N-ABLE™

Cove Data Protection™

Guida completa al ROI della protezione dei dati

Ecco spiegato l'approccio dei professionisti IT di successo e come adottarlo

E-book

Sommario

Quando l'attività aziendale si basa sui dati, la protezione è fondamentale

Tutte le aziende, dalle società di grandi dimensioni fino alle piccole imprese, dipendono dai dati. Ecco perché le tradizionali soluzioni di backup si sono evolute fino a diventare soluzioni di protezione dei dati, una tutela indispensabile contro la perdita dei dati.

Le aziende abbastanza grandi da poter disporre di team IT dedicati tendono ad essere ben protette, mentre le piccole e medie imprese (PMI) sono spesso carenti sotto questo aspetto.

Molte PMI ricorrono a un miscuglio di sistemi di backup approssimativi e inaffidabili. Queste aziende sono spesso attente ai costi, pertanto può risultare difficile convincerle ad adottare una nuova soluzione. Anche se leggono i giornali, non sempre sono consapevoli dei rischi da affrontare o delle conseguenze di un'eventuale perdita di dati.

E allora, in che modo i professionisti IT possono superare tali ostacoli e sfruttare tutte le opportunità offerte dal backup? Implementando non l'ennesimo prodotto per il backup, ma qualcosa di ben più prezioso: un servizio completo di protezione dei dati.

Qual è la differenza tra backup e protezione dei dati?

La protezione dei dati fa riferimento a una vasta gamma di funzionalità che vanno ben oltre la semplice esecuzione di un backup. Tipicamente include backup, disaster recovery e archiviazione. Le aziende oggi esigono dai propri reparti IT i seguenti servizi:

- Protezione dei dati contro perdite e compromissioni derivanti da errori umani, attacchi dannosi e interruzioni del servizio
- Decisioni basate sui requisiti vigenti in materia di sicurezza dei dati, privacy e governance
- Disponibilità dei dati quando serve e relativo ripristino immediato in caso di emergenza, con tempi di inattività minimi

La protezione dei dati può comprendere servizi costituiti da elementi molto diversi tra di loro, pertanto svolge un ruolo chiave nella dimostrazione del ROI ai tuoi team:

Modello reattivo	À la carte	Modello proattivo	Gestito
Supportare qualsiasi software di backup già utilizzato dal cliente.	Vendere software o un servizio di base come voce mensile per offrire una gestione continua di backup e reportistica.	Venduto come parte di un pacchetto (per utente, per dispositivo) per fornire backup continuo, reportistica e test del ripristino, nonché il ripristino se necessario.	Venduto come parte di un pacchetto (per utente, per dispositivo) per fornire backup continuo, reportistica e test del ripristino, nonché il ripristino con livelli SLA (contratto di servizio) definiti.
€	€€	€€€	€€€€

Più ci si avvicina al versante "gestito" del grafico, maggiore è il potenziale di profitto e il valore offerto alla clientela.

Chiarezza degli obiettivi

Molti titolari di imprese hanno impiegato 10, 20 o 30 anni per creare la propria infrastruttura e contano su di te per portare avanti la loro attività.

È uno dei motivi principali per cui devi offrire loro più di un semplice software di backup.

Come dimostrare il ROI della protezione dei dati?

Malgrado le problematiche inerenti al mercato delle PMI, la creazione di un servizio di protezione dei dati non deve risultare complicata. Semplicemente, sono necessari il corretto approccio e la giusta soluzione.

Il corretto approccio può essere suddiviso in tre fasi:

1. **Comprendere** le esigenze e le prospettive aziendali
2. **Far comprendere** all'azienda il valore dei suoi dati
3. **Creare** una soluzione su misura per le esigenze e il budget delle parti interessate

Per un approfondimento su ciascun passaggio, continua a leggere.

È utile sapere che...

Le piccole aziende sono vittime di **circa la metà (43%)** di tutte le violazioni di dati[1].

[1] "2019 Data Breach Investigations Report", Verizon, https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf (consultato a luglio 2019).

Comprendere le esigenze e le prospettive aziendali

Come capire se la mia azienda necessita di una protezione dei dati?

Molti responsabili IT tendono a proporre una soluzione nel momento esatto in cui viene identificato il primo requisito. Invece la mossa migliore consiste nel prendere tempo.

Fai una pausa e poni domande per fare in modo di comprendere veramente l'azienda e le esigenze delle principali parti interessate. Occorre capire i loro obiettivi e presupposti per scoprire gli aspetti più importanti per loro e poter offrire la soluzione ottimale.

In termini commerciali, questa viene definita la **fase esplorativa.**

Oltre a saperne di più circa le esigenze aziendali, è anche necessario cogliere questa opportunità per capire meglio dove risiedono i dati delle parti interessate. Numerose PMI archiviano dati su notebook e su applicazioni SaaS come Microsoft 365®; di conseguenza, non sono solo i server a necessitare di backup.

Fai in modo di conoscere a pieno l'impatto che una perdita significativa di dati avrebbe sull'attività dell'azienda e il tempo necessario per riprodurre i dati in questione. Dovrai tenere presenti i requisiti normativi in materia di privacy dei dati ai quali l'azienda può essere vincolata (ad esempio il GDPR) e le conseguenze che potrebbero derivare dalla mancata conformità.

Una volta acquisite tali informazioni, sarai in una posizione privilegiata per individuare con esattezza i punti in cui la protezione dei dati è necessaria. Potrai inoltre valutare con maggiore efficacia il sistema di backup esistente e attirare l'attenzione sulle aree da migliorare.

Ricorda: l'esperto sei tu

I tuoi dirigenti ti hanno assunto per la tua esperienza e perché tu possa garantire loro un'affidabile consulenza informatica. In definitiva, è probabile che non siano interessati al tipo di soluzione di protezione dei dati che stai utilizzando. La marca non conta, l'essenziale è che sia una soluzione funzionale ed efficace.

Attraverso la fase esplorativa, è possibile offrire una soluzione affidabile e in grado di soddisfare le esigenze dell'azienda, guadagnando la sua fiducia nel lungo periodo.

Quesiti da porre nella fase esplorativa

Per iniziare:

- Qual è l'approccio attuale per la protezione del business?
- L'azienda è mai stata colpita da ransomware o altro malware?
- Ci sono stati tempi di inattività nelle procedure operative aziendali? Quale è stato il loro effetto?

- L'impatto dei tempi di inattività sull'azienda è fonte di preoccupazioni?
- Esiste una soluzione in caso di indisponibilità dei sistemi o dei dati?
- Come è cambiato il modo in cui l'azienda si affida ai sistemi informatici negli ultimi cinque anni?
- La nostra azienda potrebbe operare se dovesse tornare provvisoriamente a metodi manuali/cartacei? Per quanto tempo?
- La nostra situazione attuale è fonte di preoccupazione?
- Quali sono gli obiettivi per i prossimi due anni? Qual è l'approccio per modernizzare e far crescere l'attività aziendale?

Per approfondire:

- Quante transazioni vengono completate generalmente in un'ora? Quale sarebbe il costo orario dei tempi di inattività?
- Quali responsabilità legali sono previste se i servizi diventassero improvvisamente non disponibili?
- Realisticamente per quanto tempo è possibile andare avanti senza accedere ai dati?
- Quale sarebbe l'impatto sulla reputazione dell'azienda se non si riuscissero a svolgere attività per un giorno? E per una settimana?
- Quali procedure e applicazioni aziendali sono più essenziali e quindi più importanti da ripristinare in caso di problemi tecnici?
- Quali sistemi e dati di base sono necessari per ripristinare l'operatività di queste applicazioni critiche? Su quali server o dispositivi si trovano tali sistemi e dati?

Infine prendi in considerazione le altre applicazioni aziendali e tipologie di dati:

- Quali potrebbero essere indisponibili per un periodo più lungo senza avere un impatto significativo sull'attività?
- Quanto costerebbe (in termini di tempi di lavoro e stipendi) ricreare i dati meno importanti se andassero completamente perduti?

Parla in modo chiaro

A seconda del livello tecnico delle parti interessate, probabilmente è meglio non ricorrere a termini come **RTO** (Recovery Time Objective) o **RPO** (Recovery Point Objective). È sufficiente sapere che, tramite le domande poste, stai sostanzialmente definendo tali qualità.

Far comprendere all'azienda il valore dei suoi dati

Come convincere la mia azienda della necessità della protezione dei dati?

Non iniziare cercando di vendere un prodotto o una soluzione specifica alle parti interessate. Per convincerli della necessità della protezione dei dati, occorre insegnare loro il valore dei dati archiviati su server e dispositivi e spiegare che l'eventuale perdita di tali dati potrebbe danneggiare seriamente l'attività aziendale.

La discussione può essere suddivisa essenzialmente in due parti:

La perdita di dati è un'eventualità possibile

Le modalità con le quali le attività commerciali possono perdere presentazioni, report finanziari e altri file importanti sono numerose. Danneggiamento dei file, errori hardware, errori umani, attacchi malware, cancellazione accidentale o catastrofi naturali: sono tutte situazioni che mettono a rischio qualsiasi attività. Sebbene le parti interessate possano scartare l'idea che inconsapevolmente potrebbero distruggere un file importante, l'eliminazione accidentale è, in effetti, una delle forme più comuni di perdita di dati. Inoltre, avranno certamente letto sui giornali di varie aziende paralizzate da ransomware e devono essere consapevoli che, prima o poi, potrebbero trovarsi nella stessa situazione.

La produttività ne soffre

Un file essenziale andato perso impone che venga creato nuovamente, il che fa perdere ore di lavoro che invece potrebbero essere utilizzate per altre attività critiche. Ciascuna azienda dispone di dati importanti che sarebbe difficile o, in alcuni casi impossibile, ricreare. Mesi o anni di informazioni finanziarie sono insostituibili, tuttavia molte attività memorizzano la propria contabilità o altri dati critici su una singola workstation, senza alcun duplicato.

È utile sapere che...

Come conseguenza di una perdita importante di dati[2]:

- Il 19% delle PMI ha avuto un tempo di inattività del sistema inferiore a un'ora
- Il 41% ha avuto un tempo di inattività di 1-8 ore
- Il 40% ha avuto un tempo di inattività di oltre 8 ore

[2] "Cisco Cybersecurity Special Report – Small and Mighty: How Small and Midmarket Businesses Can Fortify Their Defenses Against Today's Threats," Cisco. https://www.cisco.com/c/dam/en/us/products/collateral/security/small-mighty-threat.pdf (consultato a luglio 2019).

Conoscere i costi reali del downtime

Quando si sostiene la "causa" della protezione dei dati, occorre utilizzare un termine chiaro per qualsiasi dirigente di azienda: denaro.

Due aspetti che giustificherebbero rapidamente l'acquisto della protezione dei dati sono le perdite di dati che si traducono in gravi perdite finanziarie o di dati che impiegherebbero ore o addirittura giorni per essere ripristinati o sostituiti (con conseguente impiego di tempo e risorse da parte dei dipendenti).

Per rendere tutto più concreto, chiedi alle parti interessate di immaginare uno scenario in cui i sistemi sono completamente fuori uso e i dati inaccessibili, quindi calcolane i costi. A confronto, una soluzione di protezione dei dati risulterà molto più conveniente.

A supporto della conversazione è possibile ricorrere all'esempio seguente:

Azienda di progettazione con 25 dipendenti

Ricavi pari a 100.000 € per dipendente ogni anno

25 dipendenti X 100.000 € all'anno = 2,5 milioni di € di ricavi totali ogni anno

250 giorni lavorativi all'anno = 400 € di ricavi al giorno

400 € X 25 dipendenti = 10.000 € di ricavi al giorno

IMPATTO TOTALE:

Perdita di produttività pari a 10.000 € al giorno

Rimedio: 800 € al giorno

Costi per i danni alla reputazione: incalcolabili

- Cosa succede se un progetto non viene consegnato?
- Cosa succede se si perde un cliente?
- Qual è l'impatto del passaparola?

Altri tipi di rischi

Oltre ai rischi finanziari, quali calo di produttività, costi di correzione dei problemi e danni alla reputazione, esistono altre tipologie di rischi che la tua azienda si aspetta che tu risolva.

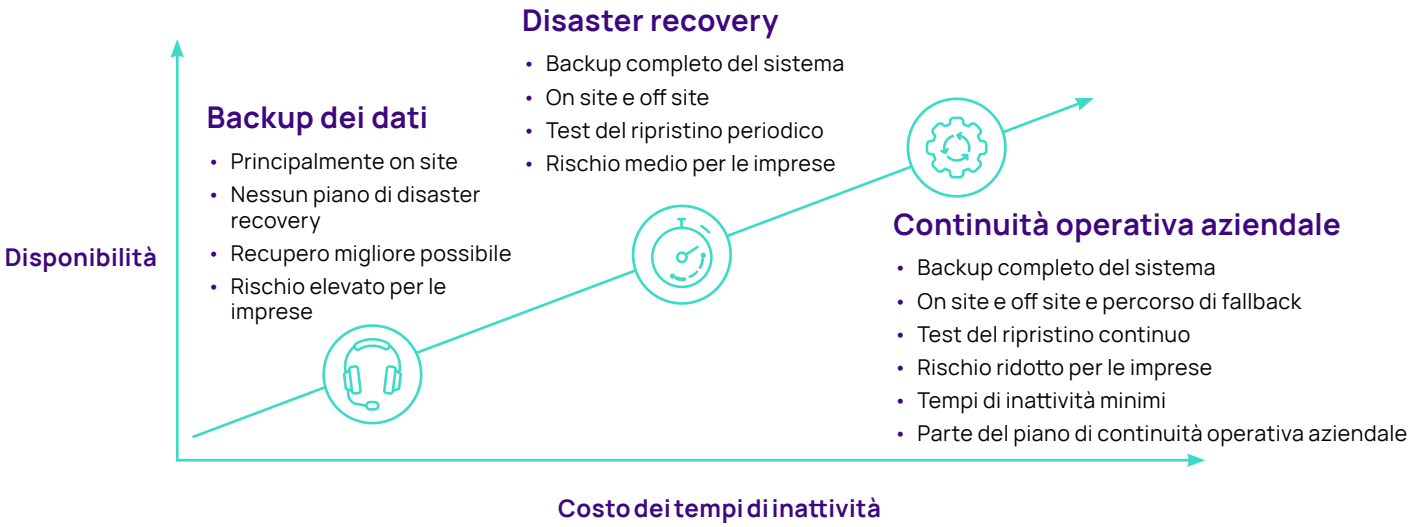
Ad esempio, l'azienda deve rispettare normative stringenti in materia di privacy dei dati, sicurezza e archiviazione? Quali conseguenze potrebbero esserci in caso di perdita o furto di dati personali, finanziari o medici?

Creare una soluzione su misura per le esigenze e il budget dell'azienda

Esiste una soluzione adatta a tutti?

Per farla breve, no. Non tutti i reparti o i dispositivi hanno bisogno di avere (o possono permettersi) lo stesso livello di protezione. Ecco perché è importante allineare le tue aspettative e i tuoi requisiti al tema della disponibilità e dei tempi di inattività.

Osserva il seguente "modello evolutivo":



Attualmente a che punto siamo in termini di soluzioni di backup, ripristino o protezione dei dati implementate? Siamo in grado di soddisfare le esigenze dell'azienda in ogni aspetto del modello? Se sì, è probabile che riscontrerai un ROI più elevato.

Consiglio pratico

Dopo aver individuato un approccio corretto per vendere la protezione dei dati a un determinato reparto, spesso potrai adottare metodi simili anche per altri reparti.

Come faccio a soddisfare le esigenze di tutte le parti interessate?

L'offerta di un'unica soluzione faciliterebbe il lavoro dei tecnici, ma si tradurrebbe in un'esperienza alquanto scadente. Allo stesso tempo è vero che, se dovessi creare soluzioni completamente personalizzate per ogni reparto, la situazione diventerebbe alquanto difficile da gestire.

Tuttavia, offrendo **due o tre livelli di servizio**, è possibile gestire in modo efficace i requisiti di ripristino e di budget della maggior parte dell'azienda.

Con la creazione di opportuni dati adatti ai diversi livelli di servizio (ad esempio a basso costo, fascia media, fascia alta), potrai mettere a disposizione dei reparti una protezione dei dati efficace e sufficiente per esigenze e tipi di dati specifici. Ecco un esempio:

Buona	Migliore	Ottimale
• Backup completo del sistema • Un backup al giorno • Conservazione per 28 giorni • Archiviazione off site	• Backup completo del sistema • Due backup al giorno • Conservazione per 60 giorni • Archiviazione off site • Backup ibridi per ripristini più rapidi • Archiviazione mensile • Test di ripristino trimestrale	• Backup completo del sistema • 12 backup al giorno • Conservazione per 90 giorni • Archiviazione off site • Backup ibridi per ripristini più rapidi • Archiviazione mensile • Test di ripristino mensile • VM in standby con schermata giornaliera
Per i dati meno importanti (o budget molto limitati), è possibile proporre soluzioni di base per il ripristino entro 24 ore e diverse sedi di ripristino.	A questo livello, puoi proporre il ripristino su cloud, con la possibilità di ripristinare l'operatività entro 4-12 ore.	Un server completo di standby a caldo è disponibile per il ripristino immediato di dati e applicazioni più critici.

Con queste diverse opzioni di servizio, le parti interessate potrebbero scegliere di proteggere diverse tipologie di dati a diversi livelli.

Quali sono le caratteristiche da ricercare in una soluzione per la protezione dei dati?

In ultima analisi, il successo dipende dall'offerta della soluzione più idonea per la protezione dei dati: quella che soddisfa le esigenze aziendali in termini di costi e funzionalità.

Lo strumento ideale di protezione dei dati deve essere sufficientemente flessibile e configurabile per essere offerto in più livelli di servizio. Inoltre, deve essere:

Semplice da implementare e da utilizzare

È necessario poter gestire i dati nel modo più efficiente possibile. Cerca una dashboard multitenant basata su web che consenta ai tecnici di visualizzare tutti i tipi di dati in diversi ambienti a colpo d'occhio, controllando lo stato del backup di ogni server e dispositivo gestito e quindi analizzando i problemi nel dettaglio con un solo clic. La protezione dei dati offerta come applicazione SaaS in hosting completo ti fa risparmiare tempo altrimenti speso per server delle applicazioni, patch, aggiornamenti, ecc.

Versatile

La soluzione deve essere in grado di eseguire il backup e il ripristino dei dati da qualsiasi luogo, su server e workstation fisici e virtuali e su cloud come componente di applicazioni SaaS, quali Microsoft 365. Deve proteggere i dati nella gamma completa di sistemi operativi e hypervisor Ed essere anche in grado di garantire qualsiasi forma di ripristino, tra cui ripristini a livello di file/cartella, ripristini bare metal e immagini di standby per un failover rapido in qualsiasi momento.

Basata su cloud

Una copia on-site del tuo backup è utile per il ripristino rapido, ma l'archiviazione in locale è soggetta alle stesse vulnerabilità degli altri sistemi IT on-premise. Infatti, i ransomware spesso mirano in modo specifico ai file di backup archiviati sulla rete locale, sottoponendoli per primi a crittografia. Ecco perché una soluzione che invia i tuoi backup su cloud è l'opzione migliore. La soluzione ideale offrirà entrambe le soluzioni, inviando i backup prima ad uno storage remoto sicuro e fornendo l'opzione di conservare una copia aggiuntiva locale a seconda delle necessità. I tradizionali prodotti per il backup che hanno aggiunto il cloud come funzionalità secondaria potrebbero non essere sufficienti, ma i prodotti basati su cloud come N-able™ Cove Data Protection™ sono abbastanza efficienti per prendere un backup incrementale e inviarlo al cloud con una frequenza di 15 minuti, senza una costosa appliance che fa da intermediario.

Utilizzando un'unica soluzione che offre tutte queste funzionalità sarà più facile fornire i livelli di servizio per soddisfare le diverse esigenze. Ridurrai inoltre il costo di fornitura dei servizi tramite una migliore efficienza e automazione.

Migliora la produttività del personale tecnico

Passare da un prodotto per il backup all'altro può aumentare le ore lavorate in una settimana per i tecnici. Ridurre il numero di prodotti e dashboard per il backup da supportare può comportare reali vantaggi per la produttività e liberare i tecnici, in modo che possano occuparsi di attività più utili, interessanti e coinvolgenti.

Trucchi e suggerimenti per dimostrare il ROI

Qual è il momento migliore per parlare della protezione dei dati?

Quando si verifica un'emergenza, gli utenti e i dirigenti inevitabilmente ti chiameranno, aspettandosi da te un intervento risolutivo. A quel punto, è ormai troppo tardi per parlare della protezione dei dati. Se non stanno ancora utilizzando una soluzione idonea, le opzioni per aiutarli risulteranno estremamente limitate.

Qual è il modo migliore per evitare un simile scenario? **Non aspettare**. In occasione della successiva riunione strategica, inizia a parlare della protezione dei dati. Se possibile, fallo durante un incontro di persona anziché al telefono o tramite e-mail, per sottolineare la serietà dell'argomento. Prendi l'iniziativa e illustra passo dopo passo la soluzione di protezione adatta alle esigenze aziendali specifiche.

Come giustificare il passaggio da un backup di base a una soluzione più avanzata

Se recentemente l'azienda ha perso dei dati e ha avuto problemi nel ripristinarli mediante il sistema in uso, avrai l'occasione giusta per spiegare in che modo una soluzione di protezione dei dati più avanzata avrebbe potuto evitare un simile scenario.

Verifichi e analizzi regolarmente il corretto funzionamento dell'ambiente IT delle parti interessate? Fornisci report puntuali sui backup e riesci a stabilire come il suo sistema attuale potrebbe non offrire le garanzie necessarie in termini di storage remoto o ripristino affidabile? Dalla tua ultima valutazione, l'azienda ha adottato nuovi servizi o piattaforme oppure ha trasferito su cloud alcune delle applicazioni critiche per l'attività aziendale?

Ognuno di questi punti rappresenta un'opportunità per educare e per giustificare il ROI di una soluzione di protezione dei dati più evoluta e completa.

Il passaggio a una soluzione più avanzata prevede che si inizi con il proporre per prima l'opzione di livello intermedio/"migliore". Se il tuo interlocutore esita a causa del prezzo, puoi sempre offrire l'opzione a costo inferiore. E se dovesse decidere per un maggiore livello di protezione, assicurati che stia assecondando le necessità di ogni reparto o dispositivo critico.

Sfrutta le notizie a tuo vantaggio

Le notizie di cronaca su violazioni dei dati, ransomware e altri attacchi informatici possono rappresentare un utile punto di riferimento durante le conversazioni con le parti interessate.

Non esitare a sottolineare cosa è successo ad aziende che hanno perso tutti i dati e spiega che hai intenzione di fare tutto il possibile per evitare che si trovino nella stessa situazione.

Come gestire eventuali obiezioni?

Alcune aziende attente ai costi possono esitare a finalizzare l'investimento. Spesso faranno improbabili confronti, ossia potrebbero aver svolto una rapida ricerca online e scoperto un prodotto per il backup veramente economico, senza riuscire a comprendere perché la tua soluzione completa di protezione dei dati non abbia lo stesso prezzo.

Il tuo compito consiste nell'insegnare loro la differenza tra le due soluzioni e come il servizio di protezione dei dati che suggerisci sia molto di più che un semplice software di backup.

Sarà necessario spiegare con chiarezza che, oltre al software e all'archiviazione, viene fornita una protezione completa, comprensiva di monitoraggio e test dei backup, continuità operativa aziendale e ripristino dei dati con una chiamata se si verifica un problema.

Potresti anche presentare il tuo suggerimento come una sorta di polizza assicurativa da pagare ogni mese, che consente di stare tranquilli poiché offre la copertura adeguata in caso di emergenza. In definitiva, l'azienda non rinuncerebbe mai all'assicurazione sulla propria attività. E allora perché non dotarsi di un servizio di protezione per i dati?

Il prezzo non costituisce mai un'obiezione

Anche se qualcuno ha da obiettare sul prezzo del servizio, quando inizierà a rispondere alle tue domande, quasi sempre capirai che i suoi dubbi non provengono affatto da questo aspetto della questione. Concentrandoti sul valore dei tuoi servizi, è più facile che tu riesca a placare i dubbi delle parti interessate.

Come reagire a un rifiuto

Se la conversazione non va come sperato e il tuo interlocutore si rifiuta comunque di investire anche nel livello di protezione più basilare, ti restano tre opzioni:

- Prepara una liberatoria in cui dichiari esplicitamente di non poter essere ritenuto responsabile in caso di perdita dei dati e se non è stata implementata una soluzione adeguata di backup. La richiesta stessa di firmare questo documento indurrà molte delle parti interessate a riflettere attentamente e a riconsiderare la propria decisione.
- Configura il tuo prodotto per la protezione dei dati in background lavorando con ridotti budget trimestrali. In questo modo, sarai l'unico in grado di risolvere eventuali problematiche, offrendo allo stesso tempo la possibilità di passare a servizi di protezione dei dati di livello superiore, se necessario. Con un approccio del genere, non richiedi specificamente il budget e la priorità del servizio, ma ne includi l'importo nelle operazioni di base.
- Inserisci un piano di protezione dei dati di come parte standard delle operazioni. Evita che l'acquisto di una soluzione tanto importante resti facoltativo. Al fine di poter svolgere le normali operazioni aziendali, chiedi a tutti i reparti di sottoscrivere almeno un servizio di protezione dei dati di base, da inserire come voce in ogni budget. Se il tuo interlocutore manifesta dei dubbi, puoi discutere con lui dei livelli di protezione e dei prezzi disponibili.

Rivolgiti a un professionista

Anche se si sceglie di redigere una liberatoria autonomamente, è consigliabile farsi aiutare da una parte terza, oltre a richiedere una consulenza gratuita da un terzo per confrontare i risultati, per mostrare che non si tratta solo della tua opinione.

Vuoi migliorare la protezione dei tuoi dati? Siamo qui per questo!

Per sfruttare al meglio i consigli forniti nella presente guida, sarà necessario offrire a tutti gli interessati un'eccellente soluzione di protezione dei dati.

Cove Data Protection è una moderna soluzione di protezione dei dati basata su cloud e sufficientemente efficace per gestire dati di qualsiasi tipo e dimensione; supporta inoltre tutte le tipologie di ripristino, dai singoli file eliminati ai sistemi completi. In un unico prodotto, avrai a disposizione un software di backup, lo storage cloud e una dashboard basata su web per gestire tutta la tua attività, nonché la flessibilità di offrire più livelli di servizio per soddisfare al meglio le esigenze delle parti interessate. Sicuramente apprezzerai backup, disaster recovery e archiviazione con storage cloud completamente gestito nella tua area geografica.

Per ulteriori informazioni consulta la pagina https://www.n-able.com/it/products/cove-data-protection/backup

Forniamo inoltre assistenza commerciale e tecnica per permetterti di fornire un pacchetto completo di protezione dei dati.