utilizzano elementi delle proprie tecnologie centrali di backup, deduplica, gateway cloud e ripristino e li riscrivono per creare una nuova soluzione unificata sul front-end e sul back-end.

Il risultato finale è un prodotto leggero e integrato, che offre tutte le funzionalità necessarie in un'unica posizione e un'esperienza di gestione semplificata.



Mettono insieme pacchetti di prodotti sperimentati e complementari di backup e ripristino, facilmente accessibili tramite un singolo portale di gestione. Anche se consente agli utenti di scegliere tra una gamma più ampia di applicazioni e di accedervi da un unico punto, questo approccio si traduce nella crescita rapida delle dimensioni del sistema durante il processo evolutivo, non sempre consente un'integrazione perfetta e richiede la gestione di ulteriori risorse.

È importante tenere presente che si tratta ancora di una tendenza emergente e che il livello di integrazione della tecnologia e la maturità delle interfacce sono in fasi di sviluppo diverse, dunque la ricerca va condotta con attenzione.

Capitolo 5:

Tendenza da tenere d'occhio: licenze all-inclusive

Licenze all-inclusive: mito o realtà?

Più che di una tendenza, si tratta di un messaggio pubblicitario. In realtà, per ora solo un numero ridottissimo di soluzioni è davvero all-inclusive, anche se il mercato sta iniziando a muoversi in questa direzione.

Perché?

In poche parole, i prezzi non sono chiari e i vendor che tenteranno di ridurre la confusione dei clienti e fornire un'esperienza più positiva cavalcheranno l'onda del cambiamento.

Quali sono le opzioni di licenza software all-inclusive attualmente disponibili?

Quando disponibili, le licenze di questo tipo possono essere basate su:

- Numero di server o socket
- TB di dati protetti

Se sono basate sulla capacità, quest'ultima può essere calcolata in base ai dati protetti prima o dopo la deduplica, un fattore che può incidere notevolmente sui costi.

Ciononostante, questi modelli di tariffazione consentono di eliminare le ambiguità e determinare rapidamente i probabili costi della soluzione.

E le licenze illimitate?

Sono piuttosto rare e il vendor può non essere in grado di fornire la capacità necessaria con il modello di tariffazione desiderato dal cliente, dunque bisogna fare attenzione a non creare una falsa economia.

Quali sono le offerte disponibili sul mercato?

È molto più probabile che i vendor concedano in licenza bundle delle funzionalità più diffuse, offrendo le funzionalità speciali sotto forma di componenti aggiuntivi a pagamento (in sintesi: spese nascoste). Questa situazione rende molto più difficile determinare il prezzo finale.

State valutando le appliance di backup con deduplica?

In alcuni casi le funzionalità extra, come crittografia, replica e accelerazione del backup, vengono fornite dietro pagamento di una tariffa aggiuntiva. In alcuni casi limitati, anche l'algoritmo o il software di deduplica rappresentano componenti aggiuntivi a pagamento. Si tratta invece di elementi che ci si aspetterebbe di trovare inclusi nel prezzo di un pacchetto "all-inclusive".

Siete interessati alle appliance di backup integrate fornite in bundle con licenze software?

Fate attenzione. Segondo DCIG*, poco più del 20% delle appliance integrate include tutte le caratteristiche e le funzionalità necessarie. Vi verranno fornite con un software di deduplica e una console, ma controllate se la licenza include anche replica, crittografia e software agente del sistema operativo o se queste funzionalità rappresenteranno costi aggiuntivi.

Informatevi al meglio

Indipendentemente dal tipo di licenza offerta, limitata o all-inclusive, è necessario prestare la dovuta attenzione e mantenere un atteggiamento di apertura: l'opzione di licenza migliore per l'azienda potrebbe non essere quella che immaginavate.

Parlando di dovuta attenzione, vi invitiamo a leggere **tutti i dettagli del contratto.**

* Arcserve (17 dicembre 2014). Trends in Data Protection with DCIG [Webinar]. Il documento è disponibile quí.

Capitolo 6:

Requisiti per l'architettura di prossima generazione

La protezione dei dati è diventata sempre più complessa e alcune soluzioni in commercio sono ormai obsolete. Come assicurarsi di non fare una scelta sbagliata?

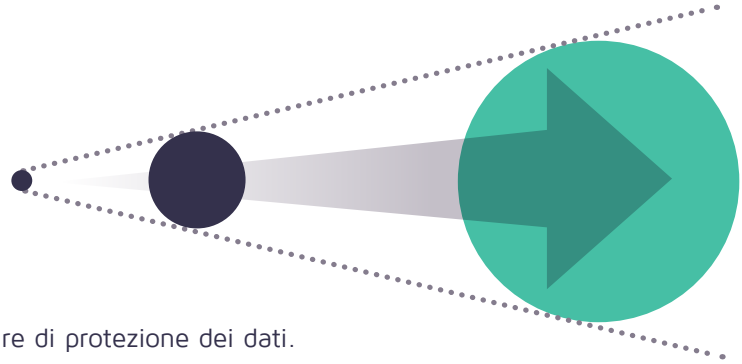
Le architetture di protezione dei dati di prossima generazione rappresentano un ottimo punto di partenza. Quando mantengono le loro promesse, rendono tutto più semplice. Sono accessibili e offrono un livello elevato di scalabilità e funzionalità complete.

Cosa aspettarsi man mano che queste soluzioni maturano?

Completezza della soluzione

Le architetture di prossima generazione vi forniranno tutte le principali tecnologie di protezione dei dati di cui avete bisogno all'interno di un'unica soluzione, tra cui:

Attualmente solo alcuni vendor sono in grado di fornire soluzioni solide come questa.



Scalabilità della soluzione

Ci aspettiamo molto dalle nuove architetture di protezione dei dati.

Non solo devono adattarsi a gestire volumi di dati più ampi, ma devono anche assicurare il rispetto degli SLA relativi ad esempio a RPO (Recovery Point Objective), RTO (Recovery Time Objective) e performance delle finestre di backup. In più, devono essere abbastanza flessibili da garantire il funzionamento su un'ampia gamma di piattaforme, su disco o nastro, on-premise, off-premise, nell'appliance o nel cloud.

Inoltre, devono essere modulari e scalabili, per adeguarsi alla crescita dell'azienda o a eventuali operazioni di fusione e acquisizione, continuando a fornire performance elevate.

Cosa vuol dire, in parole povere?

Potreste iniziare installando un software di protezione dei dati, in seguito, quando l'azienda cresce, acquistare un'appliance, e infine spostare parte dei dati nel cloud man mano che l'azienda matura.

Una soluzione altamente scalabile supporterà tutte e tre le operazioni, quando e dove è necessario.

Facilità d'uso della soluzione

Le architetture di protezione dei dati moderne devono essere semplici da implementare e allo stesso tempo facili da usare. Le soluzioni che non rispondono a questi requisiti di semplicità perderanno terreno a favore dei prodotti della concorrenza che invece lo fanno.

Cercate soluzioni che consentano di:

- Unificare molte tecnologie in un modo semplice da configurare
- Creare piani sulla base degli obiettivi RPO e RTO con la massima immediatezza e semplicità
- Permettere l'esecuzione di attività e workflow complessi "dietro le quinte"
- Consentire comunque il fine tuning delle funzionalità

Prezzo della soluzione

In passato solo le grandi aziende potevano beneficiare di un simile livello di protezione e ripristinabilità dei dati. Infatti, soltanto fino a due anni fa la deduplica e le console di gestione unificata erano funzionalità di livello enterprise.

Ora non più.

Oggi le tecnologie di protezione dei dati sono abbastanza flessibili da permettere svariate modalità di deployment. Consentono di ottimizzare l'efficienza e i costi operativi e sono offerte con modelli di licenza particolarmente convenienti

Capitolo 7:

Il panorama attuale del mercato

Abbiamo valutato il mercato e riteniamo che sia pronto a nuove soluzioni.

Quando la tecnologia di protezione dei dati è partita da un prodotto software, si è poi evoluta con l'offerta di infrastrutture ibride affamate di appliance e con l'emergere del cloud come destinazione.

Questa evoluzione ha avuto come risultato un gran numero di prodotti legacy ormai obsoleti. Alcuni hanno costi di licenza eccessivi, altri non consentono di misurare le inefficienze dei processi. Poi ci sono quelli non scalabili oppure carenti in termini di facilità d'uso. Altri ancora sono soluzioni di nicchia, che per fornire le robuste funzioni di protezione dei dati e ripristinabilità oggi necessarie devono essere accoppiate ad altre, aggravando la complessità.

In ogni caso, queste soluzioni limitano la capacità dell'IT di erogare in modo costante servizi di qualità elevata agli utenti finali.

Cosa vuol dire per un vendor offrire una vera soluzione di prossima generazione?

Prima di tutto, vuol dire mettere da parte il software legacy e le soluzioni adattate in retrofitting.

I vendor più lungimiranti guardano all'attuale panorama di protezione dei dati nel suo complesso e stanno realizzando nuove tecnologie integrate altamente flessibili, adattabili e configurabili.

Cosa offre attualmente il mercato?

Se siete pronti a cimentarvi nella ricerca di una soluzione, badate bene: non tutti i vendor hanno iniziato ad allineare le proprie soluzioni alle nuove, pressanti esigenze.

Oggi:

22 **vendor offrono 26 soluzioni software per il backup di server virtuali**

10 **vendor offrono 47 appliance di backup con deduplica**

14 **vendor offrono 72 appliance di backup integrate**

E queste cifre non prendono in considerazione le appliance di backup con deduplica e integrate disponibili anche come appliance virtuali.

Naturalmente, nel mare dei vendor emergono chiaramente dei leader.

Si tratta di:

- Arcserve® UDP
- CommVault® Simpana®
- Dell® AppAssure
- Symantec Backup Exec™
- UniTrends™
- Veeam®

Con un numero così elevato di provider che propongono sul mercato così tante soluzioni, individuare quella giusta può essere come trovare il proverbiale ago nel pagliaio.

Eppure, vale la pena di impegnarsi a fondo nella ricerca.

Un'architettura di prossima generazione che offre una soluzione completa, scalabilità e facilità d'uso vi permetterà di affrontare al meglio le sfide attuali e migliorare le efficienze da ogni punto di vista.

Capitolo 8:

Acquisto di una soluzione di prossima generazione

Quando si valutano le varie soluzioni disponibili sul mercato e quindi si esaminano in dettaglio le caratteristiche e le funzionalità offerte da ciascuna di esse, fare un confronto diretto può essere complicato.

Il compito si complica ulteriormente quando i vendor sono poco chiari rispetto alle caratteristiche incluse e non incluse nel prezzo di listino pubblicizzato.

Quali sono dunque gli aspetti da considerare nella valutazione delle opzioni?

Non lasciatevi abbagliare e scoprite quali sono le caratteristiche effettivamente incluse.

Non mancate di chiedere:

- La soluzione è disponibile come appliance fisica, virtuale o entrambe?
- La soluzione offre una console di gestione unificata?
  - In caso affermativo, a che punto è il vendor nel processo di sviluppo?
  - Quanto profondamente la console si integra con le varie appliance che dovrete gestire?
  - Prima di firmare un contratto, eseguite un test di integrazione o assistete a una dimostrazione per verificare che la soluzione sia all'altezza delle promesse del vendor.
- La soluzione è dotata di un'appliance gateway cloud per il backup, lo storage dei dati e il ripristino in ambiente cloud?
- Se il set di funzionalità della soluzione comprende la deduplica, è lato origine o lato destinazione? O entrambe le opzioni?
- La soluzione è dotata di appliance di failover per backup e disaster recovery e offre il ripristino istantaneo?

Per quanto riguarda la licenza, leggete tutti i dettagli del contratto con la massima attenzione.

Ponete domande come:

- La licenza è all-inclusive? In caso affermativo, il vendor è in grado di rispettare quanto promette?
- Il vendor concede in licenza un set di funzionalità più limitato? In caso affermativo, qual è il prezzo finale dopo l'aggiunta delle funzionalità speciali di cui avete bisogno?

Quali sono gli altri aspetti da considerare?

Vi invitiamo a prestare particolare attenzione alle caratteristiche che le architetture di protezione dei dati di prossima generazione possono, e devono, offrire.

Si tratta di:

- Completezza della piattaforma: un unico punto di riferimento per tutte le esigenze di protezione dei dati
- Tecnologie unificate: integrazione semplice e immediata ed eliminazione dei silos di dati impenetrabili
- Virtualizzazione: macchine virtuali che consentano di eseguire più applicazioni e sistemi operativi su un singolo server fisico
- Facilità d'uso: progettazione incentrata sull'utente, che consenta il deployment e la gestione della soluzione da parte dei generalisti IT
- Failover/BMR istantaneo: disponibilità elevata e disaster recovery per garantire la business continuity
- Replica: miglioramento della fault tolerance grazie alla replica automatizzata dei dati
- Nastro/Archivio: supporto della replica su nastro per una maggiore affidabilità
- Riduzione dei dati: deduplica basata sulla destinazione oppure lato origine più efficiente, per ridurre il volume totale dei dati da proteggere
- Servizio cloud: migliore capacità di spostamento dei dati nel cloud e di gestione

Ecco un confronto tra le principali soluzioni

	Arcserve UDP 8000	CommVault	Dell	Unitrends	Veeam
COMPLETEZZA DELLA PIATTAFORMA					
Unificata					
Virtualizzazione					
Facilità d'uso					
Failover/BMR istantaneo					
Replica					
Nastro/Archivio					
Riduzione dei dati					
Servizio cloud					

Fonte: Arcserve

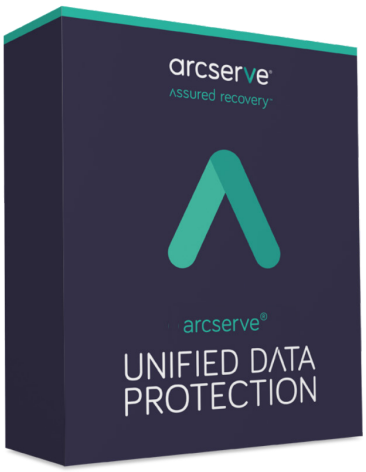
Naturalmente nessuna soluzione è adatta a qualsiasi azienda, dunque, armati dei requisiti della vostra architettura, indagate attentamente per trovare quella che fa per voi.

Capitolo 9:

Arcserve UDP

È in gioco la vostra reputazione. Siete disposti a lasciarla al caso?

Con Arcserve Unified Data Protection di nuova generazione, o Arcserve UDP, potete contare sulla prima soluzione del settore per la protezione completa dei dati, completa di Assured Recovery™ e funzionalità native del cloud.



Vantaggi

Arcserve UDP risolve le complessità del lavoro quotidiano, con vantaggi come:

- **Una protezione dati e un'architettura di recovery semplificate, da gestire facilmente e da impostare una volta sola.**
- **Una protezione per il sistema e i dati molto migliorata, che comprende opzioni di recovery delle soluzioni legacy.**
- **Deciso miglioramento dell'efficienza operativa e riduzioni dei costi.**

Il valore di Arcserve UDP

Arcserve UDP è una soluzione chiavi in mano che offre software di protezione e ripristino dei dati completo di funzionalità di backup, replica e vera deduplica globale in dotazione standard. In più, Arcserve UDP è dotato della console di gestione più unificata del settore ed è la soluzione di protezione dei dati basata su immagini più integrata oggi in commercio.

Arcserve UDP offre inoltre:

- Tecnologie di failover per backup/disaster recovery e disponibilità elevata, con supporto di tre macchine virtuali in standby
- Funzionalità software native del cloud che consentono di replicare i dati per i servizi cloud pubblici e privati e per Service Provider.
- Protezione per server virtuali e fisici, l'unica soluzione software unificata sul mercato che è in grado di farlo.
- Software per il testing DR automatizzato di sistemi, applicazioni e dati business- critical, senza tempi di inattività e senza alcun impatto sui sistemi di produzione
- Licenze software all-inclusive basate su socket di CPU (sia per fisico che virtuale) o per TB di dati protetti