# Prevenzione sulla perdita dei dati e trasformazione digitale

## INTRODUZIONE

L'era digitale che stiamo vivendo produce quantità di dati senza precedenti. Molti di questi dati sono considerati sensibili, come le informazioni personali su clienti e dipendenti, i dati finanziari e la proprietà intellettuale che le aziende devono tenere al sicuro. In passato, queste informazioni venivano stampate su carta e protette in un archivio per i documenti sotto chiave. Ora, queste preziose sequenze di zeri e uno corrono da un posto all'altro, diventando sempre più vulnerabili.

La necessità di proteggere tali dati è indiscutibile. Costituiscono la linfa vitale di un'organizzazione e includono le informazioni che sono state affidate all'organizzazione, che ha il compito di garantirne la sicurezza. Pertanto, alcuni tipi di dati sono regolamentati e le aziende si trovano a essere sottoposte a sanzioni molto ingenti, in caso di gestione errata. Non c'è da sorprendersi se tali dati sono preziosi anche sulla dark net, dove è possibile ottenere fino a cinque dollari per un singolo numero di carta di credito con indirizzo, ovvero la tipologia di informazioni che molti database memorizzano in quantita' elevata. Per tutti questi motivi, implementare delle soluzioni complete di prevenzione sulla perdita dei dati (DLP) costituisce una necessità incombente per le organizzazioni.



## LA NECESSITÀ DI UNA SOLUZIONE DLP

Una soluzione DLP è un insieme di tecnologie e processi che monitorano e ispezionano i dati sulla rete aziendale per garantire che le informazioni sensibili non vengano perse o rubate. Uno strumento DLP dovrebbe sempre far parte di un'iniziativa di protezione dei dati che copra l'intera organizzazione, riunendo i leader aziendali e IT per identificare ciò che deve essere considerato tra i "dati sensibili" e concordare come tali dati debbano essere gestiti e cosa rappresenta una violazione degli stessi. Tali linee guida possono quindi essere tradotte in un insieme di regole all'interno di uno strumento DLP. Le soluzioni DLP affrontano tre principali sfide organizzative: conformità normativa, protezione contro la perdita dei dati e visibilità.

1

**Conformità normativa:**

Secondo Gartner[1], la conformità normativa è di gran lunga il caso d'uso di DLP più comune, citato nel 75% di tutte le distribuzioni DLP registrate. A partire da maggio 2018, il GDPR, il Regolamento generale europeo sulla protezione dei dati, ha portato le soluzioni DLP sotto il radar degli specialisti della protezione dei dati nelle organizzazioni al di fuori dei settori regolamentati, le quali sono sempre state soggette all'obbligo di adottare determinate misure per proteggere le informazioni personali identificabili (PII) e le informazioni sanitarie protette (PHI). Anche se le normative non richiedono esplicitamente l'uso di una soluzione DLP, spesso, i requisiti di protezione dei dati presentano il concetto di DLP per agevolare la conformità.

## Sembra una soluzione DLP...

Il New York State Department of Financial Services (NYDFS) — 23 NYCRR 500, allude all'uso di una soluzione DLP basata sui dati in movimento, ma non la illustra:

**Sezione 500.15 (a)**

"(...) ogni Entità coperta deve attuare controlli, includendo la crittografia, per proteggere le Informazioni non pubbliche detenute o trasmesse dall'Entità stessa, sia in transito su reti esterne che a riposo".

[1] Market Guide for Enterprise Data Loss Prevention:
https://www.gartner.com/en/documents/3890116/market-guide-for-enterprise-data-loss-prevention

# LA NECESSITÀ DI UNA SOLUZIONE DLP

## 2 Protezione contro la perdita dei dati

Le ragioni per cui proteggere le informazioni sensibili dall'esposizione a soggetti non autorizzati vanno ben oltre la conformità. Esse sono spesso oggetto di furti. Un buon indicatore del loro valore è rappresentato dal fatto che i malintenzionati sono disposti a pagare prezzi molto più alti sul dark Web per i dati non regolamentati, come le iscrizioni ai premi e i numeri di programmi fedeltà, rispetto ai numeri di previdenza sociale statunitensi[2].

Seppure le organizzazioni ricevano degli incentivi per essere conformi, come evitare sanzioni o che le proprie operazioni aziendali siano sottoposte a restrizioni, la perdita dei dati comporta rischi finanziari e correlati alla reputazione ad ampio raggio che si traducono, ad esempio, nella perdita di clienti, nel rimborso di "punti" persi in ambito di membership, nel danneggiamento del marchio o persino in conseguenze legali".

Secondo lo studio di Ponemon del 2019, Cost of a Data Breach Study (Costo della violazione dei dati)[3], il 30% delle organizzazioni subirà una violazione entro due anni, il cui esito si traduce in media in:

**costo di $3,9M** **25.000 record persi**

I settori soggetti a conformità normativa, come i servizi sanitari e finanziari, subiscono violazioni più costose. Il costo medio per ogni record rubato è stato di:

**$429** Assistenza sanitaria

**$210** servizio finanziario

**$150** tutti i settori

Le soluzioni DLP sono fondamentali per evitare perdite accidentali dei dati dovute a errori umani, come la condivisione involontaria di dati sensibili con terze parti tramite condivisione di file o social media, o attraverso fallimenti dei processi IT o aziendali[4]. Nonostante le rigide normative per la gestione delle informazioni sanitarie, la perdita accidentale dei dati è particolarmente elevata nel settore sanitario, dove rappresenta il 57,5%[5] della divulgazione involontaria dei dati, secondo il rapporto Verizon Protected Health Information Data Breach (Rapporto Verizon sulle violazioni dei dati sanitari protetti) del 2018. Verizon ha osservato che è l'unico settore in cui gli addetti ai lavori rappresentano una minaccia per la perdita dei dati di entità maggiore rispetto ai malintenzionati esterni.

[2] https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/; https://www.comparitech.com/blog/information-security/how-much-are-stolen-frequent-flyer-miles-worth-on-the-dark-web/#gref

[3] [4] Ponemon 2019 Data Breach: https://databreachcalculator.mybluemix.net/

[5] Protected Health Information Data Breach Report: http://www.verizonenterprise.com/resources/protected_health_information_data_breach_report_en_xg.pdf



# LA NECESSITÀ DI UNA SOLUZIONE DLP

## 3 Visibilità dei dati

La trasformazione digitale sottopone le organizzazioni e, in particolare, i CISO a delle sfide correlate alla visibilità su ciò che accade ai dati nelle proprie reti. Con l'aumento delle quantità dei dati, titolari dei dati sempre diversi e l'incremento del numero di luoghi in cui risiedono tali dati, è difficile identificare tutte le informazioni sensibili e adottare delle misure per proteggerle; del resto, non è possibile proteggere ciò che non si riesce a vedere. Ci sono tre tendenze principali che generano punti ciechi per le organizzazioni: adozione del cloud, mobilità degli utenti e crittografia.

L'**adozione del cloud** sta costringendo le organizzazioni a gestire tutti i dati archiviati non solo all'interno del datacenter, ma anche all'interno dell'organizzazione stessa. Prima di poter trasferire i dati nel cloud, è necessario conoscere la natura dei dati in proprio possesso.

I dipendenti non sono più obbligati a lavorare dietro alle proprie scrivanie, il che significa che ora accedono alle proprie app e ai file di lavoro da qualsiasi luogo e in qualsiasi momento. Tali **utenti mobili** possono accedere ai dati e archiviare i file al di fuori del datacenter, lasciando spesso l'organizzazione all'oscuro di quanto accaduto.

Sempre più spesso, le organizzazioni impiegano tecniche di **crittografia** nel tentativo di proteggere i dati. Tuttavia, i sistemi di sicurezza basati su hardware non sono in grado di controllare i contenuti dei file crittografati, il che lascia le organizzazioni ignare del tipo di dati contenuti.

# LA NECESSITÀ DI UNA SOLUZIONE DLP

**I dati si spostano su diversi canali**

Nel nostro mondo digitalizzato, i dati si muovono più liberamente che mai. In qualsiasi momento possono trovarsi su uno di questi tre canali: un endpoint, in un sistema di archiviazione o in transito. Ogni canale in cui i dati vengono memorizzati o trasferiti richiede un diverso set di strumenti o tecniche per prevenirne la perdita. Le soluzioni DLP sono segmentate in base ai tre canali che proteggono:

**Dati all'endpoint:** le soluzioni DLP di endpoint sono basate su agenti e monitorano i dati che vengono elaborati in corrispondenza dell'endpoint. La loro funzionalità è varia, ma solitamente include restrizioni di stampa, che impediscono il copia-incolla tra le applicazioni e il download su un dispositivo di archiviazione portatile, come un'USB.

**Dati a riposo:** tutti i dati presenti sui server di file, database o archiviazione cloud sono considerati a riposo. La soluzione DLP per i dati a riposo esegue la scansione di tutti i contenuti dell'archivio per rilevare le informazioni sensibili.

**Dati in movimento:** denominate anche DLP Web o DLP di rete, le soluzioni per i dati in movimento controllano tutto il traffico che si sposta dal punto A al punto B sul Web (Internet) o via e-mail, ad esempio i dati che vengono spostati dall'archiviazione cloud a un endpoint.

La trasformazione digitale ha generato un cambiamento nel comportamento degli utenti e dei modelli di traffico, che ha influenzato i canali di endpoint e i dati a riposo. Man mano che un numero maggiore di dati si sposta sul cloud, le soluzioni per i dati a riposo stanno diventando irrilevanti, perché le loro funzionalità possono essenzialmente essere sostituite dalle soluzioni CASB (Cloud Access Security Provider). Inoltre, sempre meno dati e meno applicazioni rimangono sugli endpoint, attribuendo pertanto maggiore importanza alla protezione dei dati che si spostano tra endpoint, sistemi di archiviazione e applicazioni cloud con una soluzione per i **dati in movimento**.



## PERCHÉ LA SOLUZIONE DLP NON HA MANTENUTO LA PROMESSA?

### Il mercato DLP si sta evolvendo

Le soluzioni DLP sono disponibili da 15 anni e il mercato è maturo. Ci sono state così poche differenze tra le soluzioni DLP aziendali concorrenti che la società di analisi leader di Gartner ha lasciato il Magic Quadrant per DLP aziendali. Al contrario, Gartner si sta concentrando su una guida di mercato che evidenzi l'importanza di una strategia olistica di protezione dei dati e fornisce istruzioni sull'uso di soluzioni DLP integrate.

Rispetto alle soluzioni **DLP aziendali,** che in genere forniscono una varietà di prodotti (agenti, dispositivi fisici e virtuali) su tutti i canali, le soluzioni **DLP integrate** sono fornite in modo nativo da tecnologie come i Secure Web Gateway, i sistemi di gestione dei contenuti, la crittografia delle e-mail o la tecnologia CASB e, pertanto, hanno un focus più ristretto.

Le soluzioni DLP aziendali sono notoriamente complesse e costose. Le organizzazioni che acquistano soluzioni DLP aziendali si avvalgono spesso solo di un piccolo sottoinsieme di funzionalità e affrontano solo i casi d'uso di base che possono essere risolti con una soluzione DLP integrata, evitando che l'organizzazione debba eseguire configurazioni e integrazioni costose e dispendiose in termini di tempo.

> **Secondo le stime di Gartner,** entro il 2021, il 90% delle organizzazioni implementerà almeno una forma di DLP integrata, con un aumento del 50% rispetto a oggi. [6]

Le soluzioni DLP aziendali e integrate non si escludono l'una con l'altra. Le organizzazioni che hanno già investito in tali prodotti devono lavorare con la propria infrastruttura esistente. Tuttavia, qualsiasi organizzazione dovrebbe considerare l'aggiunta di soluzioni DLP integrate, per affrontare ulteriori casi d'uso che colmino le lacune nella propria strategia di protezione dei dati esistente, generate a causa della trasformazione digitale.

[6] How to Choose Between Enterprise DLP and Integrated DLP Approaches https://www.gartner.com/doc/3757464?ref=mrktg-srch

# PERCHÉ LE SOLUZIONI DLP NON HANNO RISPETTATO LA PROMESSA



**La prevenzione sulla perdita dei dati è un'iniziativa che deve interessare l'intera organizzazione, non uno strumento IT**

Nonostante si tratti di una soluzione matura, le organizzazioni continuano a segnalare problemi con le distribuzioni di soluzioni DLP, molti derivanti dalla scarsa pianificazione e da altri inconvenienti organizzativi.

La maggior parte delle organizzazioni ritiene erroneamente che le soluzioni DLP debbano essere implementate e gestite a lungo termine solo dalla sicurezza IT. Una volta stabilite le regole DLP, la responsabilità della soluzione DLP deve essere trasferita alle operazioni aziendali. Inoltre, coloro che implementano soluzioni DLP devono assicurarsi il consenso della dirigenza senior, per ottenere visibilità sulle unità di business o sui team di gestione del rischio aziendale.

Per evitare di dover cercare ulteriori sponsor e casi d'uso per giustificare il progetto, il che aggiungerebbe inevitabilmente richieste e complessità alle distribuzioni, i team dovrebbero assicurarsi il consenso interno e legare i progetti DLP a iniziative o obiettivi specifici.



## REQUISITI CLOUD DELLE SOLUZIONI DLP

Man mano che le organizzazioni si spostano sul cloud, anche la loro sicurezza dovrebbe spostarsi lì. Tuttavia, la semplice riconfigurazione di uno stack hardware tradizionale per il cloud è inefficiente e non fornisce le protezioni e i servizi di una soluzione creata invece appositamente per il cloud. Questo vale anche per le soluzioni DLP. Per affrontare le sfide relative alla protezione dei dati, conseguenza della trasformazione digitale, e superare le carenze delle soluzioni DLP tradizionali, una soluzione DLP basata sul cloud richiede i seguenti tre elementi:

1. **Protezione identica per tutti gli utenti in rete o fuori dalla rete**
   Con le soluzioni DLP tradizionali, ancorate al datacenter, il livello di visibilità e protezione dipende da dove si trovano gli utenti. Gli utenti remoti possono bypassare l'ispezione quando sono fuori dalla rete, connettersi direttamente alle applicazioni cloud e aggirare la VPN, nonché qualsiasi misura di protezione dei dati. Per fornire una protezione completa dei dati, una soluzione DLP dovrebbe offrire una protezione identica a tutti gli utenti, indipendentemente dalla loro posizione, che si trovino in ufficio, in una lounge aeroportuale o lavorino da casa.

2. **Ispezione del traffico crittografato**
   Con oltre il 70% del traffico odierno che utilizza la crittografia, è necessario che le organizzazioni ispezionino tale traffico. Tuttavia, dato che la crittografia è stata originariamente creata come misura di sicurezza, le soluzioni di sicurezza tradizionali non controllano in modo nativo questo tipo di traffico. Di conseguenza, le organizzazioni tendono a ispezionare solo una frazione del traffico crittografato, pertanto qual è il reale contributo di una soluzione DLP che vede solo il 30% del traffico totale? Cercare di rafforzare il proprio posizionamento di sicurezza mediante l'aggiunta di apparecchi di applicazione SSL non è probabilmente fattibile finanziariamente, né accettabile in termini di complessità IT. L'unico modo per ottenere visibilità sul traffico crittografato è utilizzare una soluzione DLP che ispezioni in modo nativo l'SSL.

3. **Scalabilità elastica per l'ispezione in linea**
   L'enorme crescita del traffico Internet richiede aggiornamenti costanti delle soluzioni DLP tradizionali basate su apparecchi di applicazione, poiché la loro capacità di ispezione limitata viene rapidamente surclassata. Nel tentativo di superare la complessità e il costo di questo sforzo, molte organizzazioni desistono nell'implementazione di una soluzione DLP in linea fin dal principio. Purtroppo, ciò porta le organizzazioni a effettuare un controllo sui danni solo dopo che i loro dati sono già stati compromessi. Una soluzione cloud offre una capacità di ispezione scalabile elasticamente, in grado di prevenire la perdita dei dati controllando tutto il traffico in linea, prima che i dati possano essere compromessi.



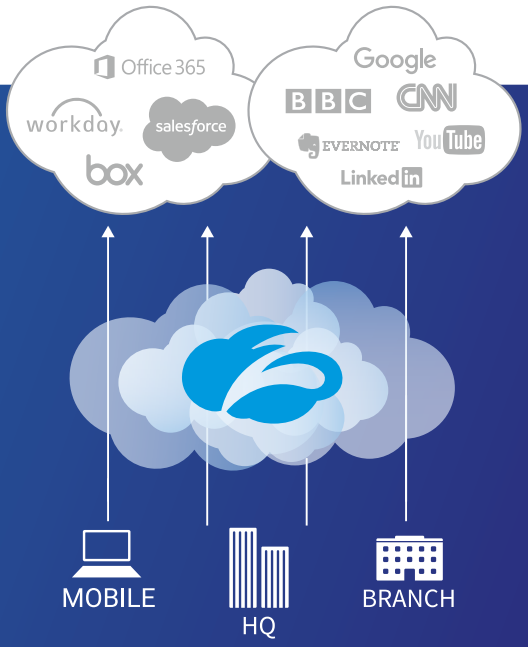
# ZSCALER™ CLOUD DLP

**Parte di Zscaler Internet Access**

Zscaler Internet Access™ (ZIA™) è un Secure Web e Internet Gateway fornito come servizio dal cloud. ZIA si posiziona tra gli utenti e Internet, ispezionando ogni byte di traffico in linea attraverso diverse tecniche di sicurezza, anche all'interno dell'SSL, fornendo pertanto una protezione completa dalle minacce di Internet. Questa piattaforma cloud, creata appositamente, include Cloud Sandbox, Next-Generation Firewall e Cloud Application Visibility and Control, nonché Cloud DLP.

## Una panoramica su Cloud DLP

Zscaler Cloud DLP offre una protezione completa dei dati mediante un contesto completo e un'ispezione dei contenuti per tutti i dati in movimento. Dispone inoltre di funzionalità avanzate, tra cui Exact Data Match, machine learning e policy granulari per una protezione ottimale.




**Zscaler Cloud DLP soddisfa i tre requisiti**

Zscaler Cloud DLP fornisce lo stesso livello di sicurezza a tutti gli utenti, spostando la sicurezza dei dati sul cloud. Zscaler si colloca tra gli utenti e le applicazioni a cui si stanno connettendo. La policy di Cloud DLP segue gli utenti dove lavorano, in rete o fuori dalla rete, e fornisce lo stesso livello di protezione a tutti, in ogni momento.



Fornisce inoltre un'ispezione completa del traffico crittografato. Circa il 70% del traffico in uscita è crittografato e quindi non è soggetto all'ispezione da parte delle soluzioni DLP tradizionali. Con Zscaler, non ci sono vincoli di capacità per abilitare l'intercettazione SSL su larga scala. Zscaler è concettualmente un proxy che esegue l'ispezione SSLsu tutto il traffico, senza le limitazioni di ispezione degli apparecchi di applicazione.

Inoltre, Zscaler è una soluzione progettata per essere in linea, in modo che possa bloccare le informazioni sensibili prima che lascino la rete, anziché limitarsi al controllo dei danni dopo che i dati sono stati compromessi. L'architettura di sicurezza di Zscaler è stata costruita dalla base sul cloud e il servizio è basato sull'utente, non basato sulla capacità, consentendo all'ispezione di Cloud DLP di scalare elasticamente con prestazioni garantite dagli SLA.

## CONCLUSIONE

Le soluzioni DLP devono essere considerate un processo di sicurezza ben definito, potenziato da una tecnologia di supporto ben gestita. Tuttavia, anche in questa fase avanzata di maturità delle soluzioni DLP, le organizzazioni continuano a lottare con le relative distribuzioni. Ciò è dovuto principalmente a una rappresentazione interna errata delle soluzioni DLP nel contesto dei programmi di sicurezza. Inoltre, molti sul mercato enfatizzano la semplicità delle implementazioni, il livello di accuratezza standard nell'identificazione dei contenuti, nonché la visibilità e il controllo su tutte le applicazioni.

Con l'aumento dei rischi e l'espansione delle normative per la protezione dei dati, le organizzazioni devono colmare le lacune di sicurezza create dal cloud e dalla mobilità. In passato, ciò avrebbe comportato l'aggiunta di più apparecchi di applicazione a un set di servizi della security già complesso. Zscaler offre un modo migliore. Con Zscaler Cloud DLP è possibile colmare le lacune nella protezione dei dati, indipendentemente da dove gli utenti si connettano o da dove le applicazioni siano ospitate, senza apparecchi di applicazione costosi e complessi.

# Informazioni su Zscaler

Zscaler consente alle organizzazioni di trasformare in sicurezza le proprie reti e applicazioni per un mondo mobile e cloud-first. Zscaler collega gli utenti ad applicazioni e servizi cloud, indipendentemente dal dispositivo, dalla posizione o dalla rete, fornendo allo stesso tempo una sicurezza completa e un'esperienza utente veloce. Tutto questo senza dispositivi gateway costosi e complessi.



zscaler™