Guida pratica alla prevenzione della perdita di dati per dirigenti

Adozione di un programma per la sicurezza dei dati in 5 fasi

Forcepoint

White paper

Sommario

Il problema

Nel mercato regna molta confusione in materia di controlli per la prevenzione della perdita di dati (DLP). Vi sono molteplici fattori concomitanti, in particolare una generale mancanza di comprensione tra i fornitori su come funziona la protezione dei dati o sul modo in cui le aziende percepiscono il rischio. Sono stati attuati processi non funzionali, che hanno causato colli di bottiglia nelle operazioni, senza ridurre la costante minaccia di perdita e furto di dati. Le esperienze poco felici delle organizzazioni possono essere collegate direttamente alla scarsa chiarezza sugli obiettivi dei programmi, a una pianificazione carente e a un'implementazione mediocre.

Il risultato è che le organizzazioni che vogliono proteggere i propri dati riservati, proteggere gli accessi e una forza lavoro sempre più ibrida e rispettare le leggi e i regolamenti sono spesso scettiche e non sanno a chi rivolgersi. Alcune sono rimaste scottate da implementazioni non riuscite.

È importante capire che la tecnologia alla base dei controlli DLP non è il fattore determinante per il successo: sono la metodologia e la strategia di esecuzione del fornitore a definire sia l'esperienza che i risultati.

Questo white paper intende porsi come guida e riferimento:

- → Illustrando la difficoltà di proteggere la forza lavoro ibrida e il contesto per fare della protezione dei dati il punto focale di un programma di protezione degli accessi.
- → Spiegando le differenze importanti da considerare nella valutazione di un potenziale fornitore.
- → Offrendo informazioni preziose e approfondite sulle tendenze nelle violazioni dei dati.
- → Proponendo un semplice processo in cinque fasi per adottare e realizzare una strategia di protezione dei dati intrinsecamente adattiva al rischio, pratica e misurabile.
- → Offrendo diverse best practice pratiche per evitare gli errori più comuni e superare la maggior parte delle sfide operative alle implementazioni DLP.

"È importante capire che la tecnologia alla base dei controlli DLP non è il fattore determinante per il successo: sono la metodologia e la strategia di esecuzione del fornitore a definire sia l'esperienza che i risultati".

Un punto di partenza

Tutti i controlli DLP devono conseguire i primi due obiettivi dell'elenco seguente.

1. Consentire l'identificazione dei dati.

- → **Dati in movimento** (che viaggiano sulla rete)
- → **Dati in uso** (che vengono utilizzati nell'endpoint)
- → **Dati a riposo** (che sono fermi negli archivi)
- → **Dati nel cloud** (dati in uso, in movimento, a riposo)

2. Identificare i dati come "descritti" o "registrati".

- → **Descritti:** classificatori predefiniti e modelli di policy contribuiscono a identificare i tipi di dati. Ciò è utile quando si cercano contenuti come, ad esempio, dati a carattere personale (PII).
- → **Registrati:** i dati vengono registrati sul sistema per creare un'"impronta digitale", che consente di individuare corrispondenze complete o parziali con informazioni specifiche, ad esempio proprietà intellettuale.

Una soluzione DLP più avanzata consentirà di conseguire anche il terzo obiettivo descritto di seguito.

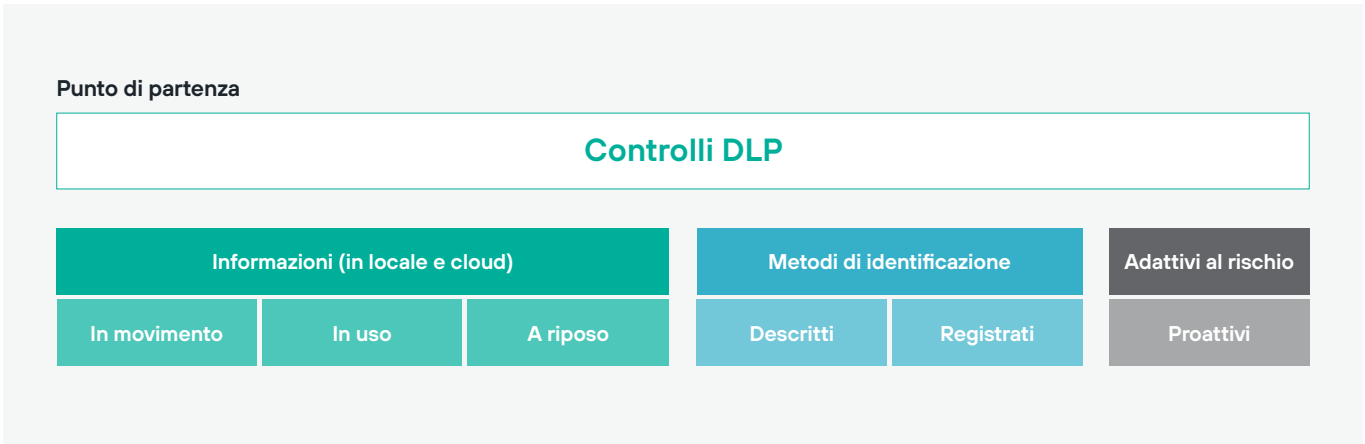
3. Adottare un approccio alla DLP adattivo al rischio.

- → La DLP adattiva al rischio distingue le soluzioni di prevenzione della perdita di dati avanzate dagli altri set di strumenti DLP. La DLP adattiva al rischio discende dall'approccio CARTA (Continuous Adaptive Risk and Trust Assessment) di Gartner, che integra caratteristiche di flessibilità e proattività. Regola e applica in modo autonomo le policy DLP in base al rischio che una persona rappresenta per un'organizzazione in un determinato momento. L'applicazione in tempo reale è poi in grado di prevedere e bloccare le violazioni prima che vengano portate a termine. La produttività cresce perché gli utenti sono meno intralciati da misure di sicurezza intrusive, mentre le indagini IT si semplificano grazie alla riduzione dei falsi positivi e della classificazione di rischio degli incidenti.

Per descrivere la logica delle prime due funzionalità comuni, a un controllo DLP viene indicato:

- → Che cosa cercare (ad es. numeri di carte di credito)
- → Il metodo per identificare le informazioni (descritte/registrate)
- → Dove cercarle (ad es. rete, endpoint, archiviazione, cloud)

Ciò che accade dopo che un controllo DLP identifica le informazioni dipende a) dalla tolleranza al rischio del proprietario dei dati, b) dalle opzioni di risposta disponibili quando viene rilevata la perdita di dati e c) dalla soluzione, ovvero se è adattiva al rischio.



Dalla visione all'implementazione

Sebbene tutti i controlli DLP offrano funzionalità simili, è importante capire che non tutti i fornitori hanno la stessa visione di come la DLP contribuisce a risolvere il problema della perdita di dati. Pertanto, il primo passo da compiere nella valutazione di un fornitore consiste nel comprenderne la metodologia e la strategia di esecuzione.

Quando si chiede a un fornitore: "Che metodologia adottate?" in realtà si chiede: "Qual è la vostra visione su come questo strumento può contribuire a risolvere il problema della perdita di dati?"

Si tratta di una domanda importante ma posta raramente. La risposta consente di comprendere la visione di un fornitore, che a sua volta consente di identificare le sue specifiche capacità e la direzione verso cui è probabilmente orientata la sua roadmap. Ai fini del successo e della soddisfazione sul lungo termine dell'organizzazione, per i decisori è molto più importante conoscere i motivi che muovono i fornitori piuttosto che sapere ciò che fanno.

La metodologia di un fornitore ha inoltre un forte impatto sulla sua strategia di esecuzione o di implementazione. Ad esempio, se la metodologia di un fornitore parte dalla valutazione dei dati a riposo e quella di un altro fornitore parte dalla valutazione dei dati in movimento utilizzando controlli adattivi al rischio, le loro strategie di esecuzione differiscono in modo notevole. Il modo in cui un fornitore esegue i controlli DLP è importante perché influisce sia sul costo totale di proprietà (TCO) sia sul time-to-value previsto, entrambi fattori fondamentali per prendere la decisione di acquisto giusta e per definire correttamente le aspettative delle parti interessate.

Nota importante: bisogna evitare di applicare la metodologia di un fornitore alla tecnologia di un altro. La metodologia definisce e guida la roadmap tecnologica di un fornitore, quindi mescolando i due aspetti si rischia di investire in una tecnologia che non soddisferà le esigenze a lungo termine.

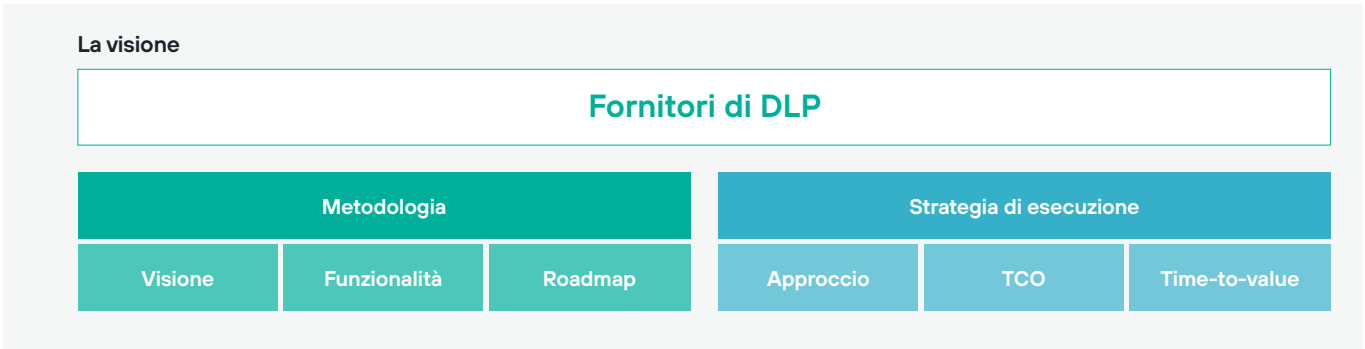
DLP misurabile e pratica

Chi ha partecipato a una conferenza oppure letto un articolo sulle best practice riguardo alla DLP, probabilmente conosce già il detto "non fare il passo più lungo della gamba"; in pratica significa che non è possibile attuare un programma DLP completo tutto in una volta. Questa è però una best practice utile, visto che non aiuta a capire cosa fare e quando. Per alcuni aspetti, "non fare il passo più lungo della gamba" suona più come un avvertimento che come una best practice.

Purtroppo, molte best practice pubblicate non sono sempre utili. A causa di mancanza di risorse, finanziarie o di altro tipo, e di altri problemi organizzativi, spesso le best practice non vengono seguite e risultano di fatto inutili. Analogamente, molte linee guida possono essere fin troppo caute: i dati devono essere conservati al sicuro, ma anche restare accessibili, mentre procedure eccessivamente rigide e invasive possono ostacolare la produttività e rappresentare un rischio per le aziende. Sono molto più utili delle best practice pratiche, che prendano in considerazione il costo, i vantaggi e l'impegno richiesto per seguirle, e che siano anche misurabili, per consentire alle organizzazioni di determinare la fattibilità e la convenienza della loro adozione.

Per verificare se un controllo DLP è misurabile e pratico nella gestione e nella mitigazione del rischio di perdita di dati, è necessario conoscere e comprendere due informazioni chiave:

1. Per verificarne la misurabilità, è necessario conoscere e applicare la formula del rischio per la perdita di dati. Sebbene simile ad altri modelli di rischio, la formula del rischio per la perdita di dati presenta una sostanziale differenza, che spiegheremo più avanti.
2. Per verificarne la praticità, è necessario capire dove è più probabile subire una violazione dei dati ad alto impatto e utilizzare la regola 80/20 per concentrare l'attenzione e le risorse dove sono più utili.



La formula del rischio per la perdita di dati

La più nota formula base per il calcolo del rischio è la seguente:

Rischio = Impatto x Probabilità

Con la maggior parte dei modelli di rischio, la sfida consiste nel determinare la probabilità che una minaccia si presenti. Questa probabilità è fondamentale per decidere se investire in una soluzione di prevenzione della minaccia o se farne a meno e accettare il rischio.

La differenza con la formula del rischio per la perdita di dati è che non si ha a che fare con l'ignoto. Si riconosce il fatto che la perdita di dati è inevitabile e di solito involontaria. Ma soprattutto, la formula consente di misurare e mitigare il rischio a un livello adeguato per l'organizzazione.

Pertanto, la metrica utilizzata per monitorare la riduzione del rischio per i dati e del ROI dei controlli DLP è la frequenza di occorrenza (FO).

Rischio= Impatto x Frequenza di occorrenza (FO)

La FO indica con quale frequenza, in un determinato periodo di tempo, i dati vengono utilizzati o trasmessi in un modo che li espone al rischio di smarrimento, furto o compromissione. La FO viene misurata prima e dopo l'esecuzione dei controlli DLP per dimostrare l'entità della riduzione del rischio.

Ad esempio, se si inizia con una FO di 100 incidenti in un periodo di due settimane e si è in grado di ridurre tale quantità a 50 incidenti in un periodo di due settimane successivo all'implementazione dei controlli DLP, la probabilità di un incidente di perdita di dati (violazione dei dati) viene ridotta del 50%.

Le soluzioni adattive al rischio sono particolarmente efficaci nella riduzione della FO, in quanto identificano il rischio reale dei dati in modo molto più accurato nel contesto delle interazioni più ampie di un utente. Riducono nettamente i falsi positivi e, in questo modo, procurano un vantaggio rispetto alla DLP tradizionale, non soltanto per la riduzione del rischio ma anche per la capacità di presentarlo in modo più accurato.

La regola 80/20 della DLP

Oltre a identificare la FO, è importante scoprire dove è più probabile che l'organizzazione subisca una violazione dei dati ad alto impatto. A tale scopo, è necessario studiare le ultime tendenze nelle violazioni e quindi utilizzare la regola 80/20 per determinare da che parte cominciare ad attuare i controlli DLP. Uno studio recente ha reso prontamente disponibili queste informazioni.

Secondo uno studio condotto nel 2021 da Ponemon Institute, le credenziali compromesse sono il vettore d'attacco iniziale più comune, responsabile del 20% delle violazioni, seguito dal phishing al 17%.[1]

Per attuare un programma veramente efficace di protezione contro la perdita di dati, è necessario sentirsi sicuri della propria capacità di rilevamento e di risposta allo spostamento dei dati sul web, e-mail, cloud e supporti rimovibili.

È qui che una soluzione DLP adattiva al rischio può offrire un vantaggio. Le soluzioni DLP tradizionali spesso riscontrano difficoltà nell'identificazione di aspetti quali processi aziendali interrotti o attività irregolari, che possono portare a una significativa perdita di dati. La DLP adattiva al rischio riconosce il comportamento dei singoli utenti e lo confronta con l'osservazione lungo un periodo di riferimento, in modo da rafforzare i controlli DLP in modo rapido e autonomo se l'attività non è in linea con la funzione lavorativa o il comportamento usuale dell'utente finale. Questo approccio proattivo può ridurre i rischi di perdita e di esposizione accidentale di dati.

[1] Cost of a Data Breach Report 2021, prodotto da Ponemon Institute per conto di IBM.

La metodologia e la strategia di esecuzione DLP di Forcepoint

L'osservazione delle ultime tendenze in fatto di violazioni dei dati e l'applicazione della formula del rischio per la perdita di dati rappresentano i primi passi per creare una strategia di prevenzione della perdita di dati. La metodologia DLP più efficace si concentra sulla comprensione dell'intento dell'utente per prevenire la perdita di dati prima che si verifichi. L'esecuzione dovrebbe concentrarsi sulla fornitura del miglior time-to-value per dimostrare una riduzione misurabile del rischio.

Time-to-value

Il time-to-value è la differenza di tempo tra l'implementazione dei controlli DLP e il conseguimento di risultati misurabili nella riduzione dei rischi. Poiché l'utente rappresenta il massimo punto di rischio dei dati – che si tratti di un collaboratore interno disonesto o poco attento, oppure di una vittima di vettori di attacco esterni – il miglior time-to-value si ottiene quando la DLP è focalizzata sui dati in movimento e i dati a riposo, con una tecnologia adattiva al rischio che funziona in background.

Questa affermazione potrebbe destare le tue perplessità se ti è stato detto da altri fornitori o esperti che i controlli DLP devono essere concentrati in primo luogo sui dati a riposo. Spesso dicono: "Se non sai quello che hai e dove si trova, non puoi pensare di essere in grado di proteggerlo". Ma questa affermazione non è vera. Infatti, i controlli DLP sono progettati per svolgere proprio questa funzione. Le possibilità sono due: o gli altri fornitori ed esperti non capiscono come valutare e gestire correttamente il rischio, oppure si limitano a ripetere ciò che dicono altri perché sembra funzionare per loro.

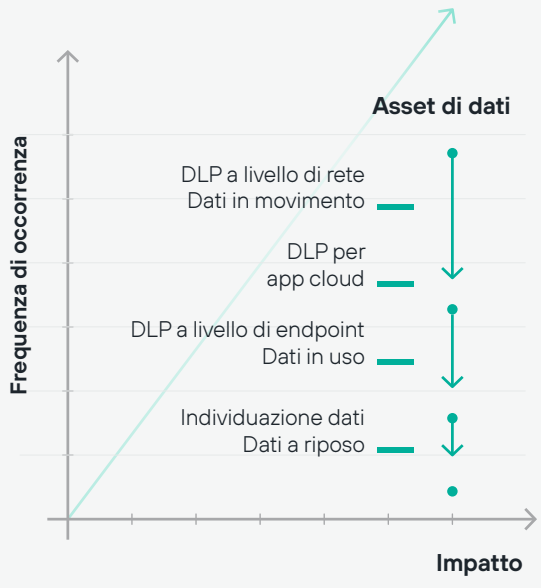


Figura 1. La metodologia e la strategia di esecuzione DLP di Forcepoint

Perché dovresti mettere in dubbio la raccomandazione di partire dai dati a riposo? Considera le seguenti domande:

1. Conosci un'organizzazione che ha identificato e protetto con successo tutti i dati sensibili, soprattutto in un contesto di adozione accelerata del cloud?
2. Hai idea di quanto tempo sia necessario per scansionare, identificare e proteggere ogni singolo file che contiene informazioni sensibili?
3. Sai di quanto verrà ridotto il rischio di conseguenza?

Il problema di focalizzarsi come prima cosa sui dati a riposo è che ci si concentra sul rischio potenziale, non su quello effettivo, e pertanto non è possibile misurarlo nel contesto della riduzione del rischio. Rischio potenziale significa che devono essere soddisfatte altre condizioni prima che possa verificarsi una conseguenza negativa. Nel contesto della perdita di dati, tali condizioni sono:

- → Qualcuno o qualcosa con intenti dannosi deve trovarsi sulla tua rete o accedere ai tuoi ambienti cloud.
- → Deve essere alla ricerca dei tuoi dati sensibili.
- → Deve trovarli.
- → Deve spostarli.

Questo vale per tutte le organizzazioni e ci porta alla domanda più importante: "Credi che la tua organizzazione sia in grado di rilevare minacce e contrastarle quando i dati sono in movimento?"

Tre sono i canali attraverso i quali si verifica la perdita di dati, in cui si rileva e si risponde al rischio effettivo:

- → La rete (ad es. e-mail, web, punti di accesso remoto, FTP)
- → Canale endpoint (ad es. supporti USB, stampanti)
- → Canali cloud (ad es. Office 365, Box)

Considerazioni su dati a riposo e conformità

Molte normative richiedono la scansione degli archivi di dati alla ricerca di dati a riposo non protetti e potresti quindi chiederti perché una metodologia e una strategia di esecuzione DLP non partano da lì. Ma la verità è che i revisori si preoccupano più della conformità al momento del controllo che di quella passata.

Quindi, la scansione dei dati a riposo è importante per la conformità, ma non è né l'obiettivo primario né il valore principale del controllo DLP. Pertanto pianifica l'utilizzo della DLP per il rilevamento e la conformità dei dati, ma in modo pratico e sostenibile per la tua organizzazione.

Crea delle policy per l'eliminazione difendibile (cioè per distruggere i file che non sono più necessari) per ridurre il rischio e delle policy per la conservazione sul lungo termine quando richiesto dalla legge. Il modo migliore per iniziare è quello di utilizzare la DLP per mettere automaticamente in quarantena i file che sono rimasti inutilizzati per almeno sei mesi. Assegna le autorizzazioni ai team legale e di conformità in modo che possano prendere decisioni in base alle policy di conservazione dei dati.

Le cinque fasi per il successo della DLP

Le cinque fasi descritte di seguito forniscono un processo per l'implementazione dei controlli DLP che è applicabile in pratica dalla tua azienda e che può produrre risultati misurabili. Queste fasi aiutano a implementare con successo le applicazioni DLP tradizionali o a rafforzare un approccio alla sicurezza dei dati che adotta già la DLP adattiva al rischio, a prescindere che la tua azienda abbia già una DLP consolidata oppure si stia muovendo in tal senso.

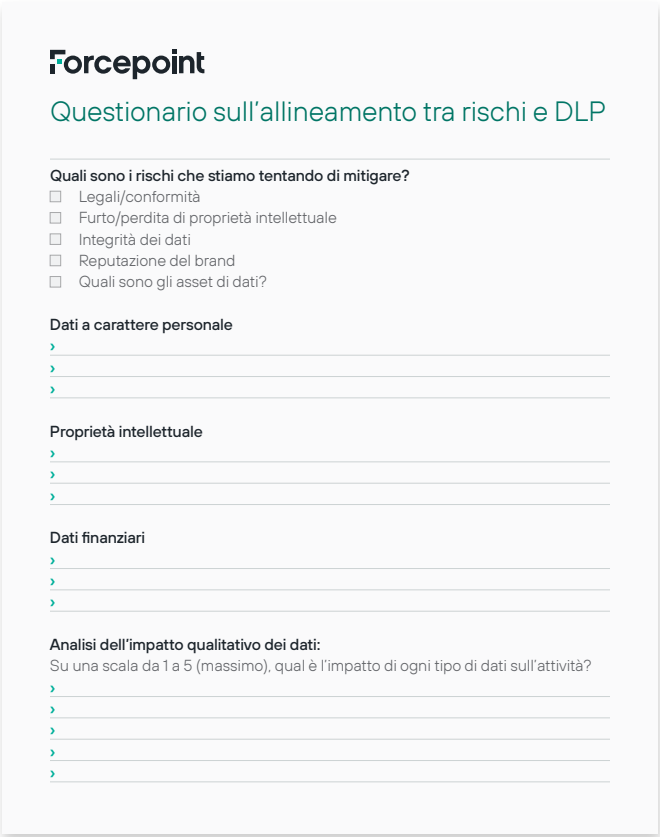
Fase 1:

Creare un profilo di rischio per le informazioni

Obiettivo: comprendere l'ambito delle tue esigenze di protezione dei dati.
Descrizione generale: crea un profilo iniziale di rischio per le informazioni che includa:

- → Una descrizione delle potenziali conseguenze di un mancato intervento.
- → Una descrizione dei tipi di dati inclusi nell'ambito (ad esempio, PII, IP, dati finanziari).
- → Le definizioni dei canali di rete, endpoint e cloud in cui i dati possono essere persi o rubati.
- → Un elenco dei controlli di sicurezza esistenti e in uso per la protezione dei dati (ad es. la crittografia).

1. **Dichiara il rischio che intendi mitigare**
2. **Redigi un elenco degli asset di dati e raggruppari per tipo**
3. **Fai un colloquio con i proprietari dei dati per determinare l'impatto**
4. **Elenca i canali che possono trasmettere le informazioni**



Forcepoint

Questionario sull'allineamento tra rischi e DLP

Quali sono i rischi che stiamo tentando di mitigare?
- ☐ Legali/conformità
- ☐ Furto/perdita di proprietà intellettuale
- ☐ Integrità dei dati
- ☐ Reputazione del brand
- ☐ Quali sono gli asset di dati?

Dati a carattere personale
›
›
›

Proprietà intellettuale
›
›
›

Dati finanziari
›
›
›

Analisi dell'impatto qualitativo dei dati:
Su una scala da 1 a 5 (massimo), qual è l'impatto di ogni tipo di dati sull'attività?
›
›
›
›
›

Fase 2:

Creare un grafico di correlazione tra gravità degli incidenti relativi ai dati e tempi di risposta

Obiettivo: determinare i tempi di risposta agli incidenti di perdita di dati, in base al grado di gravità.

Descrizione generale: organizza un incontro fra il team di implementazione DLP e i proprietari dei dati per determinare il livello di impatto in caso di perdita, furto o compromissione dei dati. Per descrivere l'impatto usa l'analisi qualitativa, ad esempio una scala da 1 a 5. La scala aiuta a classificare gli sforzi di risposta agli incidenti in base alla priorità e a determinare il tempo di risposta appropriato.

Opzione DLP adattiva al rischio: tieni presente che una soluzione DLP che adotta un approccio adattivo al rischio è progettata per dare la priorità alle attività ad alto rischio, applicare autonomamente i controlli in base al rischio e ridurre il tempo necessario per indagare su un incidente. Il risultato è un minor rischio di impatto e un controllo più proattivo sui dati critici.

Le fasi iniziali restano le stesse, ma verranno potenziate con la DLP adattiva al rischio.

1. **Comincia definendo i tipi di dati da proteggere**
2. **Allinea i regolamenti con i tipi di dati identificati**
3. **Determina in che modo identificare i dati**
4. **Determina la gravità dell'impatto e la risposta agli incidenti**

"Ai sensi dell'RGPD, le violazioni dei dati devono essere notificate all'autorità di controllo competente entro 72 ore dal momento in cui se ne viene a conoscenza".

Normativa			**Passo 1:** discutere i tipi di dati generici **Passo 2:** normative relative (procedura guidata) **Passo 3:** "ID" – Registrato o descritto **Passo 4:** quantità o % per Alto Medio Basso		Leggenda di classificazione impatto		
Notifica di violazione	HIPPA	PCI/PCI-DSS			5, 4	3, 2	1
			Dati a carattere personale	ID	Alto	Medio	Basso
			VIP PII	R	1	-	-
			PII	D	>100	>25	>2
			PHI	D	>100	>50	>2
			Informazioni finanziarie	ID	Alto	Medio	Basso
			Carte di credito	D	>25	>5	>2
			Informazioni sulle buste paga	D	>25	>5	>2
			Proprietà intellettuale	ID	Alto	Medio	Basso
			Progetto X	R	>25%	>10%	10%<
			Documento di progetto	R	>25%	>10%	10%<
			Nomi utente e password	R	>25%	>10%	10%<

Passo 1: Determinare la risposta agli incidenti in base alla gravità e al canale

Obiettivo: definire che cosa succede in risposta a un incidente di perdita di dati in base alla gravità e al canale.

Descrizione generale: l'organizzazione dispone di un numero limitato di canali attraverso i quali avviene il passaggio dei dati. Questi canali diventano i punti di monitoraggio utilizzati dai controlli DLP per rilevare e rispondere alle perdite di dati. Elenca tutti i canali di comunicazione disponibili nella rete, nell'endpoint e nel cloud (ovvero le applicazioni cloud approvate) in un foglio di lavoro. Quindi applica una risposta (in base alla gravità dell'incidente) utilizzando una delle opzioni di risposta disponibili nei controlli DLP per lo specifico canale.

Puoi anche chiarire eventuali requisiti aggiuntivi della tua organizzazione per fornire la risposta desiderata, come la crittografia o l'ispezione SSL. Ad esempio, i supporti rimovibili sono tra i primi tre vettori per la perdita di dati; tuttavia sono anche un ottimo strumento per aumentare la produttività.

Un'opzione per mitigare il rischio di perdita di dati per Box o Google Drive consiste nell'annullare automaticamente la condivisione di file contenenti informazioni sensibili che vengono trasferiti nell'archiviazione cloud e condivisi esternamente.

Opzione DLP adattiva al rischio: una soluzione DLP adattiva al rischio può fornire alle organizzazioni controlli di applicazione granulari tra i canali, offrendo la flessibilità necessaria per regolare la risposta in base al livello di rischio dell'utente (ad esempio, solo controllo per gli utenti a basso rischio e blocco per gli utenti ad alto rischio). In questo modo gli utenti possono di svolgere in modo efficace il loro lavoro, senza compromettere i dati.

1. **Scegli i dati o il tipo di dati**
2. **Conferma i canali da monitorare**
3. **Determina la risposta in base alla gravità**
4. **Prendi nota di eventuali requisiti aggiuntivi per la risposta desiderata**

Canali	Livello 1 **Basso**	Livello 2* **Medio-basso**	Livello 3 **Medio**	Livello 4 **Medio-alto**	Livello 5 **Alto**	Note
Web	Controllo	Controllo/notifica	Blocco/notifica	Blocco/avviso	Blocco	Proxy da bloccare
Web sicuro	Controllo	Controllo/notifica	Blocco/notifica	Blocco/avviso	Blocco	Ispezione SSL
E-mail	Crittografia	Eliminazione allegati e-mail	Quarantena	Quarantena	Blocco	Crittografia
FTP	Controllo	Controllo/notifica	Blocco/notifica	Blocco/avviso	Blocco	Proxy da bloccare
Stampante di rete	Controllo	Controllo/notifica	Blocco/notifica	Blocco/avviso	Blocco	Installa agente di stampa DLP
Applicazioni cloud	Controllo	Controllo/notifica	Quarantena con nota	Quarantena	Blocco	
Personalizzato	Controllo	Controllo/notifica	Blocco/notifica	Blocco/avviso	Blocco	TBD

*Maggiore granularità disponibile con la DLP adattiva al rischio

Figura 2. Mappatura delle policy dei canali DLP

Passo 2: Stabilire un flusso di lavoro degli incidenti

Obiettivo: assicurarsi che vengano seguite le procedure per l'identificazione e la risposta agli incidenti.

Descrizione generale: fai riferimento alla Figura 3. Flusso di lavoro degli incidenti, che illustra come vengono gestiti gli incidenti in base alla gravità e che cosa accade quando viene rilevato un incidente. Automatizza per quanto possibile la gestione degli incidenti di gravità bassa, ad esempio inviando notifiche a utenti e manager in caso di comportamenti rischiosi. Puoi anche fornire coaching ai dipendenti per insegnare loro a rimediare al rischio in modo autonomo.

Gli incidenti di maggiore impatto richiedono l'intervento di un analista di incidenti, che indagherà e determinerà il tipo di minaccia (ad esempio, accidentale, intenzionale o malevola). L'analista di incidenti inoltra l'incidente e la relativa analisi al responsabile di programma, in genere il responsabile della sicurezza o della conformità, che determina quindi le azioni da intraprendere e i team da includere.

Opzione DLP adattiva al rischio: Se si sceglie di sfruttare una soluzione adattiva, l'indagine da parte di un analista di incidenti non è necessaria prima di intraprendere un'azione. Gli incidenti attribuiti a utenti a basso rischio possono non rappresentare una minaccia per l'organizzazione e pertanto dovrebbero essere autorizzati in modo da non ostacolare la produttività. Tuttavia, queste azioni consentite dovrebbero includere misure di sicurezza come la richiesta di crittografia per il salvataggio su USB o l'eliminazione degli allegati inviati tramite posta elettronica.

Per gli utenti a rischio più elevato e gli incidenti associati, gli amministratori possono adottare un approccio proattivo, bloccando o limitando automaticamente azioni specifiche in attesa dell'indagine da parte dell'analista di incidenti.

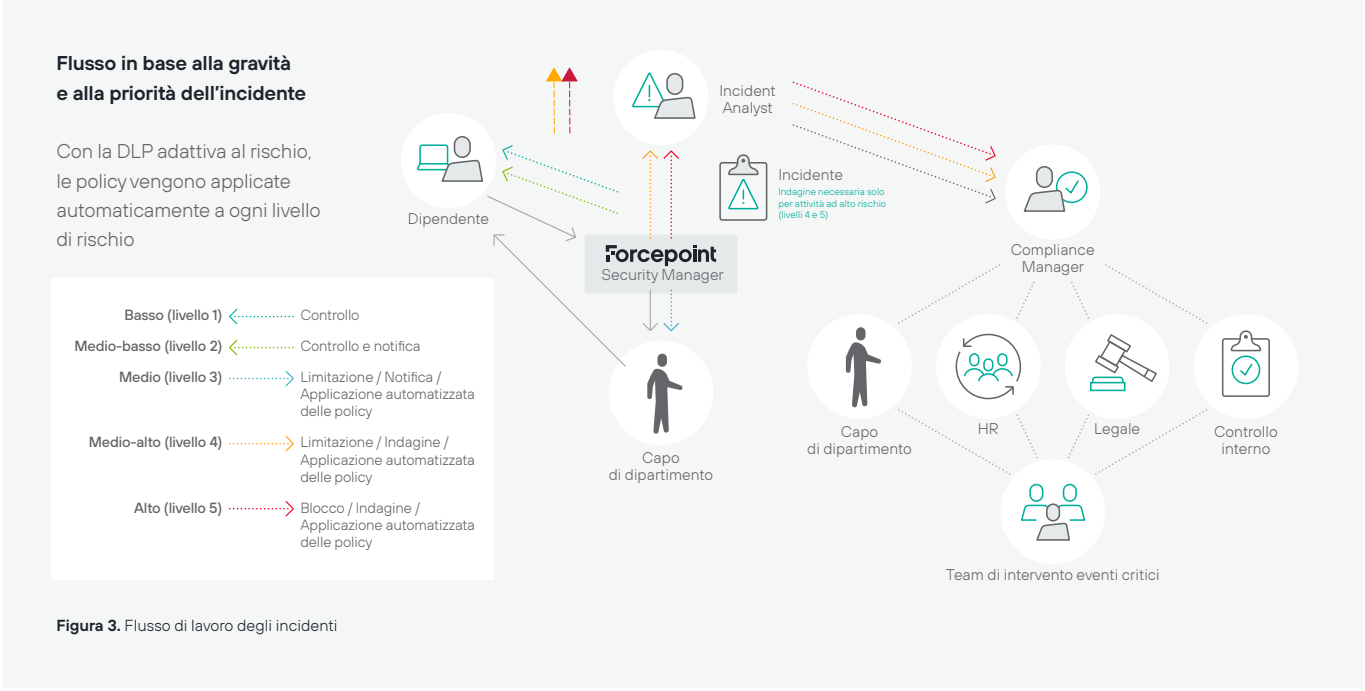


Figura 3. Flusso di lavoro degli incidenti

Fase 3:

Realizzare un progetto pilota di monitoraggio

Obiettivo: implementare la DLP di rete per misurare il rischio e cominciare a ridurlo.

Descrizione generale: la fase 3 comporta quattro passi secondari. Nel passo 1 si assegnano ruoli e responsabilità ai principali interessati. Nel passo 2 viene definito il quadro tecnico. Nel passo 3 si amplia la copertura dei controlli DLP. Poi, nel passo 4, questi controlli vengono integrati a livello dell'intera organizzazione.

Prima della sua applicazione attiva, la DLP deve essere attivata in modalità passiva, per permetterti di comprendere gli effetti delle policy implementate. Man mano che ottieni maggiori informazioni sul movimento e l'utilizzo dei dati all'interno dell'organizzazione, puoi regolare i controlli per applicare le policy agli utenti a rischio più elevato.

Dopo la fase di monitoraggio iniziale, durante la quale hai distribuito un controllo DLP di rete, esegui un'analisi e presenta i risultati chiave al team dirigenziale. La presentazione deve includere attività di mitigazione del rischio raccomandate per ridurre la FO (frequenza di occorrenza) dei dati a rischio. Quindi acquisisci i risultati e riferiscili al team dirigenziale.

Opzione DLP adattiva al rischio: Se scegli di implementare una rete DLP adattiva al rischio, puoi eseguire un'analisi degli incidenti in modalità di solo controllo e, per confronto, in modalità di applicazione graduale.

Il confronto dei dati evidenzierà la riduzione del numero di incidenti che richiedono un'indagine senza compromettere i dati. I risultati osservati saranno più indicativi dei veri positivi. Questo processo consente anche di dimostrare i vantaggi dell'automazione, le minori risorse necessarie per monitorare e gestire gli incidenti e la maggiore produttività dei team coinvolti.

Passo 1: Assegnare ruoli e responsabilità

Obiettivo: aumentare la stabilità, la scalabilità e l'efficienza operativa del programma DLP.

Descrizione generale: di norma, per preservare l'integrità dei controlli DLP e aumentarne l'efficienza operativa vengono assegnati quattro ruoli diversi:

- → Amministratore tecnico
- → Analista/manager di incidenti
- → Investigatore forense
- → Revisore

Ogni ruolo è definito in base alle proprie responsabilità e assegnato alla parte interessata appropriata. In questa fase, è comune vedere i membri del team di implementazione DLP svolgere la funzione di manager di incidenti. Tuttavia, man mano che i controlli DLP giungono a maturazione e ispirano un elevato livello di fiducia, questi ruoli verranno passati al proprietario dei dati appropriato.

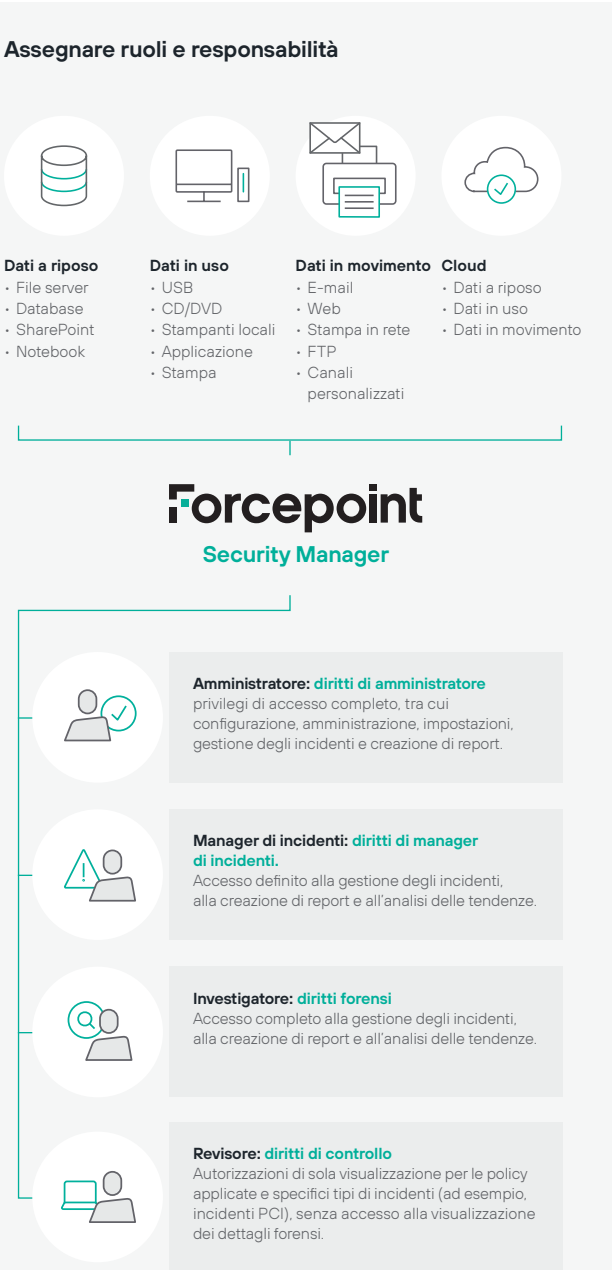


Figura 4. Assegnare ruoli e responsabilità

Passo 2: Stabilire il quadro tecnico

Obiettivo: creare una base di riferimento per i controlli di protezione dei dati, per aiutare l'organizzazione a riconoscere il normale comportamento degli utenti e prevenire violazioni dei dati ad alto impatto.

Descrizione generale: in questa fase, il ruolo del controllo DLP è principalmente di monitoraggio e vengono bloccati soltanto gli incidenti di gravità alta (ad esempio, il caricamento di dati in destinazioni note come dannose oppure il caricamento in massa in un'unica transazione di record non protetti e a rischio). Questo approccio di solo controllo può essere adottato anche utilizzando una DLP adattiva al rischio, assegnando a ogni livello di rischio l'impostazione di solo controllo.

Le fasi 4 e 5 trattano in modo più approfondito la creazione di report, il ROI e il monitoraggio della riduzione del rischio.

1. **Installare e configurare**
2. **Monitorare la rete**
3. **Analizzare i risultati**
4. **Aggiornamento del gruppo dirigente 1**
5. **Attività di mitigazione del rischio** (ad es., attivazione policy di blocco)
6. **Analizzare i risultati**
7. **Aggiornamento del gruppo dirigente 2**

Stabilire il quadro tecnico	Lunedì	Martedì	Mercoledì	Giovedì	Venerdì
Settimana 1: installazione / messa a punto / formazione					
Settimana 2: monitoraggio					
Settimana 3: monitoraggio					
Settimana 4: aggiornamento del gruppo dirigente 1					
Settimana 5: mitigazione del rischio					
Settimana 6: aggiornamento del gruppo dirigente 2					

Figura 5. Tempistica dell'implementazione – Parte 1

Passo 3: Espandere la copertura dei controlli DLP

Obiettivo: implementare la DLP sugli endpoint e sulle applicazioni cloud approvate per misurare il rischio e cominciare a ridurlo.

Descrizione generale: ora tutto è pronto per passare a considerare i dati in uso e i dati a riposo. Durante questo passo, distribuisci la DLP sugli endpoint e sulle applicazioni cloud approvate, monitori e analizzi i dati, aggiorni il team dirigenziale ed esegui le attività di mitigazione dei rischi, analogamente a quanto fatto all'inizio della fase 3. La differenza principale è che ora scegli di rispondere agli incidenti in base ai diversi canali e alle opzioni disponibili per i dati in uso, che si trovano negli endpoint e nelle applicazioni cloud. La gravità dell'incidente e la risposta sono state determinate nella fase 2, in base al canale.

Per i dati a riposo, il processo identifica gli obiettivi da scansionare, ne definisce la priorità e sposta i dati vecchi in quarantena, dove il team legale e il team di conformità possono procedere in base alle policy di conservazione dei dati dell'organizzazione. Per quanto riguarda la conformità, la collaborazione è fondamentale. Pertanto è necessario collaborare, ma a una velocità ragionevole per l'organizzazione. Ricorda che non è una gara in cui vince chi arriva per primo.

Se ti occorre svolgere un'attività di individuazione con urgenza, ricorda che puoi aumentare temporaneamente (o definitivamente) la velocità di individuazione usando agenti di individuazione locali o configurando più dispositivi di individuazione di rete.

1. **Implementare gli endpoint e l'applicazione cloud (approvata) e monitorare**
2. **Avviare le scansioni di individuazione**
3. **Analizzare i risultati**
4. **Aggiornamento del gruppo dirigente 3**
5. **Attività di mitigazione del rischio**
6. **Analizzare i risultati**
7. **Aggiornamento del gruppo dirigente 4**

Espandere la copertura dei controlli DLP	Lunedì	Martedì	Mercoledì	Giovedì	Venerdì
Settimana 7: distribuzione endpoint e applicazione cloud (approvata)					
Settimana 8: monitoraggio endpoint e applicazione (approvata) / dati a riposo					
Settimana 9: monitoraggio endpoint e applicazione (approvata) / dati a riposo					
Settimana 10: aggiornamento del gruppo dirigente 3					
Settimana 11: mitigazione del rischio					
Settimana 12: aggiornamento del gruppo dirigente 4					

Figura 6. Tempistica dell'implementazione – Parte 2

Passo 4: Integrare i controlli DLP nel resto dell'organizzazione

Obiettivo: la gestione degli incidenti è delegata alle principali parti interessate delle principali unità aziendali.

Descrizione generale: se non hai ancora coinvolto direttamente nell'implementazione della DLP i proprietari dei dati e le altre parti interessate principali, ora è arrivato il momento di farlo.

In particolare, il ruolo di manager di incidenti è più adatto per i proprietari dei dati, visto che sono responsabili in caso di perdita di dati. Affidando a loro la gestione degli incidenti, si rende superflua la presenza di intermediari e si migliora l'efficienza operativa. Si consente loro anche di valutare con precisione la loro tolleranza al rischio e comprendere correttamente come i loro asset di dati vengono utilizzati dagli altri.

Durante questo passaggio, chiedi al team di implementazione DLP di tenere una riunione introduttiva per presentare agli altri i controlli DLP. Poi organizza un corso di formazione per far conoscere ai nuovi membri del team l'applicazione di gestione degli incidenti. Prima di delegare le responsabilità di gestione degli incidenti, prevedi un periodo di tempo durante il quale fornirai una risposta assistita agli incidenti per consentire ai nuovi membri del team di diventare operativi.

1. **Creare e attivare la commissione**
2. **Aggiornamento del programma e ruoli**
3. **Formazione**
4. **Risposta assistita agli incidenti**
5. **Aggiornamento del gruppo dirigente 5**
6. **Risposta agli incidenti da parte della commissione**
7. **Aggiornamento del gruppo dirigente 6**

Integrare i controlli DLP nel resto dell'organizzazione	Lunedì	Martedì	Mercoledì	Giovedì	Venerdì
Settimana 13: selezione e notifica					
Settimana 14: aggiornamento del programma e ruoli					
Settimana 15: formazione con risposta assistita					
Settimana 16: aggiornamento del gruppo dirigente 5					
Settimana 17: risposta agli incidenti da parte della commissione					
Settimana 18: aggiornamento del gruppo dirigente 6					

Figura 7. Tempistica dell'implementazione – Parte 3

Fase 4:

Passare alla sicurezza proattiva

Obiettivo: passaggio alla protezione e risposta automatizzata agli eventi ad alto rischio.

Descrizione generale: in genere le organizzazioni adottano una strategia in due passaggi per implementare una protezione automatizzata, proattiva e personalizzata. Il primo passaggio consiste nella transizione dal controllo all'analisi. Il secondo nell'automatizzare la risposta. Ricorda che, quasi sempre, questo percorso non consente scorciatoie.

Passo 1: analisi e avvisi

Obiettivo: cominciare l'analisi dei dati e del loro spostamento all'interno di un'organizzazione per capire che cosa è successo durante una violazione dei dati.

Descrizione generale: per analizzare come si è verificata una violazione, devi andare oltre la modalità di controllo. A tal fine ti occorre visibilità su dove risiedono i dati, come vengono utilizzati e dove si spostano. Il limite degli strumenti di ricerca dei Big Data e dei tradizionali prodotti DLP che offrono soltanto funzionalità di rilevamento e controllo dei dati è che possono notificare una violazione dei dati agli amministratori della sicurezza informatica soltanto a fatto compiuto; in più sono privi di strumenti forensi robusti per eseguire le analisi. Sono configurati in modalità di solo controllo per un buon motivo, cioè per evitare di ostacolare le transazioni aziendali lecite, ma per questa stessa ragione non sono di grande aiuto nel prevenire gli incidenti. In questa fase le organizzazioni saranno magari "conformi", ma questo non le renderà sicure.

Le analisi post-violazione possono essere molto solide e sfruttare i migliori strumenti forensi disponibili, ma si tratta comunque di un approccio reattivo. In ogni caso le organizzazioni che si trovano in questa situazione possono imparare dai propri errori e rettificare manualmente le policy per la sicurezza dei dati in modo da consolidare la loro protezione per il futuro.

Passo 2: Automazione e personalizzazione proattiva della protezione dei dati

Obiettivo: diventare totalmente proattivi riguardo alla prevenzione di una violazione dei dati sia tramite infiltrazione che esfiltrazione, analizzando automaticamente il comportamento di utenti e sistemi, bloccando le attività e gli accessi considerati minacciosi e rettificando, sempre in modo automatico, le policy in base alle persone a mano a mano che si contestualizzano i comportamenti che adottano. Un approccio del tutto automatizzato genera una classificazione del rischio comportamentale relativo al singolo utente di un'organizzazione e, sulla base di tale classificazione, ritaglia la sicurezza su quella specifica persona in modo proattivo, senza ostacolarne la produttività. Le classificazioni del rischio tengono conto della variabilità nell'interazione degli utenti con i dati, i sistemi e le applicazioni, contestualizzando il comportamento come necessario in modo da ridurre i falsi positivi. Le azioni a basso rischio sono consentite, mentre quelle ad alto rischio provocano risposte automatizzate che vanno dalle notifiche agli amministratori, alla crittografia e arrivano fino al blocco totale, accanto ad altre misure di sicurezza predefinite.

Questo è l'aspetto della moderna sicurezza dei dati: un processo adattivo e automatizzato che interferisce il meno possibile con le attività lavorative, bloccando i comportamenti pericolosi ma senza ostacolare utenti e sistemi regolari per eccesso di zelo. Le soluzioni DLP basate sul rischio sono studiate per favorire gli obiettivi aziendali piuttosto che per frenarli, proteggendo dipendenti e dati senza interferire con il modo in cui le persone utilizzano i dati per svolgere il loro lavoro.

> **"Le soluzioni DLP basate sul rischio sono studiate per favorire gli obiettivi aziendali piuttosto che per frenarli, proteggendo dipendenti e dati senza interferire con il modo in cui le persone utilizzano i dati per svolgere il loro lavoro".**

Il passaggio dalla DLP passiva alla protezione dei dati adattiva al rischio consente alle organizzazioni di ridurre l'esposizione a danni finanziari oppure al brand causati dalle violazioni dei dati e, allo stesso tempo, di sfruttare l'intelligence comportamentale per facilitare la realizzazione degli obiettivi.

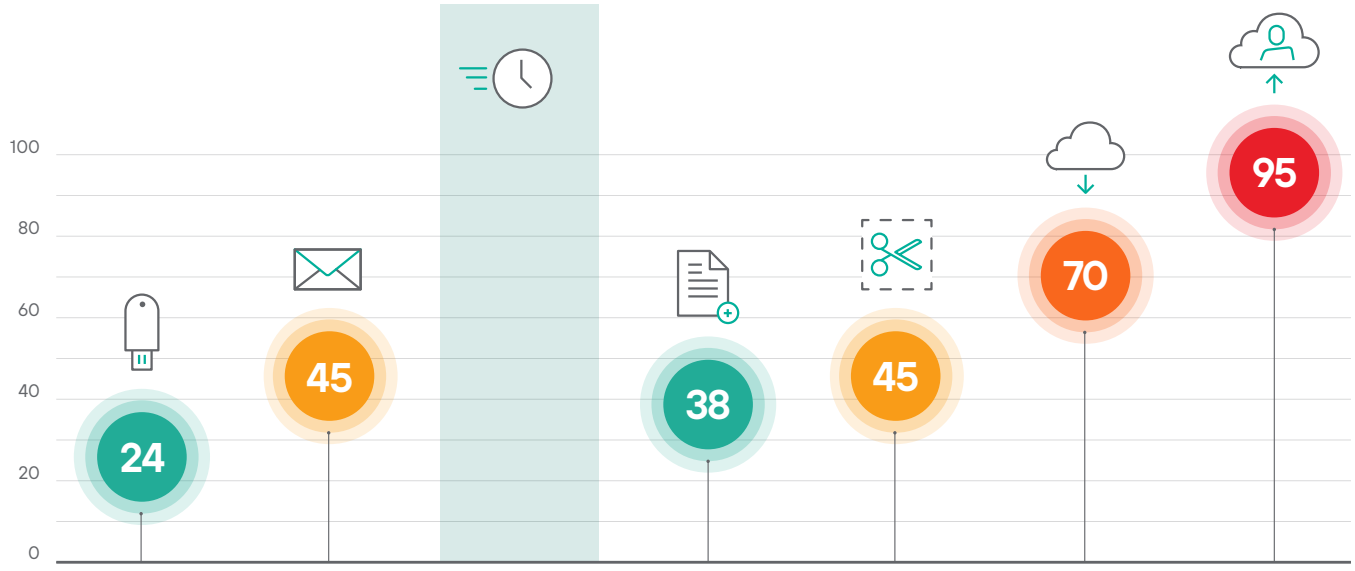


Figura 8. Aumento della classificazione del rischio in base alle attività dell'utente

Fase 5:

Tenere traccia dei risultati della riduzione del rischio

Obiettivo: mostrare il ROI dimostrando una riduzione misurabile del rischio.

Descrizione generale: al processo di monitoraggio della riduzione del rischio menzionato per la prima volta nella fase 3 devono essere aggiunti altri due punti chiave, ovvero:

1. Gli incidenti correlati devono essere raggruppati. Generalmente i gruppi sono basati su gravità, canale, tipo di dati e normativa. Per le organizzazioni più grandi, la creazione di sottogruppi aggiuntivi contribuisce a chiarire ulteriormente il rischio in base alle ubicazioni geografiche o alle filiali.

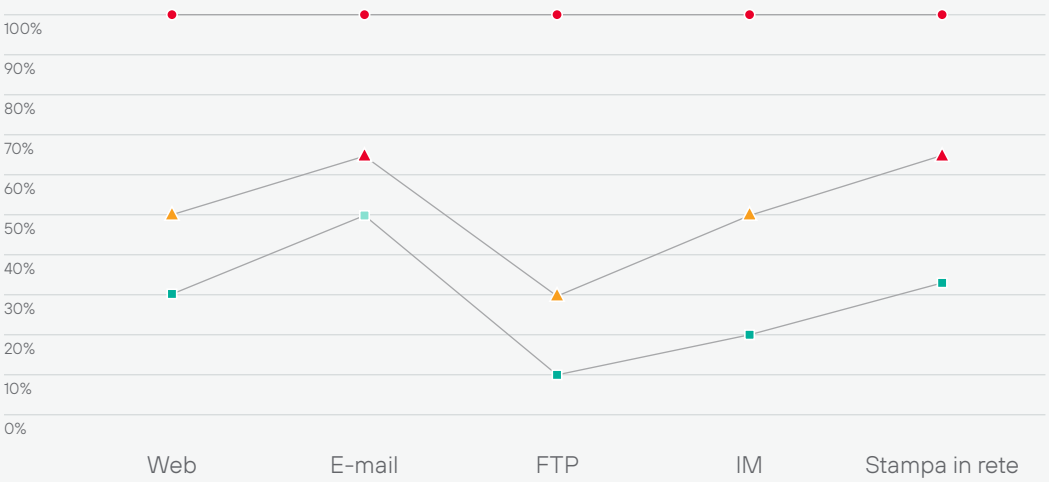
2. Mantenere la coerenza tra le fasi di riduzione del rischio. Per preservare l'integrità dei risultati, i periodi di monitoraggio e di riduzione del rischio devono avere la stessa durata. All'inizio, due settimane sono auspicabili per migliorare il time-to-value e per semplificare l'analisi. Tuttavia, sta a te determinare la tempistica più appropriata per la tua organizzazione.

Di seguito è riportato un esempio di come viene applicato il raggruppamento e di come viene tenuta traccia della riduzione dei rischi. Nell'esempio si è preso in considerazione un periodo di tempo coerente, ci si è concentrati sugli incidenti ad alto rischio e questi incidenti sono raggruppati secondo il rispettivo canale.

Opzione DLP adattiva al rischio: Se hai deciso di adottare un approccio adattivo al rischio, è consigliabile fornire un confronto tra gli incidenti acquisiti in modalità di solo controllo (tutti gli incidenti) e gli incidenti che richiedono un'indagine con applicazione graduale. La sintesi deve mostrare il numero di incidenti per ogni livello di rischio 1-5, contrapposti a quelli che effettivamente richiedono un'indagine (livelli di rischio 4-5)

Infine, quando aggiorni il team dirigenziale sul processo DLP e sui relativi risultati, ricordati che la sintesi è un pregio. Quando spieghi i vettori ad alto rischio cui è esposta l'organizzazione e delinei le attività di mitigazione del rischio consigliate, con i relativi costi, vantaggi e sforzi richiesti, concentrati sul quadro generale.

Probabilità di perdita di dati



Legenda degli indicatori

- Alto
- Moderato
- Basso
- Accettabile
- Riferimento di 30 giorni
- 60 giorni
- 90 giorni

Numero di incidenti in 90 giorni

Incidenti	Web	E-mail	FTP	IM	Stampa in rete
Riferimento di 30 giorni	200	150	50	10	45
Riferimento di 60 giorni	100	100	15	15	30
› Riduzione del rischio su 60 giorni	50%	33%	70%	50%	33%
Riferimento di 90 giorni	60	76	5	2	15
› Riduzione del rischio su 90 giorni	70%	49%	90%	80%	67%

Obbiettivi

- **60 giorni** 25% + riduzione
- **90 giorni** 50% + riduzione

Figura 9. Monitoraggio del rischio di perdita dei dati

Conclusioni

Per ottenere un'implementazione DLP di successo non è sufficiente adottare nuove tecnologie e installarle nel data center, poiché il suo successo dipenderà dalla tua capacità di:

1. Comprendere la metodologia e la strategia di esecuzione dei fornitori DLP. La tua organizzazione trae vantaggio nel riconoscere il tipo di approccio dei fornitori alla DLP. In questo modo puoi determinare le metodologie dei fornitori più promettenti per l'ambiente dell'organizzazione e quali tecnologie DLP prendere in considerazione. Un fornitore in grado di offrire una soluzione adattiva al rischio può comportare vantaggi di lunga durata per l'organizzazione e, tra questi, una maggiore efficienza e produttività. E non dimenticare: l'applicazione della metodologia di un fornitore alla tecnologia di un altro comporta delle conseguenze negative a lungo termine.

2. Applicare la formula del rischio per la perdita di dati. Una volta compresa e applicata la formula del rischio per la perdita di dati, il team di sicurezza può collaborare con i proprietari dei dati per identificare e assegnare priorità agli asset di dati. Inoltre, ogni attività di mitigazione del rischio deve essere progettata al solo scopo di ridurre la frequenza di occorrenza (FO) delle perdite di dati. La FO è la misurazione appropriata per monitorare la riduzione del rischio e mostrare il ROI per i controlli DLP. Promemoria: presta particolare attenzione quando metti a confronto le soluzioni DLP tradizionali con una DLP che si avvale di una tecnologia adattiva al rischio, per assicurarti di non confrontare falsi positivi con positivi reali.

3. Applicare la regola 80/20 per l'assegnazione delle risorse. Comprendendo quali vettori di perdita di dati rappresentano il rischio maggiore di una violazione dei dati ad alto impatto, l'organizzazione può utilizzare la regola 80/20 per assegnare risorse e formulare strategie efficaci di protezione dei dati.

4. Seguire i nove passi verso il successo con la DLP. Sia che adotti un approccio DLP tradizionale o adattivo al rischio, il nostro processo in 9 passi è una formula collaudata per implementare in modo pratico i controlli DLP e ottenere risultati utilizzabili, misurabili e adattivi al rischio.

Forcepoint

forcepoint.com/contact

Informazioni su Forcepoint

Forcepoint è l'azienda leader nel settore della sicurezza informatica per la protezione degli utenti e dei dati. La sua missione è proteggere le aziende e guidarne la crescita e la trasformazione digitale. Le soluzioni human-centric di Forcepoint si adattano in tempo reale alle modalità di interazione tra persone e dati, consentono un accesso sicuro e, allo stesso tempo, permettono ai dipendenti di creare valore. Dalla sua sede di Austin, Texas, Forcepoint crea ambienti sicuri e affidabili per migliaia di clienti in tutto il mondo.

[Practical-Exec-Guide-to-DLP-Whitepaper-IT] 24Sept2021