Acronis

WHITE PAPER

# Esecuzione e scalabilità dei servizi DLP: una guida per gli MSP

Per anni, le aziende di ogni dimensione hanno incontrato difficoltà nel contrastare i rischi di perdita dei dati, malgrado l'aumentata consapevolezza, i protocolli di sicurezza e le normative. Il problema non accenna a diminuire: secondo l'analisi di fine anno di Risk Based Security dal titolo "Data Breach QuickView", nel 2021 sono stati esposti oltre 22 miliardi di record. Il 2021 si colloca quindi al secondo posto, dopo il 2005, per il volume di dati riservati compromessi. La stragrande maggioranza di questi record sono stati esposti a causa di una fuga di dati, ovvero una violazione della sicurezza che causa la diffusione deliberata o involontaria di dati riservati, sensibili o protetti in un ambiente non affidabile o a utenti non autorizzati, all'esterno o all'interno dell'organizzazione.

# Le cause della perdita dei dati sono sostanzialmente due

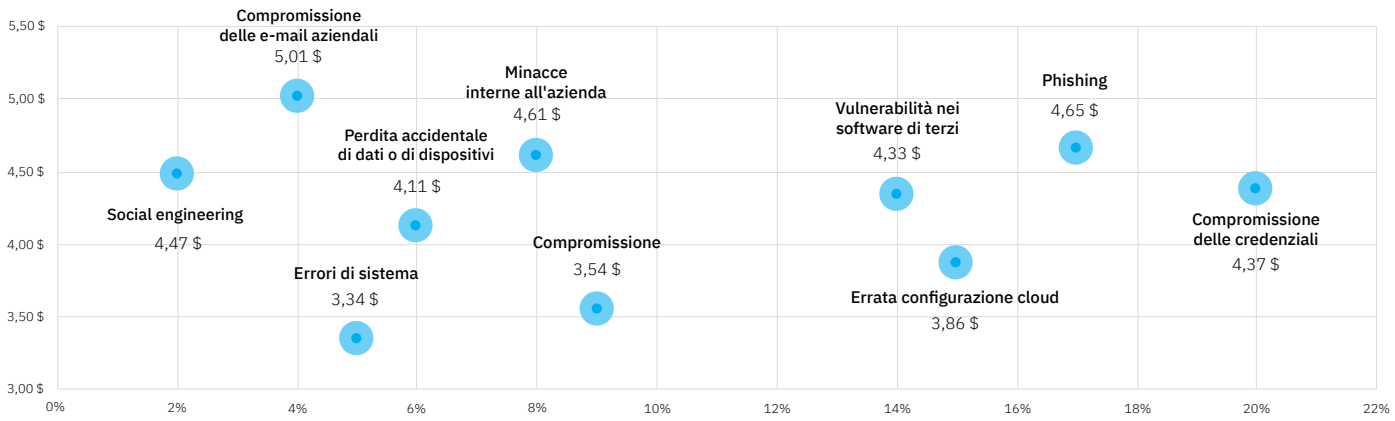
## 1. Minacce digitali esterne

Come indicato nel framework MITRE ATT&CK, l'esfiltrazione dei dati è una delle tattiche più recenti utilizzate dagli hacker nei loro attacchi. Secondo il report Data Breach Investigation Report 2022 di Verizon, in oltre l'80% delle violazioni dei dati, il motivo che spinge i criminali è il profitto economico.

I dati sensibili sono quindi l'obiettivo primario della maggior parte degli attacchi. Quando i criminali informatici riescono ad accedere all'ambiente aziendale, possono tentare di sottrarre i dati sfruttando numerosi canali. Mano a mano che gli attacchi diventano più complessi e riescono a superare agevolmente le misure di sicurezza, i rischi per i dati dell'organizzazione crescono in modo esponenziale.

## 2. Rischi interni

Mentre le tecnologie anti-malware e le altre misure di protezione degli endpoint riescono oggi a rilevare e a bloccare gli attacchi dall'esterno, i rischi interni legati agli insider sono in continuo aumento. Ne è un esempio l'utente finale che inconsapevolmente invia dati a utenti non autorizzati inoltrando un messaggio e-mail. Le cause possono essere molteplici: errori involontari dei dipendenti, configurazioni IT errate o insider che agiscono deliberatamente, ma il risultato non cambia perché la minaccia che incombe sulle organizzazioni è seria e le potenziali violazioni che ne derivano sono molto costose.




Sebbene alcune organizzazioni sottovalutino l'impatto dei rischi interni, il report del Ponemon Institute "Cost of Data Breach" del 2021 afferma chiaramente che circa un terzo delle violazioni dei dati coinvolge gli insider.

# Impatto della perdita dei dati sulle aziende

## Una perdita dei dati costituisce un serio rischio per le aziende. L'esfiltrazione di dati sensibili da parte di utenti non autorizzati è causa di:

- **Mancata conformità alle normative.** L'archiviazione, l'accesso e la protezione dei dati sensibili come le informazioni di identificazione personale o le informazioni sanitarie protette di dipendenti e clienti, o i dati delle carte di credito, sono rigidamente regolamentati da normative locali e internazionali, come GDPR, CCPA, HIPAA, PCI-DSS, ecc. Alcune, come il GDPR, impongono di segnalare le violazioni entro breve tempo dal loro verificarsi. In caso di ritardi nella segnalazione, le organizzazioni vanno incontro a sanzioni severe e perfino alla perdita delle certificazioni di conformità.
- **Danni economici.** Avvenuta la perdita dei dati, oltre alle sanzioni normative a cui potrebbero andare incontro i clienti degli MSP, i Service Provider possono subire danni economici conseguenti alla loro responsabilità nei confronti dei clienti che potrebbero citarli in giudizio. L'esfiltrazione di segreti commerciali o di proprietà intellettuale può provocare ulteriori perdite economiche alle aziende, arrivando anche a destabilizzare la loro posizione sul mercato.
- **Rischi per la reputazione.** Per le aziende, ritrovarsi in prima pagina per aver subito una violazione dei dati può essere imbarazzante ma soprattutto dannoso. Può infatti causare l'abbandono dei clienti delle aziende che servi, ma anche mettere a rischio le partnership esistenti e la possibilità di acquisire nuovi clienti. La perdita dei dati dei tuoi clienti può incidere negativamente anche sulla tua reputazione e sul tuo business.

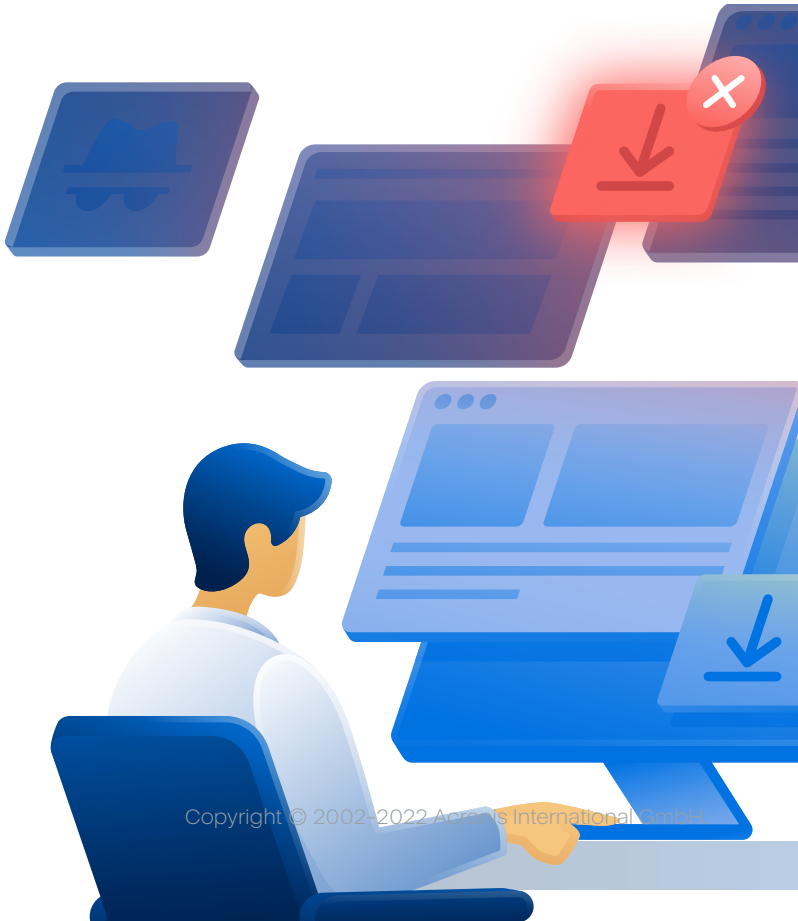
# Cos'è la prevenzione della perdita di dati (DLP)

Quella della **prevenzione della perdita dei dati** è una categoria di soluzioni di sicurezza che esiste da tempo, costituita da tecnologie di sicurezza informatica integrate che rilevano e impediscono l'uso, la trasmissione e l'archiviazione non autorizzati di dati sensibili e riservati.

Le **soluzioni DLP** funzionano mediante una combinazione di metodi per il controllo del flusso dei dati e l'analisi dei contenuti. Tali tecnologie estendono a tutta l'organizzazione le policy di utilizzo e gestione dei dati accettate dall'azienda, impedendo la consegna dei dati sensibili a destinatari non autorizzati, sia interni che esterni.

Benché la protezione dei dati sia principalmente associata al backup e al disaster recovery, esistono anche altre tecnologie fondamentali, come DLP, autenticazione e crittografia, che proteggono le informazioni sensibili da una vasta gamma di minacce, inclusa la sottrazione.

**DLP è l'unica tecnologia** in grado di fornire visibilità e controllo dei dati sensibili che entrano, escono e vengono archiviati in azienda, impedendo a entità non autorizzate di appropriarsene.



## Tipi di dati e tipologie di DLP che li proteggono

Sono **tre i tipi di stato principali** in cui possono trovarsi i dati di un'organizzazione:

- **Dati in uso:** dati che vengono utilizzati o trasferiti tramite canali locali (periferiche, supporti rimovibili) o applicazioni su computer endpoint, come ad esempio i file che vengono trasferiti da un computer endpoint a un'unità USB.
- **Dati in transito:** dati che vengono spostati o trasferiti tra sistemi informatici, come ad esempio quelli che vengono trasferiti da uno storage di file locale a uno nel cloud o da un computer endpoint a un altro endpoint tramite sistemi di messaggistica istantanea o posta elettronica.
- **Dati a riposo:** si tratta dei dati che vengono archiviati in locale o in una rete ai quali al momento non è possibile accedere o che non possono essere trasferiti, come ad esempio i dati archiviati nelle condivisioni di rete o sui server on-premise.

È bene sottolineare che lo stato dei dati cambia frequentemente e continuamente, sebbene alcuni possano rimanere nello stesso stato per l'intero ciclo di vita di un endpoint. Comprendere i diversi tipi di dati, le loro caratteristiche e differenze aiuta i clienti a gestire i dati della propria organizzazione con più sicurezza e a proteggerli dalle possibili sottrazioni.

Esistono tre tipi di DLP funzionali ai tre diversi tipi di dati:

- **DLP per dati in uso**
- **DLP per dati in transito**
- **DLP per dati a riposo**

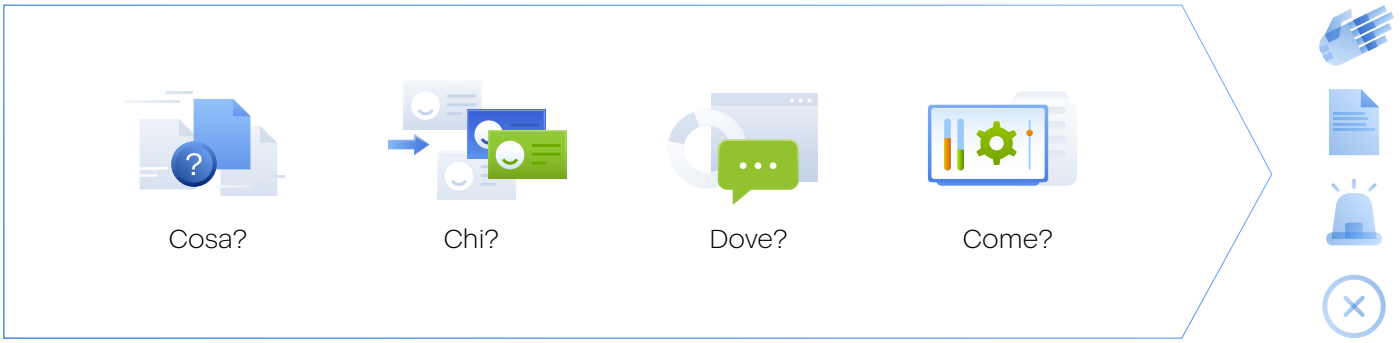
È bene ricordare che esistono altre tecnologie capaci di proteggere da altri rischi associati ai dati, come quelli di accesso o di privacy, ad esempio la gestione delle identità o la crittografia. La tecnologia DLP è però l'unica in grado di proteggere i dati nei loro diversi stati, e ha l'obiettivo prioritario di prevenirne la perdita fornendo al contempo visibilità sui flussi di dati.

## Controlli di DLP: confronto tra contenuto e contesto

In un'organizzazione, ogni flusso di dati ha un contenuto e un contesto. Con contesto intendiamo fattori ambientali come gli utenti coinvolti in un flusso di dati, i canali utilizzati, la direzione del flusso e così via. Il contenuto descrive invece la categoria o il tipo di informazione trasferita, ad esempio le cartelle cliniche dei pazienti, informazioni di identificazione personale riservate dei dipendenti, ecc.

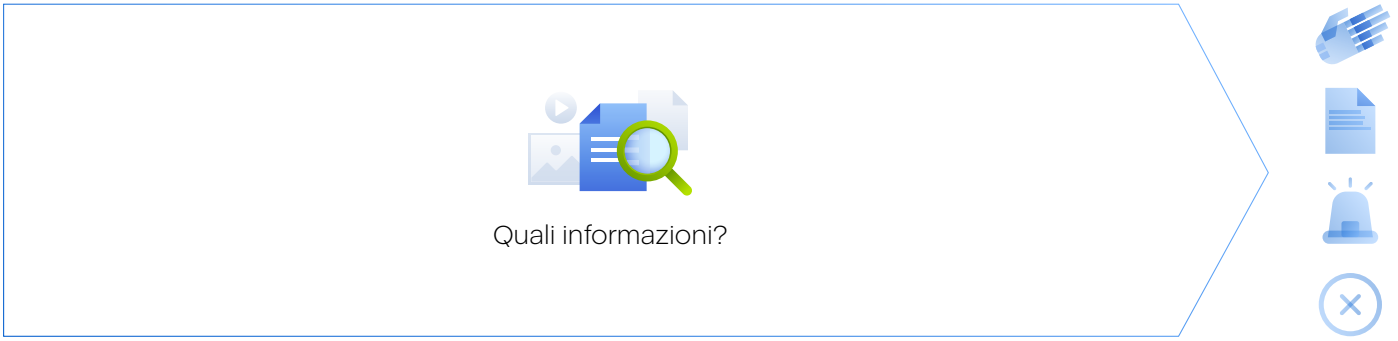
**Un'efficiente soluzione DLP è in grado di controllare i flussi di dati in base sia al contesto che al contenuto.**

- **Controlli DLP con riconoscimento del contesto**: controllo delle operazioni di trasferimento dei dati in base al contesto dell'operazione tramite attributi quali utenti coinvolti, canali utilizzati, direzione dei dati, destinatari, orari, ecc.




**Esempio:** policy che consentono la copia dei dati (che cosa) da parte degli utenti (chi) su dispositivi USB protetti (dove) e impediscono la copia dei dati su dispositivi USB non crittografati.

- **Controlli DLP con riconoscimento del contenuto**: controllo approfondito dei flussi dei dati in base al tipo e alla sensibilità delle informazioni (contenuto) che vengono trasferite.

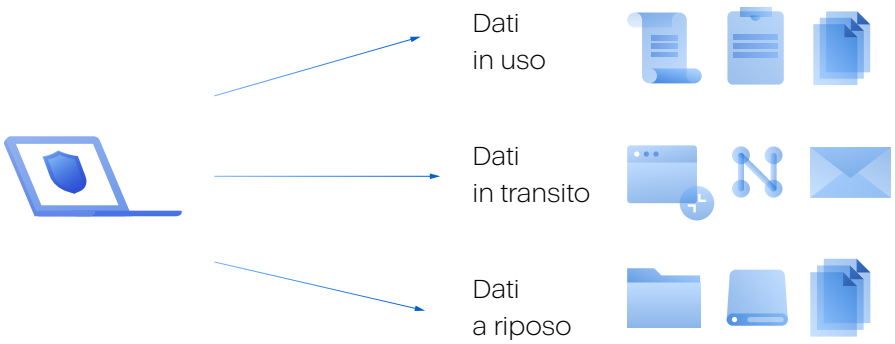



**Esempio:** impedire la copia di documenti che contengono informazioni HIPAA (quali informazioni) su qualsiasi dispositivo USB.

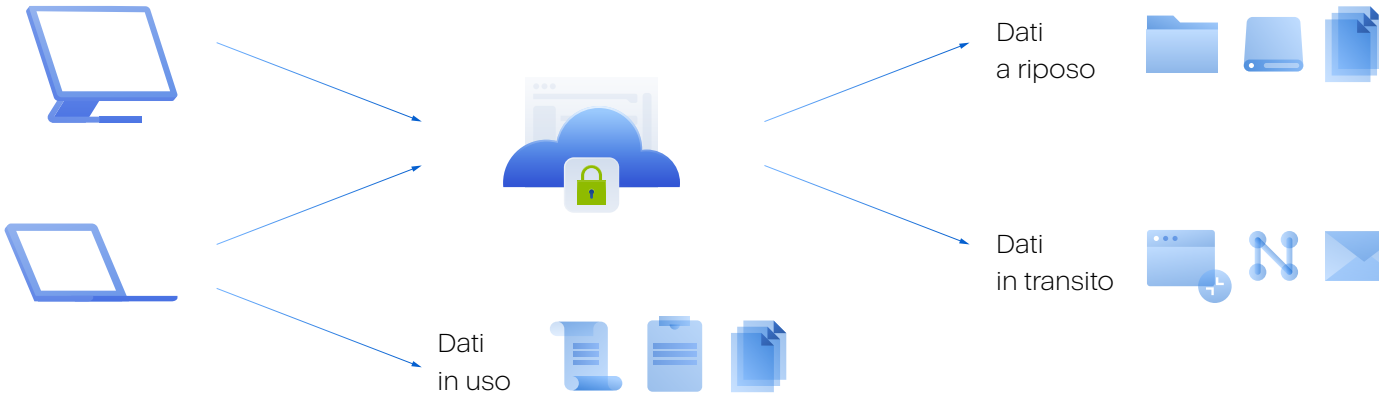
## Tipi di architettura DLP

**Possiamo distinguere tre tipi di DLP, in base alla loro installazione e al funzionamento:**

- **DLP su endpoint**: soluzioni che utilizzano gli agenti DLP sui computer endpoint e impediscono la diffusione dei dati in uso, in transito e a riposo da tali computer, che siano utilizzati all'interno della rete aziendale o su Internet.




- **DLP per rete/cloud**: soluzioni con componenti residenti solo su rete, inclusi gateway e server DLP hardware e virtuali, che proteggono i dati in transito o a riposo su computer posizionati nella rete aziendale, prevenendo la sottrazione dei dati da destinatari non autorizzati o il loro invio a destinazioni esterne alla rete aziendale.




- **DLP ibrida**: soluzioni che utilizzano sia i componenti DLP di rete che degli endpoint, per eseguire tutte le funzioni delle architetture DLP su endpoint e su network.

Le soluzioni DLP di rete non possono proteggere i dati in uso per le proprietà intrinseche della loro architettura e controllano solo le fughe dei dati verso parti non autorizzate esterne alla rete aziendale, mentre le DLP per endpoint e ibride proteggono i dati in qualsiasi stato e prevengono le fughe verso parti non autorizzate interne ed esterne.

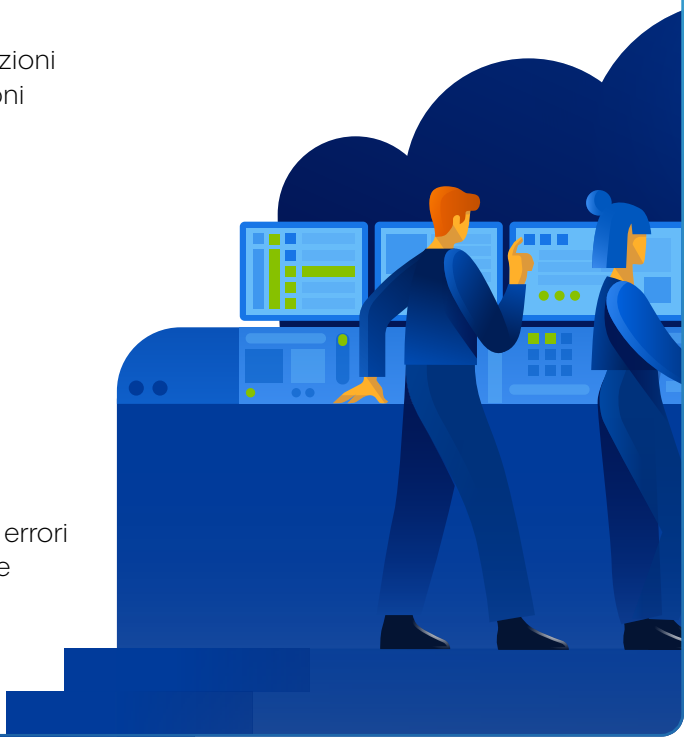
**Per le finalità di questa guida esamineremo l'avvio, l'esecuzione e la scalabilità di un servizio DLP basato su un'architettura DLP per endpoint.**

# I vantaggi della DLP per i clienti

Secondo il report del Ponemon Institute "Cost of Data Breach 2021", il costo totale medio a livello globale di una violazione dei dati è di 4,24 milioni di dollari, il 10% in più rispetto al 2020. All'aumento del costo delle violazioni si aggiunge il tempo effettivo necessario per identificarle e contenerle, che è pari a 287 giorni. È chiaro che prima che la falla venga chiusa i clienti corrono rischi altissimi, in termini economici, di reputazione e di aderenza alle normative.

**Con un servizio DLP potrai ridurre i rischi dei tuoi clienti in diversi modi:**

- **Facilitando il rispetto della conformità** alle normative e proteggendo le informazioni regolamentate: informazioni di identificazione personale (GDPR, CCPA), informazioni sanitarie protette (HIPAA), informazioni sulle carte di pagamento (PCI DSS), ecc.
- **Proteggendo** la proprietà intellettuale e i segreti commerciali dei clienti
- **Riducendo i rischi** di esfiltrazione dei dati causati da malware e attacchi di social engineering
- **Consolidando la sicurezza** del lavoro da remoto e dei dispositivi BYOD e impedendo il trasferimento dei dati sensibili verso storage in cloud
- **Prevenendo la fuga di dati** causata dai dipendenti per errori involontari, negligenza o cattiva condotta professionale
- **Facilitando la rapida reazione** agli incidenti di fuga dei dati e le indagini successive alla violazione, assicurando la visibilità continua degli eventi DLP



# Flusso di erogazione del servizio DLP

Prima di entrare nel dettaglio delle modalità di avvio, esecuzione e scalabilità di un servizio DLP, è importante notare che per le loro peculiarità intrinseche, i servizi DLP presentano un flusso di erogazione che prevede i seguenti passaggi:

- **Deployment dell'agente DLP:** tra le prime fasi del processo di erogazione del servizio c'è la decisione in merito agli endpoint nei quali eseguire il provisioning dei servizi DLP; questa fase ha la finalità di garantire la protezione accurata dei dati aziendali e il deployment degli agenti DLP sugli endpoint prescelti. Ricordiamo che è consigliabile eseguire il provisioning degli agenti DLP su tutti i workload in cui vengono creati, archiviati o utilizzati i dati sensibili. Se non sono protetti, questi workload creano potenziali falle nel sistema di sicurezza IT dell'azienda, da cui sarà facile sottrarre dati.

- **Creazione di policy DLP:** un'altra fase iniziale è la creazione delle policy DLP, che garantisce l'applicazione di policy adeguate per la gestione e l'uso dei dati. A seconda della tecnologia DLP utilizzata, questa fase può precedere il deployment. **È importante sottolineare** che le policy DLP non sono universali ma specifiche per ogni cliente, in quanto le varie organizzazioni hanno processi interni diversi, sono tenute al rispetto di normative diverse e hanno esigenze diverse per quel che riguarda l'accesso e la condivisione dei dati. Queste specifiche di creazione delle policy DLP fanno sì che le soluzioni DLP tradizionali richiedano una gestione manuale con complessità significative e costi elevati; per questa ragione, non vengono utilizzate dai Service Provider per creare servizi DLP.
- **Convalida di policy DLP:** un importante passaggio successivo alla creazione delle policy DLP iniziali è la convalida da eseguire insieme ai clienti per garantire che le policy rispettino i requisiti aziendali; la convalida deve essere congiunta perché gli MSP non possono avere un quadro completo e approfondito delle specifiche aziendali di ogni loro cliente. Più complessa e tecnica è la rappresentazione grafica della policy, più tempo ed esperienza saranno richieste dai clienti per la sua convalida.
- **Applicazione e gestione della policy DLP:** una volta convalidate le policy insieme al cliente, queste potranno essere applicate per proteggere i dati aziendali sensibili dalle perdite. Ricorda che le tecnologie DLP controllano i flussi di dati sensibili di un'organizzazione, bloccando solo quelli non autorizzati. Di pari passo all'evoluzione dell'azienda, vengono introdotte nuove procedure ed emergono nuove normative, che impongono la modifica di quelle precedenti. Per questa ragione, le policy DLP iniziali devono continuamente essere adeguate alle nuove esigenze aziendali, per garantire che non vengano bloccati nuovi flussi di dati importanti, ma prevenendo al tempo stesso tutti i tentativi di sottrazione dei dati. Questo risultato può essere ottenuto tramite la rettifica manuale delle policy o con metodi di adeguamento automatici adattivi.
- **Creazione di report sul valore del servizio DLP:** la segnalazione continua dei trasferimenti di dati sensibili impediti e delle azioni degli utenti finali correlate alla DLP è in grado di dimostrare il valore dei servizi DLP, contribuisce ad aumentare la fidelizzazione e illustra il minor rischio ai clienti non ancora consapevoli dei problemi di perdita di dati.

# Le difficoltà degli MSP con le soluzioni DLP attuali

Quello delle soluzioni DLP è un mercato maturo e orientato alle grandi aziende, con operatori di lunga data; tuttavia, il mercato più vasto (costituito dai Service Provider e dai loro clienti delle PMI) ha faticato ad adottare queste soluzioni, perché richiedono la comprensione continua e accurata delle specificità aziendali e la loro associazione ai controlli DLP, la conoscenza dei requisiti normativi e la comprensione della conformità dei dati necessaria per utilizzare tali tecnologie. Questi motivi hanno portato il settore DLP a concentrarsi soprattutto sulle grandi aziende, che possono permettersi il costo degli esperti interni dedicati alla gestione della protezione dalla perdita dei dati.

**I principali problemi a cui devono far fronte gli MSP nell'implementazione e nell'esecuzione di un servizio DLP sono:**

- **L'esecuzione di un servizio DLP è complessa e costosa.** Il servizio ha un costo molto elevato perché le soluzioni DLP convenzionali richiedono complessi processi manuali per la creazione iniziale delle policy e le rettifiche in corso d'opera, oltre a tempo e impegno per generare valore e adottare procedure di DLP efficienti presso i clienti. Per superare queste difficoltà è necessario assumere esperti di DLP, un'attività più ardua e costosa rispetto all'assunzione di specialisti generici in sicurezza IT.

- **Una DLP efficace richiede policy specifiche per il cliente.** Come già accennato, i processi e la sensibilità dei dati aziendali di ogni organizzazione sono unici e in continua evoluzione; si tratta quindi di adeguare continuamente le policy DLP alle caratteristiche dell'azienda. Un MSP non ha e non può acquisire e gestire regolarmente una tale approfondita conoscenza dei processi specifici di ogni singolo cliente. Ciò crea una barriera che ostacola in modo significativo le possibilità di crescita degli MSP che usano tecnologie DLP tradizionali.
- **Una configurazione non adeguata delle policy DLP può interrompere la continuità operativa.** Da un lato, la creazione e la configurazione manuale delle policy DLP sono soggette a errori, per la loro complessità e il livello di dettaglio. Dall'altro, le tecnologie DLP bloccano qualsiasi flusso dati non autorizzato. Se abbinate, questa complessità e le capacità preventive di DLP possono interrompere processi aziendali essenziali, bloccando per errore flussi di dati indispensabili all'azienda nel caso in cui le policy DLP vengano configurate in modo erroneo o i nuovi processi aziendali non siano associati in modo corretto alle policy.
- **I dipendenti sono l'anello debole del cliente.** Indipendentemente dal fatto che le tecnologie DLP siano difficilmente accessibili agli MSP e ai loro clienti, gli errori umani e gli attacchi dall'esterno indirizzati ai dipendenti sono la causa primaria delle perdite di dati. Anche se i Service Provider sono in grado di limitare il rischio di minacce esterne aggiungendo livelli ulteriori di protezione sugli endpoint, saranno comunque ritenuti responsabili qualora gli utenti rilascino involontariamente dati sensibili, provocando una violazione dei dati.
- **I clienti non sono sempre consapevoli del problema della sottrazione dei dati.** A causa delle difficoltà di accesso alle tecnologie DLP, non sempre i clienti sono consapevoli del problema. Avviare un servizio DLP obbliga il Service Provider a informare i clienti del rischio di sottrazione dei dati a cui devono far fronte e del fatto che la tecnologia DLP è l'unica in grado di risolvere il problema che queste minacce rappresentano per le organizzazioni di ogni dimensione.

Le tendenze e le tecnologie emergenti, come la creazione, l'estensione e il monitoraggio automatici delle policy basati sull'analisi comportamentale, possono risolvere il problema della rapida modifica delle regole DLP per tenere il passo con procedure aziendali e requisiti normativi in continua evoluzione. Queste nuove funzionalità rendono più accessibile il mercato delle soluzioni DLP ai Service Provider e ai loro clienti. È senz'altro il momento giusto per estendere la tua offerta con i servizi DLP.

# Pianificazione e lancio di un servizio DLP

## Prima di pianificare e lanciare un servizio DLP è necessario verificare che sia effettivamente necessario ai tuoi clienti.

**I clienti necessitano di un servizio DLP per ridurre i rischi di sottrazione dei dati nel caso in cui presentino alcuni o tutti i seguenti indicatori:**

- Creano, archiviano o lavorano sui propri workload utilizzando dati sensibili e soggetti a regolamentazione
- Hanno segreti commerciali o proprietà intellettuali che devono essere protetti dalle perdite
- Operano in settori con alto grado di regolamentazione
- Hanno subito una violazione dei dati e intendono proteggere i propri ambienti e ridurre i rischi
- Hanno certificato o devono certificare la propria conformità
- Hanno sottoscritto o stanno valutando un'assicurazione digitale per limitare la propria responsabilità civile
- Non hanno personale di sicurezza dedicato né competenze specifiche

**I clienti dei seguenti settori hanno dimostrato il maggior interesse nelle soluzioni DLP:**

- Servizi bancari e finanziari
- Healthcare
- Settore giuridico
- IT e telecomunicazioni
- Istituzioni e pubblica amministrazione
- Produzione industriale
- Retail e logistica
- Istruzione
- Energia

Se i tuoi clienti corrispondono a questi indicatori o operano nei settori citati, è il momento ideale per considerare l'aggiunta della protezione dalla perdita dei dati alla tua offerta di servizi; potrai così soddisfare le nuove esigenze di riduzione dei rischi di sottrazione dei dati e di rafforzamento della conformità normativa.

## Pianificazione dei servizi e stima dei costi

**I tre fattori principali che determinano il prezzo del servizio sono il costo della manodopera, il costo del prodotto e il margine che intendi ottenere. Ognuno di essi può incidere sulla definizione del prezzo come segue:**

- **Costo della manodopera:** la complessità della soluzione scelta determina il tempo dedicato dai tecnici alle attività di provisioning e gestione del servizio, nonché il livello richiesto di esperienza in sicurezza IT.
- **Costo del prodotto:** le soluzioni DLP, da sempre utilizzate nelle grandi imprese, implicano costi elevati che le rendono poco accessibili alle aziende di piccole e medie dimensioni. Se i tuoi clienti sono principalmente PMI, dovrai scegliere una soluzione che eviti un costo eccessivo per il servizio.
- **Margine desiderato:** un MSP-tipo che adotta il modello dell'utile ricorrente realizza una percentuale di margine lordo anche del 50% sui servizi erogati da remoto.

# Fornire un servizio DLP con Acronis Advanced DLP Pack

Acronis offre un servizio DLP basato sull'analisi comportamentale che crea e gestisce in modo automatico e continuativo la coerenza delle policy specifiche del cliente, senza richiedere mesi per il deployment, team da gestire o una laurea in diritto privato.

**Acronis Advanced DLP Pack assicura ai tuoi clienti una protezione DLP completa per i dati in transito e in uso con una semplicità mai vista prima, e ti consente di:**

- **Generare nuove opportunità di profitto** ampliando l'offerta per attirare più clienti e aumentare il tuo profitto per cliente, fornendo servizi DLP finora disponibili solo alle grandi imprese.
- **Ottenere valore con un impegno minimo** aggiungendo facilmente la protezione dei dati alla tua attività, senza ulteriori complessità, costi e risorse.
- **Ridurre i rischi di sicurezza dei clienti** prevenendo la sottrazione di dati sensibili.
- **Rafforzare la conformità normativa dei clienti** con modelli di classificazione dei dati pronti all'uso per i quadri di riferimento legislativi comuni, inclusi, tra gli altri, GDPR, HIPAA e PCI DSS.
- **Semplificare il provisioning e la gestione del servizio** automatizzando il provisioning del servizio DLP, la configurazione iniziale delle policy e i successivi adeguamenti.
- **Creare policy DLP specifiche per il cliente su larga scala** allineando in automatico le policy DLP alle mutevoli specificità aziendali grazie a una tecnologia basata sull'analisi comportamentale; assicurare la convalida delle policy insieme al cliente prima della loro applicazione.
- **Reagire più rapidamente agli eventi DLP** e semplificare le attività di servizio DLP, la manutenzione delle policy, i controlli della sicurezza IT e le indagini sugli incidenti, con un sistema centralizzato di registrazione degli audit basato su policy e avvisi di sicurezza.

## Acronis Advanced DLP Pack

Advanced DLP Pack per Acronis Cyber Protect Cloud aiuta i tuoi clienti a dormire sonni tranquilli, sapendo che i propri dati sensibili sono al sicuro dall'esfiltrazione verso destinazioni non autorizzate. La sua tecnologia, esclusiva basata sull'analisi comportamentale, consente la creazione e la continua estensione di policy DLP conformi alle specifiche esigenze di ogni cliente, permettendoti di avviare i servizi con una semplicità mai vista prima e di generare valore con un impegno minimo.

Acronis

Per saperne di più, visita www.acronis.com