IMPARARE FACILMENTE

Edizione speciale
Netskope

Sicurezza dei dati unificata

for dummies®
A Wiley Brand

Modernizza la sicurezza dei dati

Proteggi i dati ovunque, statici e in movimento

Minimizza i falsi positivi

Edizione targata:

netskope

Informazioni su Netskope

Netskope, leader nella sicurezza e nel networking moderni, affronta le esigenze dei team di sicurezza e networking fornendo accessi ottimizzati e sicurezza in tempo reale in base al contesto per persone, dispositivi e dati, ovunque si trovano. Migliaia di clienti, oltre 30 dei quali presenti nell'elenco Fortune 100, si affidano alla piattaforma Netskope One, al suo motore Zero Trust e alla sua potente rete NewEdge per ridurre i rischi e ottenere piena visibilità e controllo su cloud, AI, SaaS, web e applicazioni private, massimizzando sicurezza e prestazioni senza compromessi.

Vorremmo ringraziare le persone che hanno reso possibile questo book:

In Netskope: Ankur Chadda, Tom Baumgartner, Ramien Ebadypour, Emily Wearmouth, Kathy Jacobsen, Stephenie Pang

Sicurezza dei dati unificata

Edizione speciale Netskope

for dummies®
A Wiley Brand

Sicurezza dei dati unificata For Dummies®, Edizione speciale Netskope

Editore
John Wiley & Sons, Inc.
111 River St., Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-394-42063-6 (pbk), ISBN 978-1-394-42064-3 (ebk), ISBN 978-1-394-42065-0 (ebk)

Ringraziamenti dell'editore

Editore: Elizabeth Kuball

Direttore acquisizioni: Traci Martin

Caporedattore senior: Rev Mengle

Client Account Manager: Jeremith Coward

Direttore di produzione: Magesh Elangovan

Assistenza speciale: Joe Kraynak

Introduzione

Il concetto di sicurezza dei dati non è nuovo nel mondo della sicurezza informatica, ma negli ultimi dieci anni le aspettative verso i sistemi di sicurezza tradizionali sono nettamente cambiate. Un tempo, i professionisti della sicurezza potevano contare sul fatto che le informazioni da difendere erano gelosamente custodite tra le mura dei data center; ma la trasformazione digitale ha spinto le aziende grandi e piccole a trasferire i loro dati nel cloud e in posizioni distribuite. Oggi, le informazioni sensibili sono a portata degli utenti ovunque, mentre le connessioni digitali dell'azienda possono essere condivise con moltissimi fornitori, partner e consulenti esterni. Questi scenari portano con sé tutta una serie di opportunità commerciali senza precedenti (ed è una buona notizia) e di difficoltà sul fronte della sicurezza, soprattutto a livello di dati (notizia cattiva).

Le violazioni dei dati possono avere conseguenze devastanti per un'azienda, e i rischi introdotti da utenti interni (per comportamenti distratti o illeciti) sono tanto pericolosi quanto i ben più clamorosi attacchi perpetrati da vettori esterni. In entrambi i casi, le informazioni sensibili sono in pericolo. Oggi, la sicurezza dei dati è una parte fondamentale dei requisiti di compliance, con normative di settore e sulla privacy che definiscono nel dettaglio le responsabilità delle aziende e introducono pesanti sanzioni in caso di inadempimento.

Le aziende devono adottare un approccio nuovo e applicare le policy di sicurezza dei dati in modo coerente ovunque vengano trasferite le informazioni. In un mondo ideale, la sicurezza dei dati sostiene gli obiettivi commerciali e al tempo stesso tutela l'azienda, ma la gestione delle policy e degli strumenti di sicurezza spesso si rivela complicata e costosa. Alle aziende servono soluzioni di sicurezza dei dati in grado di semplificare il rispetto delle policy pur garantendone l'efficacia. Una possibile risposta è data da una nuova generazione di soluzioni DSPM (*Data Security Posture Management*) e DLP (*Data Loss Prevention*) erogate dal cloud, che sono meno complesse, altamente scalabili, più efficienti in termini di costi e capaci di proteggere i dati in modo più affidabile e accurato, riducendo l'esposizione ad accessi non autorizzati o usi impropri dei dati. Si tratta di un equilibrio difficile da raggiungere, ma con la giusta guida non è impossibile.

Informazioni su questo libro

Questo libro può prepararti a prendere decisioni informate su come valutare l'attuale approccio alla sicurezza dei dati dell'azienda ed esplorare le nuove soluzioni disponibili per trovare quella basata sui principi Zero Trust più adatta ai tuoi bisogni, per applicare i parametri di sicurezza in modo coerente e in base al contesto. Evita gli slogan promozionali per spiegarti come funzionano i moderni sistemi DLP erogati dal cloud e aiutarti a individuare le caratteristiche e le capacità indispensabili per proteggere i dati in modo affidabile, ovunque.

Qualche presupposto scontato

Questo libro parte dal presupposto che tu sappia come le aziende hanno usato il cloud computing per diventare più flessibili ed equipaggiarsi meglio per gestire la trasformazione digitale. L'altro presupposto è che ti interessa trovare il giusto mix di tecnologie e processi migliorati per garantire la protezione dei dati sensibili ovunque risiedano e possano essere trasferiti.

Icone utilizzate in questo libro

Il libro contiene alcune icone per attirare l'attenzione del lettore sulle informazioni importanti. Esse sono:


SUGGERIMENTO

Le informazioni contrassegnate da questo simbolo servono a semplificarvi la vita.


RICORDA

Questo simbolo serve a sottolineare i punti che vale la pena tenere a mente.


ATTENZIONE

Leggete con attenzione per evitare potenziali grattacapi in futuro.

Oltre questo libro...

Tutto quello che abbiamo detto qui non ti basta? Se, quando hai finito di leggere, vuoi approfondire l'argomento, visita www.netskope.com.

IN QUESTO CAPITOLO

- **Capire dove vengono salvati i dati sensibili e come vengono monitorati**
- **Scoprire cosa vuol dire in pratica "sicurezza dei dati"**
- **Saperne di più su DSPM (*Data Security Posture Management*) e DLP (*Data Loss Prevention*)**
- **Analizzare perché le soluzioni DLP tradizionali non sono più, da sole, una strada percorribile**
- **Passare a una strategia cloud-first con una soluzione unificata per la sicurezza dei dati**
- **Sfatare i miti più comuni sulle soluzioni DLP**

Capitolo 1
Aggiornamento sulle basi della sicurezza dei dati

Con la digitalizzazione, accedere ai dati, usarli, modificarli e condividerli è molto più facile, ma monitorarli e proteggerli è molto più complesso. Questo capitolo vuole essere un aggiornamento sulle nozioni di base della sicurezza dei dati e sulle sfide emergenti, e anche svelare cosa c'è dietro al mito della prevenzione della perdita di dati (DLP).

Una guida rapida ai dati sensibili

La maggior parte dei dati considerati sensibili è in circolazione da anni, decenni o anche di più:

- **Dati/informazioni personali**, come codici fiscali, numeri di carte di credito, patenti di guida, informazioni sanitarie e indirizzi postali personali
- **Proprietà intellettuali**, come progetti, invenzioni, brevetti o codici sorgente

- **Informazioni riservate e segreti commerciali**, tra cui piani finanziari, contratti, dichiarazioni fiscali, informazioni su fusioni e acquisizioni e versioni non definitive di documenti come i comunicati stampa

La novità sta nel fatto che il panorama aziendale odierno ha completamente cambiato il modo in cui le informazioni vengono condivise e (ahimè) esposte. Oggi, quasi tutti i dati sensibili vengono creati, archiviati e trasferiti tramite strumenti digitali. Quindi viaggiano da e verso servizi cloud, reti aziendali o qualsiasi altro mezzo a disposizione degli utenti. Contemporaneamente, vengono usate sempre più applicazioni per archiviare e condividere tali informazioni su più piattaforme, rendendole accessibili praticamente da qualsiasi dispositivo ovunque. La diffusa adozione degli ambienti di lavoro ibridi da parte di molte aziende non fa che complicare le cose.

Questo aumento esponenziale della quantità, varietà e velocità di trasferimento delle informazioni rende sempre più difficile individuare e proteggere i dati sensibili. E a complicare il quadro, l'imponente volume di informazioni in circolazione compromette la capacità dei tradizionali sistemi di sicurezza di tenere il passo con le minacce emergenti.

RICORDA

In generale, quando parliamo di dati sensibili ci riferiamo a informazioni riservate o personali. Cosa si intende per "sensibili" dipende da quale prospettiva si guardano i dati, se aziendale o individuale.

Uno tsunami di dati

Secondo Statista, entro il 2028 il mondo sarà sommerso da ben 394 zettabyte di dati! In grandissima parte verranno creati e salvati direttamente sul cloud, e aumenteranno di anno in anno. I sistemi di protezione dei dati e i relativi operatori si trovano quindi ad affrontare sfide come:

- **Sempre più categorie di dati sensibili:** il proliferare delle leggi e dei regolamenti sulla privacy, che tutelano categorie sempre più ampie di persone e tipi di informazioni in tutto il mondo, sta facendo proliferare le categorie di dati sensibili. Tra questi, i dati che permettono di identificare una persona, come posizione geografica, informazioni sulla condizione finanziaria o di salute, sulle preferenze personali, sul credo religioso o sull'orientamento sessuale. Ma anche i numeri delle carte d'identità e di credito, codici

sorgenti, design, piani finanziari, conti correnti, contratti, dichiarazioni fiscali, password, informazioni su acquisizioni e fusioni, dati sanitari protetti, e-mail riservate e informazioni sul genere e sulla religione. Le categorie di dati sensibili possono cambiare da un Paese all'altro.

- **Sempre più formati e tipi di dati:** Questo include file PDF, file immagine (come JPG, PNG e BMP), file video (come MP4, MOV e AVI), file compressi e archivi (come ZIP, RAR e ISO), allegati di posta elettronica, messaggi Slack, chat, moduli online, screenshot, fogli di calcolo, progetti CAD, post su social media, file di testo, presentazioni ed e-mail.
- **Espansione del contesto:** è in base al contesto che si devono stabilire le modalità di accesso, uso, trasferimento e condivisione dei dati sensibili. Il contesto aiuta a definire le azioni rischiose per la sicurezza dei dati sensibili e quali eventi considerare come dei tentativi di violazione o di accesso non autorizzato perché ci dice chi, dove, cosa, come, perché, quando, a chi e altri fattori.

Di fronte a un'ondata sempre più imponente di dati imperscrutabili, i sistemi di sicurezza tradizionali sono costretti a peccare di cautela, il che causa non pochi grattacapi a livello amministrativo. Perché? Oggi i team di incident response devono fare i conti con valanghe di falsi positivi, la maggior parte dei quali devono essere analizzati manualmente da specialisti già sommersi di lavoro.

La sicurezza dei dati non si limita ai "soli" dati

Le aziende hanno bisogno di strategie automatizzate in grado di identificare, monitorare e tutelare efficacemente le informazioni più importanti. Allo stesso tempo la sicurezza dei dati deve affrontare continuamente nuove sfide, che a loro volta aggiungono ulteriori livelli di complessità, come:

- **Nuovi rischi informatici:** le aziende sono più che mai vulnerabili a violazioni dei dati, che possono essere intenzionali e non. Comportamenti come il furto o l'uso improprio dei dati da parte dei dipendenti rappresentano un rischio serio. L'82% delle violazioni dei dati implica il fattore umano, tra cui
  - *Dipendenti malintenzionati:* un dipendente scontento che fa uno screenshot di un foglio Excel riservato e poi manda i dati

su un'app di archiviazione personale di tipo SaaS (*Software-as-a-Service*) oppure usa l'istanza personale di un account di posta elettronica aziendale (ad esempio, un account Gmail personale invece di quello aziendale).

- *Esposizione accidentale:* un dipendente che manda inavvertitamente troppe informazioni a un fornitore o condivide troppi file in una cartella OneDrive. Comportamenti di questo tipo sono tra le cause più comuni delle violazioni di dati.

  Attacchi esterni o tentativi di hacking sono altri episodi che mettono i segreti aziendali a rischio, con richieste di riscatto o minacce di essere rivelati al pubblico o alla concorrenza.

- **Applicazioni cloud, inclusi i servizi di tipo SaaS e IaaS (*Infrastructure-as-a-service*):** le applicazioni SaaS, in particolare, si stanno diffondendo a velocità sbalorditive. Secondo studi recenti l'azienda media usa più di 2.400 applicazioni cloud, il 97% delle quali come shadow IT (cioè non autorizzate dal reparto IT, oppure a esso sconosciute o addirittura invisibili). Questo crea dei problemi sul piano tecnico e della sicurezza perché i dati possono essere archiviati e condivisi in tantissime applicazioni SaaS, viaggiare liberamente tra reti aziendali e dispositivi gestiti e essere facilmente alla portata dei dipendenti (e anche di utenti esterni) che si collegano da remoto attraverso dispositivi non gestiti. Senza un monitoraggio e una gestione efficaci, le applicazioni cloud possono diventare presto un importante vettore di attacco. Quindi le aziende devono intervenire per aggiornare le soluzioni di protezione dei dati e difendersi da queste minacce.
- **Lavoro ibrido:** la diffusione degli ambienti di lavoro ibridi sta rivoluzionando il modo di archiviare e accedere ai dati sensibili delle aziende. Le procedure aziendali di routine sono cambiate drasticamente rispetto a quando buona parte delle informazioni critiche veniva custodita nei data center privati controllati direttamente dalle aziende. I modelli di lavoro ibrido hanno spalancato le porte a una nuova era, in cui i dati sensibili sono altamente distribuiti ben oltre i tradizionali confini aziendali, dove le aziende non hanno né visibilità né controllo. Oggigiorno, i dati sono distribuiti in una serie di ambienti digitali e fisici, tra cui data center, sedi centrali, succursali, uffici domestici e dispositivi (aziendali o personali) usati dai dipendenti da remoto.
- **Nuovi requisiti di conformità:** la conformità è da sempre un tasto dolente, ma con il proliferare di regolamenti che comportano sanzioni sempre più severe o rischi di incorrere in azioni legali, ogni azienda, dalla più grande alla più piccola, è sotto

pressione per rispettare gli standard e tutelare i dati sensibili, loro e dei loro clienti e partner. Le aziende devono darsi da fare per rispettare i regolamenti di settore, come il PCI-DSS (*Payment Card Industry Data Security Standard*), l'HIPAA (*Health Insurance Portability & Accountability Act*) e il GLBA (*Gramm–Leach–Bliley Act*), oltre che a un ampio ventaglio di leggi e regolamenti applicabili, tra cui GDPR (Regolamento generale sulla protezione dei dati), CCPA (*California Consumer Privacy Act*), *Colorado Privacy Act*, *Connecticut Data Privacy Act*, *Virginia Consumer Data Protection Act* e *Utah Consumer Privacy Act*, solo per citarne alcune. Tra i tanti Paesi al mondo che hanno introdotto norme sulla privacy, ci sono Brasile, Giappone, Singapore e Regno Unito. Oggi più che mai, le aziende devono dimostrare di aver preso le misure necessarie per proteggere le informazioni personali dei loro clienti e garantire il rispetto delle leggi applicabili se vogliono evitare drastiche conseguenze.

- **Talenti rari e costosi:** le risorse specializzate necessarie per attuare complessi programmi di sicurezza dei dati sono merce rara. Le tecnologie per la sicurezza dei dati richiedono una supervisione esperta per gestire l'enorme quantità di incidenti segnalati dai sistemi. E il problema non può che aggravarsi quando per monitorare i servizi cloud come le applicazioni SaaS si usano sistemi tradizionali, che non sono stati progettati per questo e generano una quantità smisurata di falsi positivi e quindi di lavoro per il team. Tecnici esperti vuol dire stipendi elevati, al pari delle loro competenze, e i costi a carico delle aziende non sono da sottovalutare: se rimangono, devono essere pagati; se invece se ne vanno per il troppo lavoro, devono essere sostituiti.

Cos'è la sicurezza dei dati unificata e come può aiutare?

La sicurezza dei dati unificata combina i migliori approcci alla gestione della sicurezza dei dati (DSPM) e alla prevenzione della perdita dei dati (DLP) per ridurre i costi e la complessità, il tutto da un unico pannello di controllo.

La tecnologia DSPM assicura un processo e un framework che aiutano le aziende a gestire e migliorare attivamente la sicurezza dei dati, sia on-premise che sul cloud. A tal fine, individua, valuta e mitiga i rischi relativi ai dati, comprese le perdite di dati, garantendo la conformità normativa. Ciò offre ai responsabili della sicurezza informatica e ai

professionisti del settore la massima visibilità sui dati detenuti dall'azienda, sulla loro ubicazione, su chi può accedere a essi e sui rischi delle interazioni con tali dati. Gestisce il rischio durante l'intero ciclo di vita dei dati, con esecuzione automatica di scoperta, classificazione e tagging dei dati, profilazione degli utenti per privilegi e accessi, tracking delle esfiltrazioni di dati e delle violazioni alle policy, remediation, escalation e reportistica.

Le tecnologie di sicurezza DLP sono sistemi progettati per identificare e proteggere automaticamente archiviazione, flusso e uso di dati sensibili distribuiti ovunque su tutte le reti, gli utenti e i servizi di qualsiasi azienda. Questa tecnologia viene implementata per individuare un ampio ventaglio di dati sensibili, tra cui dati o informazioni personali di clienti e dipendenti, documenti finanziari e proprietà intellettuale. La tecnologia DLP monitora l'accesso e l'uso ai dati, impedendone il furto, la divulgazione o l'esposizione accidentali. In più, aiuta le aziende a contenere il rischio di violazioni dei dati, tenendo d'occhio i file più critici per evitare la pubblicazione involontaria di informazioni riservate. Alla luce di un panorama legislativo sempre più ampio e rigoroso, l'importanza dei sistemi DLP come misura di sicurezza continua a crescere per le aziende, che devono difendersi da costose violazioni e soddisfare i requisiti di compliance.

Perché ormai le tecnologie DLP tradizionali sono tristemente inadeguate da sole

Le soluzioni DLP tradizionali vengono usate da oltre dieci anni per la sicurezza dei dati sensibili. Il problema è che, con il tempo, queste tecnologie tradizionali si sono guadagnate la reputazione di essere troppo complesse da implementare oltre che costose, limitate nell'ambito di applicazione, sempre meno accurate e incapaci di garantire il livello di copertura necessario per gli attuali modelli di lavoro ibrido. Le soluzioni DLP sono nate per proteggere i dati in un data center o nei locali dell'azienda, senza però riuscire ad adattarsi completamente ai cambiamenti portati dall'era del cloud. I sistemi DLP tradizionali sono ottimi in ciò per cui sono stati progettati, ma oggi sono chiamati a fare tutt'altro: devono garantire la sicurezza di dati archiviati sul cloud o trasferiti da un ambiente cloud all'altro. In più il modello su cui si fondano, che parte da un perimetro di sicurezza, non riesce a tenere il passo con dati sparsi su tantissime postazioni e applicazioni.

Lo svantaggio dei sistemi DLP tradizionali

I sistemi DLP tradizionali, fatti di numerosi componenti hardware e software, possono essere un incubo da implementare e mantenere. La configurazione può essere complessa e costosa, non certo l'ideale per aziende con budget e risorse informatiche limitate. Coprire aziende altamente distribuite è anche una sfida notevole e costosa perché molto probabilmente l'architettura DLP locale deve essere replicata in ogni filiale. E anche in questo caso, non si arriva a soddisfare gli importanti requisiti dei moderni ambienti professionali, come lo smart working, le applicazioni cloud e la flessibilità richiesta per consentire l'uso dei dispositivi personali dei dipendenti (BYOD).

Le tecnologie DLP tradizionali richiedono poi obbligatoriamente lunghi aggiornamenti software e continue correzioni, che interrompono le normali attività aziendali. Per evitare questo, spesso le aziende evitano gli upgrade, affidandosi a versioni vecchie di mesi o anni rispetto alle più recenti. Quindi, non si avvalgono delle protezioni più aggiornate e allineate ai requisiti più recenti in termini di gestione dei dati, conformità e contenimento dei rischi.

Senza gli aggiornamenti e le patch di sicurezza si rischiano problemi di ogni tipo, tra cui vulnerabilità, violazioni dei dati e protezione inadeguata delle informazioni. Questo può mettere a rischio i dati sensibili e la conformità dell'azienda ai regolamenti sulla protezione dei dati. Inoltre, la complessità intrinseca tipica dei sistemi DLP tradizionali spesso porta a pratiche di protezione incoerenti ed esageratamente specifiche, che portano a un uso inefficiente del tempo e delle risorse.

ATTENZIONE

Per alcune aziende, le interruzioni causate dalle tecnologie DLP tradizionali sono così gravi da spingerle a scegliere la modalità "solo monitoraggio", secondo cui il sistema si limita a osservare cosa accade senza applicare la policy. Un approccio di questo tipo è un po' come usare una cassaforte senza combinazione... sperando che nessuno ci porti via contanti, gioielli o documenti importanti.

Il dilemma dei falsi positivi

I sistemi DLP tradizionali non solo comportano implementazioni e processi complessi, ma richiedono anche un notevole dispendio di risorse e interventi manuali per perfezionarne i parametri e assicurare un monitoraggio efficace. Come accennato prima, i falsi positivi esercitano una forte pressione sui team di sicurezza.

Il numero di incidenti da correggere manualmente è cresciuto al punto che i team di incident response non hanno neppure il tempo di esaminarli tutti, figuriamoci di gestirli. I team di incident response ricevono molti avvisi che non sono problemi reali, senza peraltro avere un contesto per poter determinare a posteriori il livello di rischio. Sostanzialmente, tali avvisi vengono ricevuti troppo tardi rispetto a quando si verifica l'incidente, quindi, oltre a non avere contesto, i team si trovano a dover ricostruire gli incidenti sulla base delle informazioni date da dipendenti che nemmeno se li ricordano. Gli allarmi generati possono essere migliaia o centinaia di migliaia ogni giorno e provenire dalle fonti più disparate. Vista la mole di eventi da monitorare, i team di sicurezza non possono permettersi di esaminare ogni singolo allarme; anzi, sono costretti in gran parte a ignorarli se vogliono solo provare a tenere il passo.

Un importante fattore da considerare è che i dati sono dislocati in posizioni diverse e viaggiano da un luogo all'altro anche al di fuori della rete dei data center gestiti. Le soluzioni DLP tradizionali non sono equipaggiate per gestire una tale mole e varietà di dati (peraltro in continua crescita), e non possono contare su funzioni di rilevamento assistite da *machine learning* (ML), su casi d'uso moderni relativi alla condivisione dei dati e su informazioni di contesto. I criteri di sicurezza statici su cui fanno affidamento non sono in grado di adattarsi a rischi e contesti aziendali mutevoli, né di considerare variabili come chi usa i dati, in che modo, in quale ambiente e istanza applicativa, con comportamenti sicuri o meno e verso quale destinazione finale.

Nel tentativo di aggirare il problema sono stati aggiunti strumenti di orchestrazione e automazione della sicurezza informatica, come la tecnologia UEBA (*User and Entity Behavior Analytics*), che facilitano la gestione degli allarmi consentendo interventi più rapidi. Ma se il sistema DLP è inaccurato, non è possibile individuare il contesto di business o il livello di rischio, quindi i modelli UEBA non possono operare correttamente.

Assicurare una protezione efficace dei dati sensibili richiede un sistema DLP integrato e automatizzato, così da monitorare e verificare costantemente l'identità dei singoli individui e dispositivi autorizzati, i relativi comportamenti, la modalità di collaborazione tra loro e di condivisione dei dati con l'esterno, le applicazioni usate e il relativo livello di rischio, nonché diversi altri fattori contestuali. Questo approccio Zero Trust (v. il Capitolo 3) consente di applicare con precisione criteri di sicurezza e regole di *incident response*, in

grado di adattarsi a condizioni di rischio mutevoli e a specifici contesti d'uso dei dati. Questo approccio protegge i dati senza interrompere l'attività aziendale.

I sistemi DLP tradizionali non sono fatti per proteggere gli ambienti cloud

La tecnologia DLP tradizionale è fondata su un modello di sicurezza che presume che tutti i dati sono archiviati nella rete aziendale e in ambienti gestiti. Questo modello è inadatto ai giorni nostri, in cui i dati sono dislocati in moltissime applicazioni cloud e accessibili da utenti e dispositivi all'esterno della rete aziendale. Inoltre, i sistemi DLP tradizionali non erano progettati per integrarsi con l'ampia gamma di servizi e infrastrutture cloud attualmente in uso, il che rende difficile, se non impossibile, assicurare ai dati sul cloud una protezione completa.

Oggi molte aziende cercano di "cloudificare" i sistemi DLP tradizionali aggiungendo due soluzioni di sicurezza: CASB (*Cloud Access Security Broker*) per il traffico delle applicazioni cloud e SWG (*Secure Web Gateway*) per il traffico web proveniente dai lavoratori remoti e dalle filiali. La speranza è che l'aggiunta di queste soluzioni fornisca ai sistemi DLP tradizionali la capacità di estendere agli ambienti cloud le funzioni di protezione esistenti, ricercando dati sensibili anche al di fuori del data center.

Purtroppo, questo approccio presenta alcuni difetti di base:

- **L'integrazione si è rivelata molto difficile.** Comporta il reindirizzamento del traffico di rete basato sul protocollo ICAP (*Internet Content Adaptation Protocol*), un argomento molto complesso che esula dall'ambito di questo libro.
- **Le soluzioni CASB e SWG, sebbene appositamente progettate per il cloud, spesso dimostrano limitate capacità di protezione dei dati.**
- **Anche riesce nell'integrazione, questo approccio è insostenibile.** Le soluzioni CASB si avvalgono di API (*Application Programming Interface*) per collegarsi ad applicazioni cloud aziendali come Amazon Web Services (AWS), Box, Google Workspace, Microsoft 365, Microsoft Teams, Salesforce, Slack e Zoom. Garantire la disponibilità delle API per tutte le applicazioni cloud usate dagli utenti e tenerle aggiornate può rivelarsi un incubo.

RICORDA

- **Il consolidamento delle policy di sicurezza usate dai sistemi locali e da quelli su cloud è difficile.** Ad esempio, spesso le soluzioni CASB non sono in grado di replicare le policy come i sistemi DLP tradizionali. Proprio a causa di questa differenza, le policy e le console di gestione risultano frammentate e non sincronizzate.

  La disgiunzione delle console di gestione e il mancato coordinamento delle policy di protezione dei dati sono due effetti collaterali diffusi dell'integrazione di soluzioni CASB e SWG nei sistemi DLP tradizionali.

- **L'integrazione di tecnologie DLP on-premise con applicazioni su cloud tramite soluzioni CASB genera un ritardo, detto *latenza*.** Anche quando il sistema DLP tradizionale rileva violazioni alle policy sui dati in un ambiente cloud, l'innesco di una risposta potrebbe richiedere minuti o ore, se non di più. Facciamo un esempio: si è verificata una violazione, che è stata identificata ma non arrestata in tempo (quindi i dati sono compromessi!).

Puntare sull'uso combinato di un sistema DLP tradizionali e di tecnologie cloud significa mettere in campo due strumenti molto diversi fra loro. Uno (la soluzione CASB) si occupa di servizi cloud, mentre l'altro (il DLP tradizionale) è una complessa architettura on-premise che include componenti hardware e anche software. Il risultato è una soluzione fragile e facile da aggirare che genera parecchia latenza e risulta molto complessa da ottimizzare e mantenere. Le soluzioni DLP tradizionali sono on-premise. Punto.

Un sistema DLP moderno deve essere in grado di soddisfare in modo adattivo standard di cloud security altamente mutevoli, contando su policy di sicurezza dinamiche e su capacità di valutazione del rischio in tempo reale, nell'ottica di aiutare le aziende a garantire la sicurezza dei dipendenti, dei clienti e dei dati.

La soluzione? Integrazione del DSPM con l'attuale DLP erogato tramite cloud. Oltre alla protezione extra assicurata da CASB e SWG, il DSPM aggiunge rilevamento e classificazione in automatico dei dati inattivi sul cloud per contribuire ulteriormente alla gestione del rischio durante l'intero ciclo di vita dei dati, indipendentemente dal fatto che siano strutturati o meno, dalla loro posizione e da chi (persona o macchina) acceda a essi o li utilizzi.

Sicurezza dei dati unificata per l'era del cloud e dell'IA

La trasformazione digitale ha rivoluzionato il modo in cui le aziende offrono assistenza e sviluppano prodotti e servizi. Ma ha anche avuto un forte effetto sul modo di proteggere i dati. Aziende grandi e piccole si affidano ampiamente alle tecnologie cloud per alimentare la crescita commerciale, e le strategie di sicurezza devono tenere il passo. Per adeguarsi alle esigenze della nuova forza lavoro ibrida (in continua crescita), l'architettura di sicurezza dei dati deve passare a una strategia cloud-first per estendere la copertura e assicurare più efficienza e scalabilità, nonché solide capacità di elaborazione e misure di prevenzione del rischio ancora più efficaci. Riconfigurare l'architettura della sicurezza dei dati consentirà alle aziende di garantire il successo delle iniziative orientate al lavoro ibrido e di rendersi pronte per il futuro, tenendo conto anche dell'impatto dell'intelligenza artificiale (IA). Quando si tratta di fuga di dati sensibili, il crescente uso dell'IA da parte dei dipendenti aggiunge un ulteriore livello di preoccupazioni relative alla sicurezza. Avere una soluzione per la sicurezza dei dati unificata all'interno dell'azienda può risolvere tutte queste sfide, ma è un'impresa difficile. Con la continua evoluzione dei rischi e lo sviluppo delle soluzioni cloud-ready, è il momento giusto di valutare l'idea.

Le soluzioni DSPM e DLP erogate sul cloud non richiedono implementazioni complesse, ma solo l'attivazione di un servizio cloud. Non ci sono troppe componenti e soluzioni software da aggiornare individualmente e mantenere manualmente, né database DLP da gestire, esperti in database da assumere, server da sostituire in seguito a obsolescenza, o proxy hardware da aggiornare.

Le piattaforme di sicurezza dei dati basate sul cloud sono progettate per essere facilmente integrate con applicazioni di sicurezza, reti, infrastrutture e servizi cloud, e acquisiscono in modo coerente informazioni di contesto e sui rischi a partire da altri controlli. Gli algoritmi di sorveglianza e rilevamento dei dati funzionano meglio nel cloud, dove l'accesso a risorse infinitamente scalabili riduce il carico sull'infrastruttura informatica, tenendo il passo con nuovi casi d'uso e con un sempre più ampio ventaglio di agenti endpoint. Eliminando le limitazioni poste dall'infrastruttura on-premise, gli utenti sono protetti ovunque.

In più, non essendo un'architettura cloud collegata ad alcuna infrastruttura e programma preesistente, il sistema di sicurezza dei dati

riceve sempre aggiornamenti in tempo reale ovunque. Questo approccio è molto più efficiente ed efficace per proteggere i dati sensibili dell'azienda.

Miti da sfatare

Quando si parla di servizi DLP e DSPM erogati sul cloud, si sa di entrare in un mercato pieno di paroloni, slogan e promesse irrealistiche, dove gli utenti vengono bombardati di informazioni e sono spesso confusi davanti alle opzioni possibili. Ma la realtà è che le soluzioni DLP non sono tutte uguali. L'obiettivo di questo libro è aiutarti a distinguere i fatti dagli stratagemmi promozionali, analizzando le caratteristiche e funzionalità più importanti dei vari sistemi.

Quindi, facciamo un passo indietro per iniziare a sfatare alcuni dei miti più comuni sulla protezione dei dati basata su cloud: così potrai prendere decisioni informate e individuare la soluzione più adatta.

Mito: le soluzioni DLP più recenti sono anche le migliori

Realtà: quando è il momento di scegliere un programma di sicurezza dei dati, meglio non lasciare nulla al caso. Non solo servono funzioni sufficienti per garantire la sicurezza, ma bisogna anche poter contare su un fornitore specializzato e con esperienza comprovata in sistemi DLP. Le soluzioni tradizionali possono anche non essere state progettate per la tecnologia cloud, ma in fatto di maturità hanno tanto da insegnare alla maggior parte delle soluzioni DLP cloud-based.

La soluzione più affidabile sul mercato ha attraversato un lungo periodo di maturazione in cui ha sviluppato tutta una serie di nuove funzioni. Per investire in un programma completo di sicurezza dei dati e massimizzare la sicurezza, è meglio scegliere un fornitore capace di soddisfare ogni possibile esigenza, dal supporto di ambienti cloud al livello di maturità delle caratteristiche. Novità non è sempre sinonimo di efficacia.

Mito: le soluzioni DLP tradizionali erano inaccurate

Realtà: le soluzioni DLP tradizionali sono state messe a punto da aziende che hanno passato più di dieci anni a sviluppare algoritmi e parametri accurati per individuare e impedire il trasferimento non autorizzato di informazioni sensibili.

Il problema non è l'accuratezza ma il numero di falsi positivi, come abbiamo spiegato nelle pagine precedenti. I falsi positivi portano a situazioni pericolose, in cui le vere minacce passano inosservate e i dati sensibili vengono divulgati accidentalmente, mentre il personale mira a bypassare i controlli di sicurezza più approfonditi. Ma un'altra conseguenza è la crescita smisurata (con tutti i costi annessi) dei team di incident response che devono far fronte a un volume di incidenti sempre più ingestibile. Nel Capitolo 2 vedremo perché i sistemi DLP devono essere precisi e accurati per mantenere la fiducia.

Mito: l'uso dell'IA generativa non può essere protetto dalle attuali soluzioni di sicurezza dei dati

Realtà: la crescita rapida dell'IA generativa (GenAI), anche se è una novità recente, ha costretto le aziende a dare la priorità alla sicurezza dei dati sensibili, il che è fondamentale per potenziare la forza lavoro senza compromettere la sicurezza. Basandosi sulle esperienze passate, molti responsabili della sicurezza hanno previsto la necessità di integrare un'altra soluzione di sicurezza nell'infrastruttura di sicurezza esistente, spesso disgiunta.

Tuttavia, le soluzioni di sicurezza dei dati all'avanguardia dal punto di vista tecnologico e in grado di adattarsi alle tendenze emergenti devono essere in grado anche di soddisfare i requisiti di sicurezza specifici dell'IA generativa. Ciò include la compatibilità con varie iterazioni di IA generativa come ChatGPT, DeepSeek, Google Gemini, Microsoft Copilot e altre. In questo panorama in continua evoluzione, è fondamentale selezionare un fornitore in grado di rispondere in modo attivo alle tue esigenze mutevoli.

Mito: le soluzioni DLP cloud-based hanno capacità limitate rispetto ai sistemi tradizionali

Realtà: al momento, molti sistemi DLP basati su cloud usano meno di 100 identificativi di dati (v. Capitolo 2) e sono in grado di riconoscere solo alcuni tipi di file. In altre parole, hanno capacità di rilevazione estremamente limitate. La ragione va ricercata nella scarsa maturità della tecnologia. A differenza dei sistemi DLP in uso da una decina di anni, queste soluzioni sono state create per concentrarsi su determinati casi d'uso, come applicazioni cloud specifiche, e proteggere una gamma limitata di tipi di file più diffusi. Un raggio d'azione tanto

ristretto implica che i sistemi cloud-based non possono offrire il livello di precisione necessario per garantire un equilibrio ideale tra protezione dei dati ed esigenze aziendali, il che produce un conflitto costante tra le due sfere. La tecnologia DLP erogata sul cloud deve essere superiore ai sistemi DLP tradizionali, grazie alla sua notevole scalabilità. Ed è logico dare per scontato che una maggiore scalabilità permette di gestire efficacemente i falsi positivi e migliorare l'accuratezza.

ATTENZIONE

Quando si tratta di sicurezza dei dati, è l'esperienza che conta. Anche se a prima vista le ultimissime novità possono sembrare interessanti, le soluzioni DLP mature, specialmente se integrate con il DSPM, sono in grado di offrire un livello di sicurezza maggiore proprio perché hanno potuto crescere e perfezionarsi nel tempo. Meglio scegliere un provider dall'esperienza comprovata e testare personalmente sistemi diversi per ottenere il livello di protezione adeguato.

Mito: un insieme di sistemi di sicurezza dei dati è efficace quanto una soluzione di sicurezza dei dati unificata

Realtà: quando si tratta di sicurezza dei dati, può sembrare logico raggruppare una varietà di prodotti e servizi DLP di fornitori diversi. Dopo tutto, non è così raro che applicazioni SaaS, servizi di cloud pubblici, firewall e soluzioni SWG siano venduti con tanto di servizi DLP già in dotazione. Ma prima o poi, questi programmi di sicurezza dei dati che includono più servizi non basteranno più. L'uso di una suite di sistemi diversi non sviluppati come una soluzione integrata rischia di offrire scarsi vantaggi in termini di visibilità sui rischi e sul contesto degli incidenti. Inoltre, gli addetti alla sicurezza dei dati saranno costretti a fare i conti con più console e policy di sicurezza scoordinate. Anzi, l'ambito di applicazione di ciascun servizio DLP è spesso limitato ad ambienti e canali specifici, coprendo ad esempio solo il traffico web o determinati punti di controllo, come una o alcune applicazioni SaaS. Tutto questo significa lasciare che i dati restino vulnerabili a eventuali attacchi.

Per tutelare efficacemente l'azienda, è bene puntare su una soluzione integrata che offra una sicurezza dei dati completa, in grado di coprire tutte le potenziali aree di rischio su servizi cloud, sistemi locali, servizi di posta elettronica ed endpoint, per ottenere una copertura completa su molti tipi di dati e di controlli.

IN QUESTO CAPITOLO

- **Individuare le sfide che devono essere affrontate dalle soluzioni DLP tradizionali**
- **Prepararsi a scalare le soluzioni in vista di una crescita o di cambiamenti**
- **Conoscere le realtà e le limitazioni dei sistemi DLP in cloud**
- **Comprendere come i sistemi DSPM e DLP rendono più efficaci altri strumenti di sicurezza**

Capitolo 2
Una protezione completa per le aziende basate sul cloud

Perché è importante che i sistemi di sicurezza proteggano tutta l'azienda, incluse le applicazioni cloud? Perché la perdita di dati o l'accesso non autorizzato alle informazioni può avere gravi conseguenze sull'azienda e sui suoi portatori di interessi. Può sembrare scontato ma, nella pratica, molte forze giocano contro.

Questo capitolo spiega perché ottenere una protezione completa dei dati in tutta l'azienda porta risultati nell'immediato e vantaggi strategici nel lungo periodo.

Le difficoltà associate all'evoluzione dei sistemi DLP

Come visto nel Capitolo 1, i sistemi DLP (*Data Loss Prevention*) erano soprattutto concentrati sulla protezione dei dati archiviati *all'interno* dei data center aziendali. Tuttavia, l'azienda moderna non è più limitata a una sede fisica. L'azienda ora include i numerosi endpoint usati

dai dipendenti per connettersi alle risorse interne, nonché le migliaia di app cloud approvate (o anche no) che possono essere usate in azienda (vedere la Fig. 2-1).

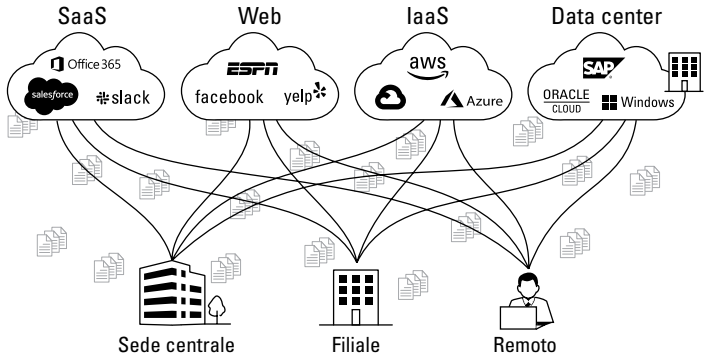

FIGURA 2-1: Nelle moderne aziende altamente distribuite, i dati risiedono e confluiscono su molti ambienti nuovi.

È importante proteggere i dati ovunque possono essere trasmessi, cioè in ambienti cloud, su dispositivi mobili, sulla rete aziendale o in posizioni esterne. Questo significa che i sistemi DLP tradizionali, sviluppati per proteggere i dati dentro l'azienda, non sono più sufficienti.

RICORDA

Anche se rimane fondamentale identificare tutte le posizioni in cui vengono trasferiti e archiviati i dati, puntando l'attenzione sui dati stessi piuttosto che sugli ambienti in cui vengono generati e mantenuti, è possibile ottenere grossi vantaggi in termini di flessibilità ed efficacia. Lo si potrebbe paragonare a una squadra di calcio che passa da una difesa a zona a una difesa a uomo. Adottando un approccio completo è possibile proteggere le informazioni sensibili.

Qualsiasi soluzione per rimpiazzare un sistema DLP tradizionale dove fornire all'azienda una copertura completa sia dei canali cloud che di quelli tradizionali on-premise. Anche le soluzioni DLP più moderne erogate su cloud sono progettate per coprire solo canali specifici (come una rete o un dato gruppo di endpoint o applicazioni), senza essere applicabili a tutti i casi d'uso attuali.

Per fornire una protezione aziendale completa, la soluzione DLP deve proteggere tutti i trasferimenti di dati, strutturati o meno, da e verso qualsiasi posizione e dispositivo. Ciò comprende i dispositivi gestiti e non gestiti usati dagli utenti, sia all'interno che all'esterno della rete aziendale, oltre alle applicazioni SaaS, IaaS, alla posta elettronica, alle

app private e agli endpoint. Questo approccio richiede una soluzione DLP completa e flessibile, in grado di adattarsi di continuo alle esigenze mutevoli delle aziende altamente distribuite.

Nel seguito, esaminiamo gli aspetti chiave da considerare nella progettazione di una soluzione DLP per le moderne aziende senza confini tangibili.

Scalabilità e caratteristiche a prova di futuro

Fino a non molto tempo fa, le applicazioni SaaS nelle aziende erano relativamente limitate, ma nel tempo la diffusione di questi strumenti è cresciuta in modo sostanziale. Oggi un'azienda può avere centinaia di applicazioni SaaS approvate, e i suoi dipendenti avvalersi di migliaia di app aggiuntive di cui l'azienda non è neppure a conoscenza (il che è spaventoso).

SUGGERIMENTO

Scalabilità non significa solo adeguarsi alle esigenze attuali ma anche prepararsi alla crescita e ai cambiamenti futuri. Un approccio orientato al futuro è essenziale per creare soluzioni flessibili e agili, in grado di gestire la continua espansione dei carichi di lavoro o delle attività senza compromettere le prestazioni o le funzioni. La scalabilità aiuta ad assicurare la continua efficacia ed efficienza dei sistemi a fronte di cambiamenti imprevedibili.

Ma la scalabilità non ha a che fare solo con la gestione dei nuovi ambienti o con la protezione delle nuove destinazioni dei dati. Si riferisce anche al gestire la rapidità, la varietà e il volume delle informazioni – tutti fattori in continuo aumento. La quantità dei dati generati e raccolti oggi è senza precedenti. Con la diffusione degli strumenti online collaborativi, i dati possono essere contenuti in conversazioni su app come Microsoft Teams, Slack e Zoom, o di posta elettronica in cloud come Gmail. Possono anche essere sotto forma di immagini, fotografie e screenshot: la cattura di informazioni importanti viene usata al pari del comune copia/incolla in un documento. Scalabilità significa proteggere i diversi formati di dati e tutti i casi d'uso, compresi quelli non ancora sviluppati.

RICORDA

Il paragrafo "La sicurezza dei dati unificata DLP in azione", più avanti in questo capitolo, spiega nel dettaglio come funzionano i sistemi DLP. Per ora, teniamo a mente che la funzionalità di base di un sistema DLP consiste nel rilevare i dati sensibili e prevenire fughe all'esterno.

L'evoluzione del sistema DLP: da eroe a bambino difficile

Con l'adozione delle applicazioni cloud da parte delle aziende e l'espansione in nuove sedi, l'implementazione dei sistemi DLP tradizionali è diventata sempre più difficile da gestire. Questi sistemi erano progettati per essere installati e gestiti localmente, il che ne rendeva necessaria la duplicazione e l'installazione in ogni nuova sede e filiale. Tutto questo aggiunge un notevole livello di complessità e richiede molte risorse, in termini di apparecchiature hardware, manutenzione e personale specializzato. La progressiva diffusione dello smart-working ha complicato ancora di più la situazione, con i dipendenti che hanno iniziato ad accedere ai dati sensibili da una serie di dispositivi e luoghi diversi. Tutto ciò ha reso difficile per le aziende gestire in modo efficace i sistemi DLP, con un conseguente aumento dei costi e dei potenziali rischi per la sicurezza.

Hai mai evitato l'aggiornamento del telefono o del PC portatile per evitare problemi fastidiosi se non l'interruzione di una delle tue app preferite? Applica questo approccio a migliaia di casi e immagina di dover aggiornare il software DLP tradizionale su numerosi server e filiali, oltre che su migliaia di dispositivi dei dipendenti. Non c'è da meravigliarsi se alcuni clienti continuano a usare le vecchie versioni del loro software DLP: richiede molto meno sforzo rispetto ai tentativi di aggiornarlo.

ATTENZIONE

Saltare gli aggiornamenti periodici mette in pericolo i dati e aumenta il rischio di avere problemi di compliance e violazioni dei dati.

La soluzione DLP deve lavorare meglio, non di più

I sistemi DLP tradizionali analizzano tutti i tipi di dati e identificano le informazioni sensibili. L'idea è proteggere solo i dati sensibili, perché proteggere anche quelli non sensibili può avere effetti negativi sulla produttività. Ad esempio, anche se è importante non condividere certi dati sensibili con terzi via e-mail, non serve proteggere e possibilmente ritardare uno scambio e-mail perché può ostacolare la comunicazione e la collazione, e generare troppi allarmi per il team di incident response. Inoltre, i dipendenti possono essere autorizzati a usare risorse aziendali anche per attività non collegate al lavoro (ad es. pubblicare foto sui social), purché i contenuti non siano sensibili e non contengano segreti aziendali. Poiché i sistemi DLP tradizionali sono fatti di componenti hardware e software, usarli per scansionare

tutto il traffico web e tutti i repository e per cercare tutte le categorie di dati sensibili richiede server e moduli aggiuntivi, oltre a database più grandi.

E visto che queste soluzioni, per loro natura, devono essere attivate on-premise, i sistemi DLP tradizionali si affidano a risorse di elaborazione hardware necessariamente limitate. Ad esempio, i software DLP di endpoint installati sui computer dei dipendenti hanno capacità limitate di rilevare i dati, perché sfruttano motori di base con un più basso uso di risorse. Questo significa che, anche se le soluzioni tradizionali possono individuare alcune categorie di dati sensibili sugli endpoint, il fatto di non poter usare metodi di rilevamento avanzati può tradursi nella mancata identificazione di grosse quantità di informazioni. I sistemi DLP tradizionali, ad esempio, non possono usare tecnologie avanzate che richiedono considerevoli risorse di elaborazione, come il ML (*Machine Learning*) e l'EDM (*Exact Data Matching*, v. la prossima sezione). Le soluzioni DLP di nuova generazione scaricano sul cloud le attività ad alto dispendio di risorse, pur continuando ad applicare le protezioni a livello degli endpoint. La scalabilità di questo approccio è un enorme passo avanti perché permette al sistema di individuare dati come nomi propri, codici fiscali e altre informazioni sensibili associate alle persone.


RICORDA

Il cloud può fornire la scalabilità infinita, necessaria per massimizzare l'efficacia delle capacità di rilevamento. In questo modo, i sistemi DLP possono concentrarsi solo sui dati più importanti e proteggerli da accessi non autorizzati.

Bisogno di precisione

Un luogo comune molto diffuso è l'inaccuratezza dei sistemi DLP tradizionali (v. Capitolo 1). Ma non è questo il problema vero, o per lo meno non è quello principale. Il problema principale sono i falsi positivi (anche questi già visti nel Capitolo 1), dovuti soprattutto all'assenza di contesto granulare. Ovviamente, con l'espansione inarrestabile in una serie di dispositivi e applicazioni al di fuori del perimetro aziendale, e con i dati sensibili che diventano sempre più difficili da rilevare a causa del proliferare incontrollato delle loro categorie, i sistemi DLP tradizionali non riescono a tenere il passo ed è naturale che l'accuratezza non sia più la stessa di prima. Il problema vero, però, è che le soluzioni DLP tradizionali tendono a essere troppo restrittive, segnalando azioni legittime come violazioni, e persino bloccandole, senza capire il contesto di business o il livello di rischio.

In un mondo in cui la collaborazione è diventata fondamentale per lavorare, un numero così eccessivo di falsi positivi causa troppe interruzioni.

La soluzione DLP non deve introdurre problemi per l'azienda né interrompere il flusso di dati necessario per le normali attività di lavoro. Ad esempio, se un dipendente vuole mandare un file a un consulente esterno fidato che collabora a un progetto, è meglio se il sistema DLP non blocca il trasferimento. In un mondo ideale, la soluzione dovrebbe aumentare l'efficacia del team di incident response aiutando gli esperti a riconoscere più facilmente gli incidenti veri e propri e filtrando i falsi positivi.

Quindi, possiamo dire che precisione e accuratezza non erano i problemi principali dei sistemi DLP tradizionali, ma lo sono per le soluzioni su cloud meno mature. Due sono i fattori che tendono a influire sull'accuratezza e la precisione di questi sistemi:

- Se le funzioni di rilevamento sono inaccurate possono portare a individuare e proteggere troppi dati non sensibili, con il rischio di compromettere comunicazioni aziendali legittime.
- L'assenza di metodi per individuare i dati sensibili, ovvero l'incapacità di individuarli, può fare sì che alcuni formati di file o tipi di dati (ad esempio, immagini o formati compressi) o determinate informazioni (ad es. numeri di passaporto, informazioni sanitarie, coordinate bancarie o carte d'identità nazionali) non vengano rilevate.

RICORDA

Per mantenere la fiducia, i sistemi DLP devono essere accurati e precisi, individuando esclusivamente i dati sensibili, segnalando e bloccando solo i trasferimenti realmente dannosi senza generare troppi falsi positivi. Un tale sistema richiede diversi elementi chiave, come descritto nel seguito.

Individuazione e classificazione

Le funzioni complete di scoperta e classificazione dei dati in un prodotto DPSM (*Data Security Posture Management*) affidabile consentono di individuare, etichettare e scansionare continuamente fonti di dati strutturati e non strutturati in ambienti on-premises, cloud e ibridi, fornendo visibilità completa sui dati sensibili e una classificazione automatizzata a supporto della conformità normativa.

Individuazione e classificazione hanno inoltre un ruolo fondamentale nel minimizzare i falsi positivi.

Identificativi di dati

Gli *identificativi di dati* servono a trovare informazioni sensibili come codici fiscali o numeri di carte di credito sulla base di contenuti con descrizioni generiche, tra cui le espressioni regolari (note come *regex*); si tratta di uno strumento utile che aiuta i sistemi DLP a riconoscere automaticamente tipi di dati specifici che usano espressioni e pattern naturali e di uso comune, come "cerca un'espressione alfanumerica di sedici caratteri". Una possibile risposta è che la stringa corrisponde a un codice fiscale, ma come averne la certezza?

Gli identificativi di dati cercano la risposta applicando regole speciali basate sul numero di cifre, modelli di testo, sequenze, caratteri di separazione e parole chiave di prossimità (come codice fiscale [CF], password [PW] e via dicendo) per riconoscere questi codici e tenerli al sicuro.

SUGGERIMENTO

Seguono alcuni punti importanti da tenere a mente:

- Per garantire la sicurezza delle informazioni e la conformità ai requisiti normativi, servono migliaia di identificativi di dati predefiniti e la capacità di crearli o personalizzarli in base a esigenze specifiche. Questa capacità è essenziale perché ogni azienda potrebbe aver bisogno di proteggere diversi tipi di dati sensibili.
- Gli identificativi di dati devono supportare migliaia di tipi di file (DOC, XLS, JPG, PNG, PDF, CSV, ZIP, RAR ecc.), formati e categorie (immagini, file numerici, archivi e cartelle compresse, fogli di calcolo, file audio/video, database ecc.) (v. Capitolo 1).
- È fondamentale avere supporto per un'ampia serie di numeri identificativi specifici per Paese (tra cui coordinate bancarie internazionali, indirizzi, codici postali, carte d'identità nazionali, numeri di passaporto e prefissi telefonici) e di profili normativi e di compliance alla privacy per assicurarsi che la soluzione DLP tenga il passo con le normative più recenti.

SUGGERIMENTO

Per avere un sistema DLP davvero efficace, servono migliaia di identificativi di dati. Questo permette di individuare e segnalare con precisione informazioni potenzialmente sensibili, a prescindere dallo stato, dalla regione e dal Paese in cui si trovano.

Corrispondenza esatta dei dati (EDM - *Exact Data Matching*)

L'EDM è un modo per trovare specifiche informazioni strutturate a partire da fonti come fogli di calcolo e database. Consente a una soluzione DLP di riconoscere e indicizzare dati riservati correlati a clienti e dipendenti che possono essere usati per identificare un determinato utente attraverso il suo nome e cognome, il codice fiscale, l'indirizzo e altri codici. Può essere usato anche per trovare informazioni finanziare che identificano il patrimonio di un individuo, come numeri di carte di credito o di conti correnti, o addirittura per le informazioni sanitarie e i database di identificazione dei prodotti e del relativo prezzo. Con l'EDM, una soluzione DLP può indicizzare queste informazioni e individuarle ovunque. Per funzionare in modo efficiente e accurato, l'EDM deve poter trovare corrispondenze tra le varie informazioni indicizzate e combinare campi dati relativi a un determinato record. Inoltre, deve essere in grado di indicizzare miliardi di record per supportare le aziende in crescita, i relativi database in perenne espansione e i sempre più crescenti volumi di informazioni. La scala di elaborazione, quindi, è essenziale.

Capacità avanzate di rilevamento dei dati

Con la crescita esponenziale dei tipi di dati e dei modi per trasferirli, le aziende devono poter contare su sistemi DLP in grado di rilevare con precisione le informazioni sensibili. *Capacità di rilevamento avanzate* è un termine generale che comprende elementi come:

- **Riconoscimento delle immagini basato su funzioni OCR e di Intelligenza Artificiale (IA):** Queste funzioni stanno diventando sempre più importanti per la sicurezza dei dati. Oggi, gli utenti scattano facilmente fotografie di documenti, moduli, carte d'identità, lavagne e di altreimmagini. Ad esempio, è normale catturare screenshot o immagini di informazioni per condividerle con i colleghi. Grazie alle capacità OCR, una soluzione DLP può estrarre il testo da un'immagine per poi applicare la classificazione dei dati sulla base delle policy di rilevamento.
- **IA e ML:** La classificazione delle immagini tramite IA e ML, grazie a sofisticati metodi di rilevamento, è in grado di riconoscere i tipi di file e documenti più comuni (come carte di credito, moduli fiscali, accordi di non divulgazione, moduli per fusioni e

acquisizioni e brevetti), senza necessariamente estrarne il contenuto. Questi metodi riescono a rilevare contenuti sfocati, spiegazzati e danneggiati, anche se sono difficili da leggere. Gli algoritmi, infatti, sono stati "addestrati" per identificare pattern e caratteristiche specifiche di ogni tipo di documento, come l'impaginazione, i caratteri e i colori. Inoltre, possono tenere conto del contesto in cui viene usato il documento. Tutto ciò permette all'IA di classificare il documento con precisione, anche in condizioni difficili (ad es., immagini di scarsa qualità o documenti danneggiati.

- **Fingerprint di file e documenti:** Si tratta di una tecnica essenziale che permette alle aziende di garantire la sicurezza e la riservatezza dei documenti critici e dei file altamente sensibili. Le aziende, indicizzando l'intero documento e rilevando copie esatte o parziali dei contenuti, possono impedire l'esfiltrazione e la duplicazione non autorizzate di informazioni riservate (come documenti di fusioni e acquisizioni, informazioni preliminari, progetti tecnici o dati relativi agli investitori). Questa tecnica è utile soprattutto per rilevare copie di file sensibili in ambienti e canali di trasmissione a rischio, come le e-mail in uscita e i caricamenti su istanze personali di applicazioni.

Le soluzioni DLP tradizionali hanno effettivamente fornito delle risposte in passato, quando la protezione veniva applicata solo on-premise, ma oggi non riescono più a tenere il passo. Semplicemente, non hanno abbastanza scalabilità o potenza di elaborazione.

Tanto contesto e un modello di protezione dei dati Zero Trust

Utenti, reti, dati, applicazioni e regole di governance di un'azienda sono in continuo movimento, proprio come le onde dell'oceano. Per tenere il passo con i potenziali rischi che ciò comporta, il sistema DLP e la relativa strategia di protezione devono essere in grado di adattarsi e rispondere con rapidità ed efficienza ai continui cambiamenti che interessano il panorama dei dati. Questa agilità (nota come *Comprensione del contesto*) consente di proteggere efficacemente i dati sensibili, minimizzare i rischi di violazione dei dati e garantire la conformità alle normative senza impatti negativi sulla produttività degli utenti o sulla continuità delle attività aziendali.

Per ottenere una tale flessibilità, una piattaforma di protezione in cloud deve essere integrata con la più ampia infrastruttura di sicurezza e gestione delle reti dell'azienda. Deve anche raccogliere costantemente informazioni da fonti diverse, come gestione delle identità, analisi dei comportamenti, log di rete, strumenti di sicurezza cloud, analisi delle minacce, sicurezza di rete, posture di sicurezza di ambienti SaaS e cloud, CASB, indici di fiducia nativi in cloud e posture di sicurezza degli endpoint. Queste informazioni sui rischi e sulla sicurezza consentono alla piattaforma di impostare livelli di accesso adeguati e di applicare le giuste policy di sicurezza dei dati, valutando aspetti quali l'identità della persona, la sua posizione, le sue attività, il livello di sicurezza del suo dispositivo, l'affidabilità della rete, la reputazione dell'app usata, la destinazione dei dati trasferiti e altro ancora.

SUGGERIMENTO

Essendo consapevole dei rischi e del contesto, una piattaforma di protezione dei dati può adeguarsi continuamente e fornire un alto livello di efficacia e precisione delle attività di incident response.

Il Capitolo 3 spiega il concetto di Zero Trust e il suo ruolo centrale in una soluzione DLP efficace. Per ora, basta ricordare che la filosofia Zero Trust è un'essenziale strategia di sicurezza basata sul presupposto che tutti gli utenti, i dispositivi e le reti nell'ambiente aziendale sono potenzialmente dannosi e devono essere trattati con sospetto in ogni circostanza.

Zero Trust significa che tutti gli accessi alle risorse e ai sistemi sono sottoposti a verifiche e controlli rigorosi, indipendentemente da dove si trova l'utente o il dispositivo, dentro o fuori il perimetro di rete. Il contesto è il motore di una strategia Zero Trust perché consente al sistema DLP di fare scelte informate su quando autorizzare o meno le attività legate ai dati.

RICORDA

Lavorare con soluzioni di sicurezza integrate, abbinate a tecnologie di protezione dei dati, è quello che fa la differenza tra uno *strumento* e una vera e propria *piattaforma* di protezione dei dati.

La sicurezza dei dati unificata in azione

La piattaforma DLP è il cuore dell'architettura di sicurezza informatica di un'azienda, e aiuta ad aumentare l'efficacia di altri strumenti di protezione. Essa svolge numerose funzioni critiche, come ad esempio:

- **Identificazione e monitoraggio dei dati sensibili ovunque si trovino e vengano trasferiti, quali:**
  - *Dati in movimento*, vale a dire i dati che confluiscono su Internet, reti, applicazioni e dispositivi (come upload e download).
  - *Dati a riposo*, vale a dire le informazioni archiviate. Possono essere i dati salvati in applicazioni personali o SaaS aziendali, come nel caso delle informazioni dei clienti salvate in Salesforce o di documenti a uso interno archiviati e condivisi su Microsoft OneDrive o Microsoft SharePoint.
  - *Dati in uso*, ovvero i dati in corso di consultazione, elaborazione o manipolazione: trasferimento su USB, stampa, comunicazione tramite e-mail o invio via fax. (esistono ancora i fax?!).
- **Monitoraggio dell'ambiente dei dati per rilevare chi accede alle informazioni e come le usa:** Monitorando le azioni, il sistema può individuare gli incidenti che violano le policy aziendali (come la condivisione non autorizzata di informazioni riservate) e attuare misure correttive. Questo aiuta a impedire l'accesso o l'uso di dati sensibili senza i giusti privilegi (dipendente vs persona esterna / dispositivo aziendale vs dispositivo personale) o senza la dovuta autorizzazione o moderazione (come nel caso di sospetti download massivi di grandi quantità di file) e assicura l'identificazione e la tempestiva correzione delle potenziali violazioni alla sicurezza.
- **Intervento automatico mirato all'attuazione delle policy, ad esempio bloccando un flusso di dati, crittografandoli, mettendo in quarantena le informazioni riservate o annullando la condivisione su un'applicazione SaaS:** Se un dipendente usa OneDrive per condividere (lecitamente o meno) con utenti esterni un file che contiene delle informazioni riservate, la piattaforma DLP può bloccare automaticamente la condivisione.
- **Formazione degli utenti visualizzando automaticamente notifiche sulle violazioni e spiegando perché una determinata azione è un comportamento a rischio, promuovendo al tempo stesso prassi sicure per la gestione dei dati:** Le notifiche permettono anche di educare immediatamente gli utenti sulle policy di sicurezza, riducendo il bisogno di valutazione manuale da parte del team di incident response. Inoltre, una soluzione DLP moderna deve avvisare gli utenti immediatamente e trasmettere le notifiche anche al manager e ai team HR e di sicurezza informatica, a seconda delle esigenze.

È ora di cambiare la soluzione DLP

I sistemi DLP tradizionali sono stati un'efficace soluzione di sicurezza per anni, e non stupisce che molti specialisti ne siano ancora dei ferventi sostenitori. Dopotutto, come già detto, nell'ultimo decennio queste soluzioni sono state sviluppate in modo intensivo per proteggere le reti on-premise dalle minacce dell'era pre-cloud.

I fornitori di sistemi DLP tradizionali hanno tentato di colmare il divario tra le proprie piattaforme e i moderni requisiti delle aziende cloud-first usando tecnologie come SWG (Secure Web Gateway) e CASB, e integrazioni con protocollo ICAP (Internet Content Adaptation Protocol).

ATTENZIONE

Purtroppo, la maggior parte dei sistemi DLP tradizionali non è progettata per gestire i casi d'uso tipici del cloud e del lavoro ibrido, i quali richiedono capacità e integrazioni con servizi cloud che i sistemi DLP tradizionali non supportano nativamente. Questo può causare problemi di compatibilità e scarse prestazioni.

Tutte queste limitazioni, con le altre affrontate nel Capitolo 1, hanno compromesso la popolarità delle soluzioni DLP tradizionali, spingendo molte aziende a cercare alternative. Ora che i dati vengono trasferiti sempre più sul cloud, aumenta la necessità di sistemi DLP in cloud capaci di riconoscere i cambiamenti a livello di contesto e rischio in relazione alla gestione dei dati. Questi sistemi devono essere facili da distribuire, ampliare e scalare, oltre ad avere la capacità di coprire casi d'uso tradizionali e moderni. Essendo erogati in cloud, sono anche sempre aggiornati, il che garantisce una protezione migliore anche con l'evolversi dei rischi e del contesto.

IN QUESTO CAPITOLO

- **Vedere come le vecchie soluzioni di protezione dei dati possono compromettere le attività aziendali**
- **Scoprire i tipi di contesto dei dati e assicurare la continuità del business**
- **Adattarsi a condizioni di rischio mutevoli per proteggere i dati**
- **Garantire l'esecuzione in sicurezza dei moderni casi d'uso aziendali**
- **Valutare il contesto aziendale, il rischio e i comportamenti degli utenti per ottimizzare la protezione dei dati in futuro**

Capitolo 3
Il ruolo dello Zero Trust nella sicurezza dei dati unificata

Un concetto chiave nel campo della sicurezza, DLP (*Data Loss Prevention*) o meno, è il cosiddetto approccio Zero Trust. Una strategia Zero Trust parte dal presupposto che tutti gli utenti e i dispositivi, anche quelli all'interno della rete aziendale, sono potenzialmente dannosi e, quindi, non affidabili. Questo vuol dire che l'accesso a dati e sistemi sensibili non viene autorizzato automaticamente sulla base dell'identificazione personale e dell'appartenenza all'azienda. L'utente può accedere solo dopo un'autenticazione attenta, il controllo della postura di sicurezza e la valutazione del contesto di rischio (monitorato su base continuativa). La filosofia Zero Trust non deve ostacolare la produttività, ma consentire un uso sicuro dei dati sensibili e supportare i moderni processi di business secondo un approccio incentrato sulla sicurezza, capace di adattarsi automaticamente a condizioni di rischio mutevoli.

Questo approccio rivaluta continuamente l'affidabilità di ogni individuo, dispositivo e contesto operativo prima di permettere l'accesso ai dati sensibili o di usarli in qualche modo. Anche un dipendente già autorizzato deve comunque essere valutato accuratamente (verifica dell'identità, controllo del dispositivo e connessione di rete, un esame dei rischi correlati alle applicazioni a cui tenta di accedere e il monitoraggio del suo comportamento per verificare che sia *ancora* affidabile). Se l'utente si comporta in modo sospetto o non prudente, ad esempio condividendo troppi dati, il sistema potrebbe intervenire decidendo di limitare i suoi privilegi o altro. Questo aiuta a proteggere i dati sensibili da potenziali rischi di perdita e garantisce l'accesso e la condivisione solo a utenti fidati.

Questo capitolo approfondisce i vantaggi dell'approccio Zero Trust e il suo ruolo chiave in un ambiente di sicurezza dei dati unificata.

I rischi associati ai sistemi di sicurezza obsoleti

I sistemi DLP erano stati creati proprio per impedire la fuga di informazioni sensibili dall'azienda. Le versioni tradizionali gestiscono un numero limitato di scenari; il loro scopo principale è individuare i dati sensibili e tenerli all'interno dell'azienda, tramite un approccio basato sul perimetro che controlla il flusso di dati in entrata e in uscita dalla rete aziendale.

Basandosi su una strategia di *sicurezza implicita*, queste si limitano a riconoscere e reagire a una serie predefinita di violazioni di dati. Ma questo approccio non dispone di informazioni di contesto sugli utenti e sulle loro motivazioni commerciali, tantomeno sui rischi associati a una determinata azione.

Ad esempio, un sistema DLP tradizionale può identificare tutti i numeri di previdenza sociale e bloccare qualsiasi tentativo di inviarne uno all'esterno del perimetro aziendale. In altri casi, può impedire che i dati sensibili vengano caricati su un'applicazione SaaS (*Software-as-a-Service*) senza saper distinguere un'istanza aziendale di un'app SaaS approvata, come Microsoft Teams, da un'istanza personale della stessa app. Questo approccio può sembrare sicuro ma in realtà è piuttosto rigido e non dispone di informazioni su utenti, dispositivi, reti, applicazioni e destinazioni dei dati per poter stabilire se un'attività è autorizzata o meno. La fiducia implicita è un concetto che inibisce le comunicazioni aperte e il libero flusso di dati, condizioni necessarie per la crescita di un'azienda moderna.

ATTENZIONE

Un sistema DLP tradizionale, non potendo valutare continuamente il contesto e il rischio aziendale, non è in grado di prendere decisioni informate sulla protezione dei dati e può interrompere inutilmente le operazioni aziendali.

Con policy non particolarmente rigorose, la fiducia implicita autorizza l'accesso ai dati sensibili senza verificare su base continua l'identità e l'affidabilità dell'utente o del dispositivo. Ciò lascia l'azienda esposta a potenziali usi impropri dei dati sensibili, che una volta usciti dal perimetro aziendale non possono più essere protetti dai meccanismi di sicurezza.

Questo è un problema serio nell'era del cloud. I dati sensibili vengono usati e condivisi al di fuori dell'azienda anche per le attività più basilari. Ad esempio, applicazioni e servizi cloud comuni come Dropbox e Google Drive consentono ai dipendenti di accedere, condividere e collaborare usando dati sensibili dentro e fuori i confini aziendali. Ma i sistemi DLP tradizionali che si basano sulla fiducia implicita rischiano di ostacolare collaborazioni legittime o di far trapelare i dati all'esterno, rendendoli vulnerabili a potenziali minacce.

Un sistema di protezione Zero Trust permette di usare e condividere dati sensibili a patto che le condizioni di sicurezza siano continuamente verificate. In più, rende possibile far fluire e condividere i dati sensibili tra utenti e dispositivi, e archiviarli in diversi servizi cloud grazie alla continua verifica delle condizioni come l'identità dell'utente, la sicurezza del dispositivo, della rete e dell'applicazione e il comportamento dell'utente nel tempo. La protezione offerta dalla filosofia Zero Trust si applica nello specifico ai dati sensibili e garantisce che tutte le condizioni di sicurezza siano sempre soddisfatte, agevolando il lavoro ibrido, il cloud e i moderni casi d'uso aziendali.

RICORDA

Un moderno sistema di sicurezza dei dati unificata erogato sul cloud e basato sui principi Zero Trust monitora e controlla i dati da qualsiasi posizione usata per connettersi e accedere alle informazioni, e ovunque tali dati vengono archiviati e trasferiti (nei repository delle applicazioni cloud nonché negli ambienti on-premise).

Un altro problema degli approcci tradizionali basati su più prodotti e sulla fiducia implicita è che sono molto isolati e applicano un solo controllo di sicurezza alla volta senza un intervento integrato e senza condividere le informazioni sui rischi. Questo significa che i diversi controlli non agiscono in una piattaforma coesa, creando così delle lacune nella strategia di sicurezza complessiva. Per una protezione completa dei dati, servono molti controlli di sicurezza che lavorano insieme e condividono le informazioni.

La filosofia Zero Trust adotta un approccio più olistico e dinamico per la protezione dei dati, considerando il contesto dell'utente, del dispositivo, della rete e di altri fattori, per prendere decisioni più informate sulla protezione. Questo approccio supporta l'integrazione del sistema DLP con altri controlli di sicurezza e strumenti di produttività, e può monitorare e adattarsi continuamente all'evoluzione delle minacce, dei rischi e delle condizioni aziendali.

In generale, le aziende che usano sistemi DLP basati sulla fiducia implicita devono partire dal falso presupposto che i loro utenti interni siano affidabili e attenti alla sicurezza, e non mettano mai a repentaglio i dati sensibili. Ma proprio a causa della mancanza di un contesto di sicurezza, se si applicano rigidamente le policy DLP, spesso si ostacolano i processi aziendali legittimi. Al contrario, una soluzione DLP con filosofia Zero Trust monitora e controlla da vicino come vengono usati i dati, per impedire in modo adattivo le violazioni alle policy.

Ad esempio, un sistema DLP basato sulla fiducia implicita può proteggere il numero di una carta di credito consentendo l'accesso solo agli utenti autorizzati; ma questo implica dare per scontato che gli utenti sappiano sempre gestire i dati in modo sicuro.

A differenza dei sistemi DLP tradizionali basati sulla fiducia implicita, un sistema DLP basato sui principi Zero Trust non parte da alcun presupposto, ma protegge i dati sensibili, ad esempio i numeri di carta di credito, chiedendo a tutti gli utenti di completare un processo di autenticazione prima di poter accedere, a prescindere dal loro livello di autorizzazione predefinito. La procedura può includere l'autenticazione multifattoriale (MFA), come una password e un codice monouso inviato a un dispositivo mobile.

Inoltre, il sistema valuta continuamente i rischi potenziali associati a dispositivi, utenti, dati e applicazioni verificando se: i dispositivi sono affidabili, le applicazioni e le relative istanze (aziendali o personali) sono conformi, la rete è sicura, i dati sono condivisi con destinazioni e destinatari affidabili e il comportamento dell'utente è in linea con le policy. Queste condizioni vengono verificate di continuo, e il sistema adatta di conseguenza la risposta. In più, monitora e tiene traccia degli accessi ai dati sensibili, avvisando gli amministratori in caso di comportamenti sospetti o di potenziali violazioni e fornendo agli utenti indicazioni sulle prassi da seguire in caso di violazione delle policy aziendali. Questo approccio riduce i rischi di accesso non autorizzato ai dati sensibili, perché il sistema verifica tutti gli utenti prima di autorizzare l'accesso, e minimizza i rischi per i dati sensibili educando gli utenti in tempo reale.

Il contesto permette alla soluzione DLP di autorizzare importanti attività aziendali

La filosofia Zero Trust aiuta i sistemi di protezione dei dati a prendere decisioni informate per autorizzare o limitare determinate attività. Per farlo, considera una serie di fattori o informazioni contestuali, come l'identità dell'utente, il dispositivo usato, l'affidabilità dell'applicazione e il contesto dei dati coinvolti (il sistema Zero Trust acquisisce il contesto con l'aiuto di altre soluzioni, di cui parleremo nella sezione "La soluzione DLP non deve rimanere sola".) Grazie a tutte queste informazioni di contesto, i principi Zero Trust possono determinare con più precisione se un'attività è vantaggiosa e indispensabile per l'azienda, e autorizzare l'esecuzione. Questo contribuisce ad assicurare la protezione dei dati e a minimizzare il rischio di violazioni della sicurezza o di altre minacce, senza tuttavia ostacolare il regolare svolgimento delle attività aziendali.

Di seguito elenchiamo i tipi di contesto usati nelle soluzioni Zero Trust:

- **Contesto dell'utente:** Chi compie un'azione o il destinatario di quell'azione. Queste informazioni aiutano a stabilire se il comportamento di un utente costituisce un rischio per i dati sensibili. Supponiamo, ad esempio, che un utente decida all'improvviso di trasferire molti più dati del solito, esegua l'accesso da posizioni insolite o si comporti in modo non conforme alla norma. Tutto questo potrebbe indicare un comportamento rischioso o dannoso. Lo stesso vale per gli utenti che usano o accedono a dati sensibili e/o li inviano ad applicazioni personali. Sulla base dell'identità e del comportamento di un utente, è possibile modificare i suoi privilegi per garantire che i dati sensibili restino protetti e che solo gli utenti autorizzati possano accedere a essi e condividerli con destinatari autorizzati, e solo verso destinazioni ritenute sicure.
- **Contesto del dispositivo:** Il dispositivo che tenta di accedere ai dati. È necessario considerare se il dispositivo è personale o aziendale, tenere conto della sua postura di sicurezza e se è aggiornato con le patch più recenti. Può essere utile considerare anche altri fattori, come l'affidabilità della posizione da cui si connette. Tenendo conto di tutti questi dettagli, è possibile determinare i privilegi da applicare al dispositivo in base al livello di rischio e di affidabilità. Anche se un utente è solitamente affidabile, il dispositivo usato può essere compromesso o porre un

rischio per la sicurezza; quindi, il contesto è fondamentale per determinare i privilegi.

- **Contesto dell'applicazione:** La reputazione e l'affidabilità dell'app usata per accedere ai dati o gestirli. Questo aspetto è importante perché se un'app ha una cattiva reputazione o è inaffidabile potrebbe porre un rischio per la sicurezza delle informazioni sensibili. I sistemi di protezione possono appoggiarsi ad altri sistemi (come un CASB, Cloud Access Security Broker) per acquisire informazioni sugli attributi della compliance e del rischio dell'applicazione. Queste informazioni possono aiutare a stabilire se l'app è rischiosa, ad esempio perché viola il Regolamento generale sulla protezione dei dati (GDPR) esponendo eccessivamente i dati sensibili.

  Un utente può avere accesso a più istanze di un'applicazione cloud, il che richiede un controllo più granulare sui dati sensibili per evitare la condivisione accidentale con account personali. Anche le app di comunicazione collaborative, come Microsoft Teams e Slack, possono rappresentare un rischio se i canali nelle applicazioni includono sia utenti aziendali che esterni; il sistema deve quindi essere in grado di distinguerli per evitare fughe di dati. È importante tenere a mente tutto questo per assicurarsi che le app usate siano tutte autorevoli e affidabili, proteggendo così i dati da ogni potenziale rischio.

- **Contesto dei dati:** Il grado di sensibilità di un determinato elemento dei dati, nonché il suo formato, le sue dimensioni e altri fattori. Il contesto dei dati include anche la posizione in cui vengono usati e la legittimità di tale uso. Conoscere il tipo di dati a cui si accede o che si spostano e sapere se la posizione è effettivamente quella di appartenenza aiuta a individuare le attività potenzialmente rischiose. I dati sensibili consultati o trasferiti verso posizioni non autorizzate richiedono interventi immediati per impedire violazioni o fughe di dati. Il contesto è essenziale per garantire che i dati siano esclusivamente accessibili a utenti autorizzati e gestibili, e solo presso posizioni approvate in base al loro livello di criticità. In questo modo, è possibile stabilire se un'attività è indispensabile per il business e se giustifica il rischio.

ATTENZIONE

La maggior parte delle soluzioni DLP (non solo quelle tradizionali) causa problemi con le normali attività dell'azienda perché generalmente non raccolgono abbastanza informazioni sul business e sui rischi associati. Esse obbligano l'azienda ad affidarsi alle decisioni manuali prese dal team di incident response, il che è frustrante, inefficiente e costoso!

La filosofia Zero Trust permette di contenere questi problemi. Una moderna soluzione di sicurezza dei dati unificata basata su principi Zero Trust tiene conto di tutti i rischi: utenti, dati, reti, dispositivi e applicazioni. In questo modo, il sistema comprende molto più a fondo i rischi e può prendere automaticamente le decisioni giuste su come proteggere i dati applicando policy di protezione dinamiche, adattate alle specifiche esigenze dell'azienda. La filosofia Zero Trust aiuta a tenere i dati al sicuro e l'azienda in attività.

La soluzione DLP non deve rimanere sola

I data control vengono usati nei sistemi DLP di oggi e di ieri. Le soluzioni DLP sono state create proprio con l'obiettivo di individuare e proteggere i dati sensibili. Il problema con la maggior parte di questi controlli è che non possono contare su informazioni di contesto. Un sistema DLP deve fare parte di una piattaforma più ampia, basata sui principi Zero Trust, che si avvale di tutte le informazioni di contesto disponibili per prendere decisioni informate. Quindi ha bisogno dell'aiuto e dell'input proveniente da altre soluzioni, come quelle DSPM (*Data Security Posture Managament*), per raccogliere tutto il contesto necessario in relazione all'utente, al dispositivo, all'applicazione e ai dati. Ecco perché un sistema basato sull'approccio Zero Trust è integrato e si focalizza sui controlli contestuali, invece di fidarsi alla cieca di tutto. È un modo per adattarsi a condizioni di rischio mutevoli e proteggere automaticamente i dati in ogni circostanza con la risposta più appropriata.


SUGGERIMENTO

In un sistema di protezione dei dati Zero Trust è bene cercare controlli consolidati, ognuno dei quali condivide informazioni e lavora in modo integrato per proteggere i dati. Ad esempio, Netskope Intelligent SSE (*Security Service Edge*) abilita direttamente i principi Zero Trust e rende possibile la condivisione del contesto tra i controlli (DLP inclusa), permettendo una protezione dei dati molto facile ed efficiente.

Netskope Intelligent SSE supporta la sua piattaforma DLP con molte altre soluzioni di sicurezza. Alcune delle più importanti sono:

- **Secure Web Gateway (SWG):** Una soluzione di sicurezza SWG si posiziona tra gli utenti e la rete Internet, garantendo connessioni sicure e offrendo una protezione dalle minacce web. Netskope DLP con SWG fa sì che i dati sensibili non confluiscano in traffico web rischioso e non attendibile, anche se crittografato. Individua, monitora e protegge i dati aziendali sensibili dalla perdita e

dall'esposizione su qualsiasi connessione web, inclusi gli uffici domestici, le filiali e le reti WI-FI pubbliche.

- **CASB:** Il componente CASB della piattaforma Netskope DLP individua, monitora e protegge i dati sensibili su applicazioni SaaS, IaaS (*Infrastructure-as-a Service*), reti aziendali e uffici remoti, servizi di posta elettronica, endpoint dei dipendenti e forza lavoro flessibile. Questo servizio centralizzato, erogato su cloud, applica policy di protezione unificate ovunque vengano salvati, usati o trasferiti dati sensibili, e copre sia i dati in movimento che a riposo. Esso interviene su migliaia di applicazioni SaaS e ha visibilità soltanto sui dati trasmessi a istanze personali (ad esempio, da un OneDrive aziendale a uno personale) o applicazioni considerate a rischio. Scansiona migliaia di tipi di file diversi, accanto a post e comunicazioni asincrone inviate tramite app collaborative e servizi di posta elettronica. Le policy di protezione dei dati, compliance e privacy vengono applicate in modo coerente su tutti i servizi cloud pubblici e sincronizzate automaticamente sull'intera piattaforma DLP.
- **DSPM:** Netskope One DSPM automatizza l'identificazione di tutti i dati in possesso dell'azienda, la loro posizione, chi può accedere e i rischi delle interazioni con tali dati. Inoltre, automatizza il rilevamento e la classificazione completa dei dati ed è in grado di individuare, contrassegnare e analizzare continuamente fonti di dati strutturati e non strutturati in ambienti on-premises, cloud e ibridi. Ciò garantisce una visibilità completa sui dati sensibili e la loro classificazione automatizzata a supporto della conformità normativa.
- **SSPM (Security Posture Management) e CSPM (*Cloud Security Posture Management*):** Queste tecnologie gestiscono la postura per ambienti SaaS e cloud pubblici per garantire la sicurezza e la compliance. I servizi monitorano e valutano continuamente la postura di sicurezza, identificando i potenziali rischi e configurazioni sbagliate, e generando raccomandazioni e insight attuabili. Le capacità automatizzate correggono i problemi rilevati in tempo reale.
- **Software di protezione degli endpoint:** Netskope Endpoint DLP è una soluzione che rileva, monitora e protegge i dati sensibili sugli endpoint dei dipendenti. Essendo la soluzione integrata nel client Netskope, non c'è bisogno di implementare un agente separato. Netskope Endpoint DLP minimizza l'uso delle risorse e offre una suite completa di funzioni, tra cui classificatori basati su ML, OCR, fingerprint dei file, EDM e altro ancora. Sfruttare il

servizio DLP erogato su cloud e l'input recuperato dall'intera piattaforma DLP aiuta a evitare scansioni duplicate dei dati originati nel cloud, offrendo così un'esperienza utente fluida e una protezione più efficace.

- **UEBA (*User and Entity Behavior Analytics*):** Questo controllo di sicurezza valuta continuamente il comportamento degli utenti per identificare attività insolite o potenzialmente a rischio. In passato, veniva spesso usato come controllo isolato ma per essere davvero efficace deve essere integrato in una piattaforma DLP. Raccogliendo i log delle violazioni a carico del DLP e segnalando comportamenti a rischio per un'ulteriore valutazione, UEBA può informare modifiche successive all'applicazione della policy, il che aiuta a mantenere la sicurezza dei dati.
- **Gestione delle identità e degli accessi (*IAM, Identity and Access Management*):** IAM è un metodo di gestione e controllo degli accessi alle risorse in base all'identità degli utenti. Include tecnologie come l'autenticazione MFA e SSO (*Single Sign-On*) e le liste di controllo degli accessi. Netskope permette integrazioni con molti fornitori IAM per garantire che solo utenti autorizzati possano accedere a risorse specifiche e proteggere dagli accessi non autorizzati. IAM è una componente essenziale della strategia Zero Trust di qualsiasi azienda e contribuisce alla protezione delle risorse e al rispetto di policy e norme di sicurezza.
- **Protezione della posta elettronica:** Netskope fornisce una soluzione DLP completa per applicazioni di posta elettronica come Microsoft 365 e Gmail, per i dati in movimento e a riposo. La soluzione protegge in tempo reale le e-mail sensibili in uscita attraverso proxy SMTP (*Simple Mail Transfer Protocol*) e webmail, ed è in grado di distinguere i dati sensibili in uscita di account di posta elettronica personali da quelli di account aziendali o servizi di posta elettronica privati.
- **Accesso Zero Trust alla rete (*ZTNA, Zero Trust Network Access*):** Netskope DLP, erogato tramite il servizio di accesso remoto Netskope Private Access (NPA), impedisce la perdita e l'esfiltrazione dei dati sia in risorse private nel data center sia in ambienti cloud pubblici garantendo così la protezione dei dati per gli accessi tramite browser ad applicazioni private da qualsiasi posizione si connettono gli utenti.

Combinando questi componenti chiave in un unico sistema integrato, la piattaforma SSE di Netskope fornisce una soluzione di sicurezza

completa, in grado di proteggere l'azienda e i suoi dati da un'ampia serie di minacce.

Applicare i principi Zero Trust alla sicurezza dei dati

RICORDA

Lo scopo della protezione Zero Trust non è solo impedire ai dati sensibili di uscire dall'azienda, ma è consentire l'esecuzione di moderni casi d'uso senza perdere di vista il rischio e la sicurezza.

Questo significa supportare gli utenti che lavorano da posizioni diverse e incentivare la collaborazione, garantendo al tempo stesso la sicurezza delle informazioni. Proteggere i dati secondo la filosofia Zero Trust vuol dire essere in grado di lavorare ovunque senza perdere l'accesso alle risorse necessarie per collaborare con colleghi e partner esterni, né preoccuparsi di eventuali fughe di dati. Una soluzione unificata, come Netskope SSE, permette di tutelare i dati e sfruttare tutti i vantaggi offerti dai moderni flussi di lavoro aziendali.

Seguono un paio di esempi pratici:

- Immaginiamo di lavorare su un laptop e di aver eseguito l'accesso alla rete aziendale con Netskope SSE. Accediamo ad alcuni importanti documenti di vendita e iniziamo a lavorarci. A un certo punto, però, salviamo per sbaglio una copia dei documenti nel nostro spazio di archiviazione cloud invece di usare l'istanza aziendale.

  Con una piattaforma DLP basata sui principi Zero Trust, il sistema riconosce che stiamo cercando di trasmettere informazioni aziendali sensibili all'istanza personale di un'app e blocca il salvataggio. A questo punto visualizza una notifica informativa, cioè un pop-up che ricorda di salvare i documenti nella posizione corretta. Così possiamo lavorare da qualsiasi posizione senza perdere l'accesso a tutte le risorse necessarie e senza preoccuparci di inviare per sbaglio dati sensibili a destinazioni non autorizzate. Le notifiche informative ricordano agli utenti le buone prassi e le policy di sicurezza aziendali, minimizzando il rischio di perdite di dati e limitando il bisogno di formazioni nel corso dell'anno.
- Immaginiamo di collaborare a un progetto con partner esterni e di voler condividere con loro alcuni documenti. Con una piattaforma DLP basata sui principi Zero Trust, il sistema verificherà la reputazione e l'affidabilità dell'app usata per condividere i

documenti, la nostra identità e il nostro comportamento, il dispositivo e la destinazione.

Se usiamo un'app di archiviazione cloud personale con un livello di sicurezza diverso da quella aziendale, il sistema può impedire la condivisione dei dati tramite quell'app suggerendone invece una diversa o di inviare i documenti attraverso un canale sicuro. La soluzione DLP verificherà anche la destinazione dei dati per controllare, ad esempio, se è sicura o se il destinatario è un utente esterno o un dipendente. La piattaforma DLP può chiedere di confermare la condivisione dei dati sensibili con utenti esterni e, in certi casi, anche di fornire una giustificazione. In questo modo, possiamo collaborare in sicurezza, sapendo che i dati sono protetti e accessibili solo agli utenti autorizzati.

Approccio Zero Trust adattivo

Un approccio Zero Trust adattivo parte dal presupposto che le cose cambiano nel tempo. Questo significa che la protezione Zero Trust deve continuamente valutare il contesto operativo, il rischio e il comportamento degli utenti per garantire la sicurezza dei dati.

Prendiamo come esempio il buttafuori all'ingresso di una discoteca: Una notte, mentre è in piedi davanti alla porta, si avvicina un gruppo di persone. Il buttafuori controlla i documenti del gruppo e, poiché tutto sembra in regola, li lascia entrare. Ma con il passare della serata, il buttafuori inizia a notare comportamenti strani da parte di una persona del gruppo, che si mostra aggressiva o tenta di entrare in un'area del locale non autorizzata. Grazie all'approccio Zero Trust adattivo, il nostro buttafuori è in grado di riconoscere questo comportamento e agire per proteggere gli altri clienti. Può decidere di tenere d'occhio alcune persone per verificare che non causino problemi, e addirittura chiedere a qualcuno di andarsene. In questo modo, il buttafuori riesce a garantire la sicurezza della discoteca e di tutti gli altri clienti, anche se il comportamento di qualcuno cambia.

Esaminiamo ora alcuni scenari comuni per un'azienda:

- **Il comportamento di un utente cambia all'improvviso.** Un dipendente di fiducia ha sempre avuto accesso a certi dati aziendali sensibili. Un giorno, probabilmente dopo una valutazione delle sue performance, inizia a comportarsi in modo diverso: consulta e scarica più dati sensibili del solito o esegue l'accesso da posizioni insolite. L'approccio Zero Trust adattivo consente al

sistema di riconoscere questo nuovo comportamento e alterare di conseguenza i relativi privilegi. Ad esempio, il sistema può limitare l'accesso a certi dati o avvisare il team di sicurezza per i necessari approfondimenti. In questo modo, è possibile proteggere i dati anche se cambia il comportamento di un dipendente fidato.

- **La reputazione e l'affidabilità delle applicazioni cambiano.** Con il tempo le applicazioni cambiano, non solo in termini di caratteristiche tecniche ma anche di reputazione, postura di sicurezza e affidabilità. Ad esempio, un'app di archiviazione cloud prima considerata sicura ora può presentare nuove vulnerabilità o configurazioni errate che ne compromettono l'affidabilità. Con un approccio Zero Trust adattivo, la soluzione valuta continuamente il livello di rischio dell'app e modifica i privilegi di accesso in base alle necessità. In questo modo, è possibile proteggere i dati anche se cambia l'affidabilità di un'app.
- **I dispositivi diventano compromessi.** I dispositivi possono diventare più vulnerabili o persino compromessi senza che l'utente se ne accorga. Ad esempio, un laptop prima considerato sicuro può venire infettato da malware oppure le sue impostazioni di sicurezza possono essere modificate all'insaputa dell'utente. Con un approccio Zero Trust adattivo, il sistema valuta continuamente la postura di sicurezza del dispositivo, modificandone i privilegi di accesso se necessario. In questo modo, è possibile proteggere i dati anche se un dispositivo diventa compromesso.
- **I flussi di dati cambiano.** I flussi di dati possono cambiare a causa di modifiche alle regole di compliance a vari livelli. Ad esempio, un flusso di dati può essere considerato accettabile ma se la destinazione diventa non conforme o non sicura le norme possono comunque imporre all'azienda di proteggerlo. È il caso del GDPR, secondo il quale alcune categorie di dati personali non possono essere trasferite al di fuori dell'Unione Europea senza una decisione di adeguatezza o un accordo valido sul trasferimento. Con un approccio Zero Trust adattivo, il sistema valuta continuamente i rischi e modifica i privilegi, se è il caso. In questo modo, è possibile proteggere i dati anche se cambiano le norme in vigore.
- **Il ruolo o lo stato di un utente cambiano.** Un dipendente che si dimette può ancora accedere ai dati sensibili nel periodo di preavviso. Con un approccio Zero Trust adattivo, il sistema valuta

continuamente i rischi impliciti e modifica i privilegi, se è il caso. Ad esempio, può decidere di limitare l'accesso dell'utente a determinate informazioni o avvisare il team di sicurezza per i necessari approfondimenti.

SUGGERIMENTO

Un approccio Zero Trust adattivo valuta l'uso da più punti di vista per adeguare i privilegi di accesso, quindi proteggere i dati sensibili e la reputazione dell'azienda.

Questo approccio offre una protezione maggiore, pur favorendo la produttività delle persone e dei dati. Inoltre, permette di applicare una policy di protezione dinamica e adattiva delle informazioni, valutando continuamente i rischi e modificando i privilegi di accesso se serve. È un grosso passo avanti rispetto all'approccio tipico dei sistemi DLP (tradizionali e non), i quali si affidano a metodi standard basati sulla fiducia implicita che generano molti falsi positivi e appesantiscono il carico di lavoro dei team di sicurezza. Approcci così laboriosi obbligano il team di incident response a valutare manualmente ogni allarme, per capire se si tratta di una violazione effettiva, e quindi a contattare l'utente responsabile (che nel frattempo avrà dimenticato cosa ha fatto). Poi, il team deve decifrare l'intero flusso di dati: un processo lungo e che richiede molte risorse. Un approccio Zero Trust adattivo fornisce un modello di protezione continua, agevolando la sicurezza dei dati e il normale svolgimento delle attività aziendali.

Sicurezza dei dati Netskope con approccio Zero Trust adattivo

La sicurezza dei dati con approccio Zero Trust adattivo implementata da Netskope è interamente basata sul contesto. Monitorando il traffico tra utenti, dispositivi, applicazioni, reti e destinazioni, Netskope acquisisce una comprensione approfondita di ciò che accade nell'azienda. Questo permette al sistema di esercitare un controllo granulare sull'accesso ai dati, e quindi di proteggere i dati sensibili senza ostacolare le operazioni aziendali.

Immaginiamo, ad esempio, un utente che cerca di accedere a informazioni sensibili da un dispositivo personale. Con Netskope, il processo inizia da un accurato rilevamento dei dati sensibili. Poi, valutando una serie di fattori contestuali, la risposta agli incidenti diventa più precisa ed efficace, il che riduce il bisogno di valutare

manualmente i singoli allarmi e quindi il lavoro a carico dei team. Il sistema valuta la postura di sicurezza del dispositivo, l'identità e il comportamento dell'utente per decidere se autorizzare l'accesso.

Altri fattori considerati sono: connessione di rete, posizione, potenziali vulnerabilità, informazioni a disposizione sulle minacce e molto altro. La reputazione e i rischi associati all'applicazione vengono verificati dal Netskope Cloud Confidence Index (CCI), un database in continua crescita che oggi conta più di 83.000 applicazioni cloud valutate da Netskope sulla base di 50 criteri di rischio. Questi criteri misurano l'idoneità di un'app a casi d'uso aziendali, prendendo in considerazione fattori come la sicurezza, la verificabilità e la continuità aziendale.

Se il dispositivo è considerato rischioso o il comportamento dell'utente insolito, la soluzione può limitare l'accesso o avvisare il team di sicurezza per i necessari approfondimenti. Se il comportamento dell'utente è normale e il dispositivo sicuro, l'accesso verrà fornito.

SUGGERIMENTO

L'SSE è alla base del sistema di sicurezza dei dati di Netskope, e fa parte della più ampia piattaforma Netskope One SASE (Secure Access Service Edge). Questa soluzione integrata, nativa in cloud, consolida le tecnologie di sicurezza essenziali illustrate fin qui in una singola piattaforma. Combinando le tecnologie in un'unica piattaforma, Netskope facilita la gestione della sicurezza da una posizione centralizzata. Netskope SSE è nativa in cloud, il che la rende scalabile in modo rapido ed efficiente per soddisfare i bisogni dell'azienda. In più, è progettata per essere altamente flessibile e quindi personalizzabile in base a esigenze specifiche.

Netskope SSE è sviluppata partendo dal presupposto che garantire la sicurezza significa molto di più della semplice applicazione delle policy. È importante anche educare i dipendenti promuovendo una gestione dei dati sensibili sicura. Per questo la soluzione lascia all'utente la capacità di prendere decisioni senza rinunciare alla sicurezza dei dati. Ad esempio, nel caso di una violazione, Netskope SSE può consigliare ai dipendenti dei moduli di formazione che spiegano come gestire i dati sensibili, fare domande per valutare ulteriormente il contesto o fornire best practice o suggerimenti per lavorare in sicurezza anche da casa. Adottando un approccio olistico alla protezione dei dati, Netskope aiuta le aziende a sviluppare al loro interno una cultura orientata alla sicurezza.

IN QUESTO CAPITOLO

- **Confronto tra le soluzioni di sicurezza dei dati unificate e le soluzioni tradizionali**
- **Garantire la sicurezza da qualsiasi punto di accesso alle informazioni**
- **Usare policy e controlli degli accessi unificati**
- **Valutare i vantaggi e gli elementi differenzianti di Netskope One Data Security**

Capitolo 4
Perché implementare la sicurezza dei dati unificata di Netskope

Spesso, i Chief Information Security Officer (CISO) e i team di sicurezza informatica si trovano di fronte a una decisione difficile: conviene tenere delle soluzioni DLP mature, ma complesse e costose, o passare ad alternative basate sul cloud, più facili da implementare ma che potrebbero essere prive dei livelli di accuratezza e applicabilità necessari? In questo capitolo rispondiamo alla domanda partendo dai principali vantaggi delle soluzioni di sicurezza dei dati basate sul cloud:

- **Assicurano una protezione completa.** Indipendentemente da dove sono archiviati i dati (on-premise o sul cloud), dove vengono trasferiti o come vi si accede, una soluzione di sicurezza erogata sul cloud che include il DLP integrato e il DSPM (*Data Security Posture Management*) è in grado di proteggerli.
- **Garantiscono la protezione in ambienti cloud.** Grazie alle applicazioni SaaS, ai servizi cloud pubblici IaaS e all'accesso web, indipendentemente dal luogo da cui si connettono gli utenti nelle aziende che hanno adottato modelli di lavoro ibridi, le soluzioni di sicurezza dei dati basate sul cloud garantiscono una protezione completa.

- **Eliminano la necessità di configurare infrastrutture aggiuntive perché possono essere implementate in modo facile e veloce come servizi cloud.**
- **Proteggono i dati sensibili senza sovraccaricare le risorse della rete o degli endpoint.** Un sistema di sicurezza dei dati erogato sul cloud può gestire tutte le attività di scansione dei dati e gli algoritmi di rilevamento alla massima capacità.
- **Sono più facili da integrare con un'ampia gamma di altri strumenti di sicurezza.**
- **Assicurano più visibilità sui dati trasferiti e archiviati al di fuori delle sedi aziendali.**
- **Consentono di mantenere e aggiornare più facilmente il sistema in tempo reale e scalare in modo più facile e veloce rispetto ai tradizionali modelli on-premise.**

In questo capitolo, spieghiamo come un'azienda può usufruire di questi vantaggi e prepararsi a prendere decisioni informate sul sistema di sicurezza dei dati in cloud più adatto. Forniamo inoltre informazioni specifiche sulle caratteristiche distintive della piattaforma Netskope.

Capire le differenze tra le soluzioni di sicurezza dei dati in cloud

La sicurezza dei dati unificata deve essere erogata sul cloud. Quando si tratta di DLP, ne sono disponibili due tipi. Le soluzioni DLP native in cloud sono generalmente integrate in piattaforme IaaS e applicazioni SaaS offerte da fornitori di servizi cloud. Le soluzioni DLP erogate su cloud, in genere, fanno parte di un prodotto o servizio di sicurezza come SWG, NGFW (Next-Generation Firewall) o CASB.

Tipo 1: Netskope One Data Security e le soluzioni native in cloud a confronto

Netskope One Data Security offre una serie di vantaggi rispetto alle più limitate soluzioni native in cloud.

Include funzioni DPSM, il che significa che è in grado di individuare e proteggere i dati ovunque, garantisce un uso sicuro dell'intelligenza artificiale generativa (GenAI) aziendale, gestisce la postura di sicurezza dei dati, supporta la privacy e la conformità, riduce l'esposizione dei dati a causa di azioni dolose o negligenti e risponde in modo

efficace ai rischi e alle minacce di esfiltrazione dei dati. Il consolidamento di queste funzioni in un'unica piattaforma offerta da un solo fornitore semplifica le operazioni e riduce i costi operativi.

Un altro importante vantaggio è la maggiore copertura attraverso un singolo motore di policy DLP di livello enterprise, che assicura la protezione dei dati sensibili su una più estesa gamma di formati, canali di comunicazione e ambienti, incluse le applicazioni SaaS, i servizi IaaS, le applicazioni private, i servizi di posta elettronica e di condivisione file e le transazioni web, a prescindere dalla posizione degli utenti. Include inoltre la protezione DLP degli endpoint, che è importante in quanto aiuta a tenere al sicuro tutti i dati sensibili, anche nel caso di endpoint in posizioni remote che possono accedere o meno al cloud tramite una rete specifica. In più, il singolo motore di policy DLP riduce notevolmente la complessità rispetto al dover gestire una serie di parametri DLP per diversi canali e servizi cloud.

Inoltre, Netskope One DLP è superiore in termini di accuratezza di rilevamento. La soluzione esamina qualsiasi tipo di file e formato di dati, e usa un'ampia gamma di algoritmi di rilevamento e il machine learning per capire tutta una serie di informazioni e documenti, insieme al relativo contesto; quindi, è in grado di identificare e classificare con precisione i dati sensibili, anche se sono archiviati e trasferiti in strutture, formati o lingue diverse, o addirittura incorporati nelle immagini. Questo è importante perché aiuta a impedire la perdita o l'esposizione accidentale dei dati sensibili e garantisce l'identificazione dei soli eventi di sicurezza veri e propri, senza falsi positivi.

Infine, Netskope One Data Security integra la filosofia Zero Trust per l'analisi del contesto; questo significa che è progettato per lavorare in un'architettura di sicurezza Zero Trust completa. Ciò aiuta a garantire che tutti gli accessi ai dati sensibili siano controllati e monitorati attentamente, in misura adeguata al contesto di rischio, limitando le probabilità di accessi non autorizzati, sovraesposizione o fughe di dati.

Al giorno d'oggi, molti CSP (*Cloud Service Provider*) e fornitori di soluzioni SaaS offrono capacità DLP native nelle loro piattaforme. Queste soluzioni pronte all'uso e fortemente orientate al cloud sono spesso preferite dalle aziende che perseguono una strategia cloud-first o che sono all'inizio del loro processo di protezione dei dati. E anche se sono in grado di gestire in modo efficace i casi d'uso per cui sono progettate, possono non avere capacità di protezione più ampie o offrire un approccio completo come le soluzioni DLP tradizionali.

ATTENZIONE

Alcune aziende iniziano da soluzioni DLP native in cloud perché permettono una messa in esercizio semplice e rapida. Ma è importante tenere gli occhi ben aperti, e valutare se queste sono effettivamente sufficienti a soddisfare tutti i requisiti di protezione dei dati necessari. In alcuni casi, le aziende sono costrette ad adottare più soluzioni DLP sconnesse e isolate per far fronte a casi d'uso emersi successivamente, il che si traduce in una strategia di protezione frammentata e potenzialmente meno efficace.

Tipo 2: Le soluzioni DLP erogate su cloud non sono tutte uguali

Quando si tratta di scegliere una soluzione DLP erogata dal cloud, è bene tenere presente che molte delle soluzioni più recenti hanno grosse carenze.

- Alcune offrono una protezione ampia, ma senza la profondità tecnologica e le funzioni richieste per proteggere i dati sensibili dell'azienda in modo efficiente e accurato per tutti i casi d'uso moderni.
- Altre offrono i più recenti metodi e funzioni per specifici casi d'uso e formati di dati, ma non la copertura necessaria a proteggere i dati sensibili in modo approfondito.

ATTENZIONE

Alcune delle più recenti soluzioni DLP erogate su cloud si presentano bene su carta ma sono lontane anni luce dalle piattaforme tradizionali, più sofisticate e mature, che dovrebbero sostituire.

È importante fare ricerche approfondite e mettere a confronto le opzioni disponibili per essere certi di scegliere quella che soddisfa davvero le esigenze dell'azienda. È bene valutare fattori come il livello di maturità e sofisticazione delle capacità di rilevamento dei dati (ad esempio, quanti tipi di file possono essere esaminati e quanti identificativi di dati sono usati, compresi i tipi di dati localizzati specifici per Paese), la varietà di canali coperti, la capacità di adattarsi a rischi e ambienti in continua evoluzione e il livello di integrazione e personalizzazione offerto.

SUGGERIMENTO

Se si sceglie di adottare una soluzione DLP erogata dal cloud per la sicurezza dei propri dati, è bene capire qual è la più adatta. Ecco di cosa tenere conto:

- **Ampiezza della copertura:** Le soluzioni di sicurezza dei dati più estese che integrano anche il DLP, spesso come parte di un

servizio ZTNA, includono generalmente anche DSPM, SWG, CASB o NGFW. Esse sono erogate dal cloud e integrate in un servizio di sicurezza di rete. L'ambito di applicazione è limitato. Ad esempio, non includono funzioni di protezione dei dati per le e-mail in uscita e gli endpoint, né uno spettro più ampio di applicazioni SaaS con le relative istanze specifiche (vale a dire, account aziendali vs personali).

- **Limiti delle soluzioni:** Può darsi che soluzioni di questo tipo non coprano tutti i casi d'uso moderni e tradizionali, come la collaborazione su cloud con utenti esterni, i trasferimenti dei dati tramite account e-mail personali o bozze di messaggi di posta elettronica, i trasferimenti dei file via USB, gli screenshot e le immagini di documenti sensibili, i nuovi modelli di compliance, i dati in lingue e formati stranieri, ecc. Ma soprattutto, possono avere capacità di rilevamento più limitate e funzioni IA e ML deludenti.
- **Accuratezza del rilevamento dei dati sensibili:** Molte delle soluzioni DLP in cloud più recenti non sono in grado di rilevare i dati sensibili con la necessaria precisione e granularità, on-premise o sul cloud. Spesso si limitano a scansionare solo un numero ristretto di tipi di file e non hanno i necessari identificativi di dati, a differenza delle soluzioni più mature. Si fanno notare perché sono focalizzate su una o due funzioni particolarmente "appariscenti", senza tuttavia fornire una sicurezza dei dati veramente completa. Netskope One Data Security assicura questa copertura completa integrando DSPM e DLP in una soluzione unificata.

  Una soluzione matura offre migliaia di identificativi predefiniti di dati, tra cui un'ampia gamma di informazioni di identificazione personale (PII), passaporti, conti bancari, informazioni bancarie internazionali, documenti d'identità nazionali, dati finanziari, dati sanitari, dati anagrafici e informazioni specifiche di settore, oltre a lingue localizzate e identificativi personalizzabili. Inoltre, può fornire un'ampia gamma di profili di policy predefinite a supporto di specifici casi d'uso e requisiti di conformità come il Regolamento generale sulla protezione dei dati (GDPR), il *California Consumer Privacy Act* (CCPA), il *Payment Card Industry Data Security Standard* (PCI-DSS), l'*Health Insurance Portability and Accountability Act* (HIPAA) e il *Gramm-Leach-Bliley Act* (GLBA), solo per citarne alcuni.
- **Integrazione in una piattaforma:** Una soluzione DLP erogata dal cloud deve integrarsi perfettamente con una piattaforma di sicurezza più ampia per garantire una protezione efficace dei dati sensibili nel contesto di rischio disponibile per utenti, dispositivi,

reti, applicazioni, comportamenti e destinazioni. Una soluzione DLP integrata usa le informazioni provenienti da altri punti di controllo, come l'analisi del comportamento degli utenti (UEBA) con SWG, CASB, ZTNA e DSPM di prossima generazione, per comprendere a fondo la postura di sicurezza di un'azienda e i rischi associati a ogni singola interazione con i dati sensibili. Questo significa essere consapevoli delle istanze specifiche delle applicazioni SaaS e dei dispositivi in uso, distinguendo tra le identità utente di account personali e aziendali, i diversi destinatari delle condivisioni dei dati e molto altro. Questo livello di integrazione rende possibile un approccio più preciso e granulare al rilevamento e alla protezione di dati sensibili.

SUGGERIMENTO

Alcuni fornitori offrono strumenti DLP sotto forma di componenti aggiuntivi ai prodotti principali, ma senza le necessarie capacità rischiano di non fornire il livello di protezione che serve alle aziende.

Bisogna valutare e testare con attenzione le capacità delle varie soluzioni DLP e scegliere quella che soddisfa meglio le esigenze attuali dell'azienda, nonché quelle future anche in termini di copertura. Un set di funzioni mature e un fornitore competente sono fondamentali. Affidarsi solo alle basi può portare a rilevamenti parziali o inesatti, oltre che a tonnellate di falsi positivi.

Forte di oltre un decennio di innovazione e impegno costanti sul fronte della sicurezza dei dati, Netskope è considerata lo standard di riferimento rispetto ad altri fornitori di piattaforme SASE e SSE. Nelle sezioni seguenti, approfondiremo le caratteristiche e le funzioni che contraddistinguono Netskope One Data Security.

Come Netskope One Data Security garantisce sicurezza

Netskope One Data Security è una soluzione completa erogata su cloud che aiuta a proteggere i dati personali su tutti i principali canali, compresi cloud, reti, e-mail, endpoint e utenti da qualsiasi posizione. È progettata per acquisire conoscenze in termini di rischio e di contesto al fine di garantire la sicurezza dei dati in transito verso qualsiasi destinazione.

Netskope One Data Security è *completamente integrata* nella soluzione Netskope SSE, descritta nel Capitolo 3, ed erogata come parte di una piattaforma SASE completa. L'utente, quindi, ottiene una piattaforma

unificata e nativa in cloud che aiuta a eliminare gli angoli ciechi, offre un approccio coerente, migliora le prestazioni e riduce i costi e la complessità.

Netskope One Data Security protegge tutti i canali e i trasferimenti di dati, come mostrato nella Figura 4-1, per proteggere sempre tutte le informazioni sensibili. La soluzione copre:

- quasi 83.000 applicazioni SaaS (con classificazione dinamica di nuove app) e ogni singola istanza di queste applicazioni
- tutti i maggiori provider IaaS, tra cui Amazon Web Services (AWS), Google Cloud Platform e Microsoft Azure
- le applicazioni private ospitate nel data center o nel cloud pubblico
- le reti aziendali e le filiali
- la forza lavoro remota
- tutti i servizi di posta elettronica, on-premise e sul cloud, nonché la Web mail
- tutti gli endpoint dei dipendenti, on-premise o meno

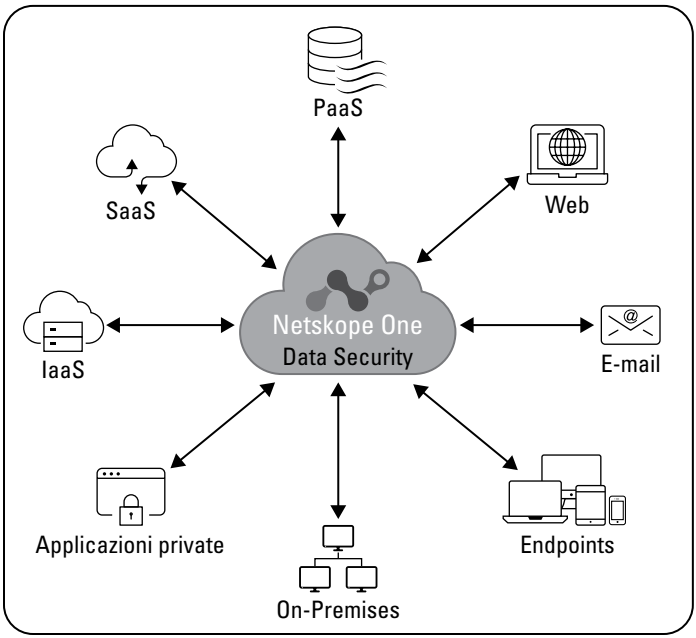

FIGURA 4-1: Netskope One Data Security, che include DSPM e DLP unificati, assicura la sicurezza dei dati ovunque si trovano o vengono trasferiti.

Principali elementi differenzianti

Spesso le soluzioni DLP tradizionali sono considerate inaccurate; il vero problema sono i falsi positivi, e per risolverlo serve molta più precisione. Questo viene spiegato nel Capitolo 2, che presenta e approfondisce anche i "fattori chiave" in grado di accrescere la precisione dei sistemi DLP. In questa sezione, vedremo come Netskope è riuscita a trasformare questi "fattori" in elementi differenzianti per sviluppare una soluzione di sicurezza dei dati unificata, personalizzabile e automatizzata in grado di soddisfare i bisogni dell'azienda.

Protezione completa di tutti i canali critici con policy unificate

I dati sensibili che vengono trasferiti al di fuori della sede tradizionale dell'azienda diventano sempre più difficili da monitorare e proteggere, e sono quindi più soggetti a esposizioni, intenzionali o meno. Netskope One Data Security scopre, monitora e protegge i dati sensibili in movimento, a riposo e in uso nell'intero ecosistema aziendale, comprese le applicazioni SaaS, gli ambienti IaaS cloud pubblici, le reti aziendali, gli uffici remoti, la forza lavoro remota, i servizi di posta elettronica e gli endpoint dei dipendenti.

Questo sistema fornisce policy di sicurezza dei dati unificata erogate tramite un servizio cloud centralizzato, per ogni singola posizione in cui le informazioni vengono archiviate, usate o trasferite.

La singola console con controllo degli accessi basato sui ruoli (RBAC) consente al personale di sicurezza autorizzato di gestire da un unico pannello la configurazione delle policy, il monitoraggio e le attività di segnalazione e incident response, per tutti i canali.

Capacità superiori di rilevamento e protezione dei dati sensibili

Gli identificativi di dati sono fondamentali per aiutare una soluzione DLP a individuare i dati sensibili sulla base di caratteristiche specifiche come parole chiave descrittive, espressioni regolari, numero di cifre, caratteri speciali, modelli, analisi di prossimità e così via. Quando si cerca una soluzione DLP, è bene verificare che il prodotto selezionato abbia le capacità di identificazione indispensabili per coprire tutti i casi d'uso attuali e futuri. Una buona soluzione DLP deve essere in grado di fornire diverse migliaia di identificativi predefiniti per cercare e identificare con precisione quante più varietà

di dati sensibili possibile, nonché le relative variazioni, anche minime. Netskope One offre tutte queste caratteristiche facendo leva sul machine learning e sulla capacità di personalizzare in modo granulare gli identificativi e i modelli di policy per far fronte a tutte le esigenze di protezione dei dati.

SUGGERIMENTO

È bene non concentrarsi solo sugli identificativi di dati che servono nell'immediato. Bisogna puntare su una soluzione "a prova di futuro" capace di supportare anche tipi di dati, applicazioni e normative non ancora esistenti. Il nostro consiglio è cercare un prodotto con migliaia di identificativi di dati e modelli di policy predefiniti per assicurare la conformità a regolamenti come il GDPR e il CCPA. E non bisogna dimenticare la capacità di creare e modificare identificativi personalizzati per soddisfare esigenze specifiche.

Le informazioni sensibili possono trovarsi nei file più disparati: cartelle compresse (ZIP, RAR, ISO ecc.), presentazioni, e-mail, immagini (BMP, JPG o PNG), fogli di calcolo, file CAD, post sui social, moduli online, messaggi di chat, allegati ed elementi grafici di ogni tipo. I tipi di dati di cui bisogna tenere traccia sono davvero molti, quindi è indispensabile avere una soluzione DLP capace di gestirli tutti.

La corrispondenza esatta dei dati è un altro aspetto fondamentale da considerare, soprattutto per le aziende grandi (o per quelle che aspirino a crescere). La soluzione DLP deve essere in grado di elaborare milioni (se non miliardi) di record con facilità. I moderni strumenti in cloud, come Netskope One, possono far leva sul cloud computing per eseguire analisi dei dati su larga scala, endpoint inclusi, senza rallentare altri processi essenziali. In questo modo, tutti i dati personali (di dipendenti, clienti, partner o altri) saranno completamente al sicuro.

TESORO, MI SI È RISTRETTA LA SUPERFICIE DI ATTACCO

Le organizzazioni che vogliono proteggere i dati sensibili dalle minacce informatiche devono colmare eventuali lacune nell'approccio usato. La *superficie di attacco* corrisponde al numero totale delle potenziali vulnerabilità o dei punti di ingresso che gli hacker o i dipendenti stessi dell'azienda possono usare, in modo sia intenzionale che malevolo. Limitare la superficie di attacco può rendere più difficile identificare

(continuazione)

(continuazione)

> e sfruttare i punti deboli; in più, colmare i divari esistenti nella protezione può ridurre notevolmente il rischio di attacchi o esposizioni accidentali dei dati. Fare in modo che tutti i dispositivi, le applicazioni e le reti siano adeguatamente protetti è essenziale per correggere i punti deboli alla base del rischio di esposizione.

Per ottimizzare la difesa dei dati sensibili, è necessario trovare una soluzione DLP con capacità di rilevamento avanzate (OCR, IA, ML, fingerprint dei file e strategie Zero Trust), tutte incluse in Netskope One Data Security (v. il Capitolo 2).

Netskope One Data Security è in grado di identificare con precisione i dati sensibili, anche se salvati in formati moderni e non strutturati come immagini (screenshot e fotografie) o in lingue diverse. Grazie ai suoi sofisticati classificatori basati sul machine learning, la soluzione è in grado di riconoscere immagini sensibili come patenti di guida, carte di credito, documenti d'identità, contratti, brevetti, documenti relativi a fusioni e acquisizioni (M&A) e assegni, anche con immagini poco chiare, sfocate, distorte o danneggiate. Questo approccio riduce inoltre il carico di lavoro dei team specializzati grazie all'identificazione e alla protezione automatica dei dati sensibili.

Netskope One Data Security dispone di una serie di strumenti di classificazione avanzati basati sul machine learning, tra cui migliaia di identificativi di dati. Inoltre, analizza più di 2.100 tipi di file facendo leva su criteri di rilevamento contestuali, EDM altamente scalabile, fingerprint di documenti strutturati e non, classificazione precisa delle immagini basata su ML, OCR avanzato e classificatori di dati basati su IA/ML per rilevare e identificare le informazioni sensibili.

Sicurezza dei dati basata sulla consapevolezza del rischio e del contesto

Il contesto è alla base di una sicurezza dei dati efficace. Monitorando il traffico fra utenti e app, è possibile esercitare un controllo granulare e autorizzare o bloccare l'uso dei dati sensibili in base a diversi fattori, come l'identità dell'utente, cosa cerca di fare e il motivo alla base di una determinata azione. Questo tipo di approccio incentrato

sui dati è il modo migliore di gestire il rischio dei moderni ambienti ibridi delle aziende.

Netskope One Data Security elimina la fatica e le interruzioni all'attività aziendale causate dall'incident response. In effetti, va oltre l'approccio statico di individuare le informazioni sensibili e rispondere sulla base di policy di violazione predefinite al fine di tenere conto del contesto organizzativo e dei rischi per la sicurezza e quindi attivare dinamicamente la protezione adeguata in base a condizioni in costante evoluzione.

Netskope One Data Security è integrata nativamente nella soluzione completa Netskope One SSE, una piattaforma di sicurezza cloud-native completamente convergente che consolida e riunisce tecnologie di sicurezza come SWG, CASB DSPM e UEBA in una piattaforma unificata e integrata. Questo approccio elimina gli angoli ciechi, garantisce l'applicazione coerente delle policy di sicurezza e riduce nettamente i costi e la complessità. La piattaforma è sempre al corrente del comportamento, della posizione geolocalizzata e della postura di sicurezza degli utenti, dei rischi a livello di dispositivo, dei rischi e della reputazione delle applicazioni, delle istanze personali di app e altro ancora, e permette alla soluzione DLP di limitare le attività di risposta ai soli incidenti effettivi, minimizzando i falsi positivi, la necessità di valutare manualmente gli incidenti e le interruzioni alle attività aziendali.

Una soluzione SASE integrata, basata sui principi Zero Trust e su controlli avanzati di protezione dei dati consente di aumentare la visibilità e la mitigazione del rischio in tutti i vettori chiave. In più, è possibile semplificare le attività di classificazione dei dati, la definizione dei criteri e la gestione degli incidenti grazie a una piattaforma unificata basata su ML, reportistica approfondita e analisi avanzate. E grazie alle policy flessibili incentrate sul contesto, abbinate a un agent leggero, si migliora l'agilità e si riduce l'attrito a vantaggio dell'utente finale.

RICORDA

Per garantire la buona riuscita del programma di protezione dei dati, è essenziale formare i dipendenti e promuovere prassi sicure di gestione delle informazioni. A questo preciso scopo, Netskope One DLP offre programmi di coaching e sensibilizzazione degli utenti in tempo reale. In più, può essere integrata con i maggiori sistemi di gestione della formazione e ha un portale utente personalizzabile per l'autoapprendimento.

Lavorare in modo più intelligente con una soluzione DLP inclusa in una strategia più estesa mirata alla sicurezza dei dati

La soluzione Netskope One DLP è erogata dal cloud, quindi non si affida a componenti on-premise. Inoltre, offre una protezione sempre attiva e aggiornata, eliminando la necessità di aggiornamenti manuali come quelli richiesti dalle soluzioni DLP tradizionali.

Puntando su policy unificate di sicurezza dei dati, su un'unica console e sul controllo RBAC, la gestione delle configurazioni delle policy, il monitoraggio, la reportistica e le attività di incident response diventano un gioco da ragazzi.

In passato, le aziende erano costrette a creare policy individuali per ogni canale (ad esempio, web, posta elettronica e ogni singola app), il che richiedeva un enorme dispendio di tempo e risorse. Netskope One Data Security è un servizio cloud centralizzato e unificato che permette di definire una sola policy per l'azienda e di sincronizzarla automaticamente su tutti i canali. Questo significa poter creare la policy una sola volta, senza doverla replicare e perfezionare continuamente in posizioni diverse.

RICORDA

Con le soluzioni DLP tradizionali servivano molti amministratori di sistema per creare e gestire le policy. L'attuale carenza di talenti impone però di scegliere una soluzione più facile da gestire.

Anche un'interfaccia utente (UI) centralizzata e una console di gestione unificata sono fondamentali per una risposta efficace ed efficiente agli incidenti. Le console separate per gli strumenti on-premise o erogati dal cloud offrono una gestione confusa e dispendiosa. Alcuni fornitori di soluzioni DLP più moderne continuano a usare un approccio basato su console multiple, che può confondere e complicare monitoraggio e gestione. Con Netskope One Data Security, tutte le violazioni vengono notificate in un'unica posizione, mentre il rilevamento dei dati sensibili e le attività di incident response vengono eseguite sempre in modo coerente e in tempo reale, assicurando risposte rapide ed efficaci alle potenziali minacce.

SUGGERIMENTO

Con un'interfaccia centralizzata e una console di gestione unificata, è più semplice tenere traccia di tutto e snellire il processo di incident response.

IN QUESTO CAPITOLO

- **Stabilire la priorità delle maggiori minacce alla sicurezza dei dati**
- **Identificare e affrontare le vulnerabilità dentro e fuori l'azienda**
- **Scegliere un fornitore e una soluzione affidabili**

Capitolo 5
Dieci punti (più o meno) per una transizione di successo verso la sicurezza dei dati unificata

Sostituire i sistemi tradizionali e consolidati, soprattutto nel caso delle soluzioni DLP può sembrare un'impresa ardua. L'iterazione in uso può essere il risultato di anni di processi complessi e a incastro. Togliere anche un solo elemento rischia di far crollare tutta la struttura, un po' come un castello di carte.

Ma niente panico! L'innovazione digitale è qualcosa per cui vale la pena cambiare, e non lo si deve fare da un giorno all'altro. Un passo alla volta, e con investimenti ben pianificati, è possibile ottenere una soluzione completa capace di proteggere le informazioni sensibili in tutte le piattaforme, on-premise e nel cloud.

In questo capitolo proponiamo una decina di punti da seguire per passare alla sicurezza dei dati unificata.

Valuta le tue esigenze in termini di sicurezza dei dati

Prenditi il tempo di valutare attentamente il contesto tecnologico dell'azienda: individua e comprendi quali dati proteggere, quali servizi e repository vengono usati per archiviare ed elaborare le informazioni sensibili, e come vengono usati tali servizi dai vari dipartimenti e dai dipendenti. Nello specifico, chiedi al team della sicurezza di individuare e valutare tutte le applicazioni aziendali, i servizi di posta elettronica, gli strumenti collaborativi, i percorsi di rete, le prassi di lavoro ibrido degli utenti, i dispositivi connessi e i processi aziendali per mappare i flussi di dati e stabilire come vengono condivise le informazioni tra i dipendenti o con i terzi.


SUGGERIMENTO

Non fermarti al team della sicurezza. Il CDO (*Chief Data Officer*), l'ufficio legale e le Risorse Umane sono tra le parti interessate che possono fornire chiarimenti sull'uso dei dati personali da parte dell'azienda.

Esamina tutte le categorie di dati salvati e qualsiasi transazione legata al trasferimento dei dati tra reti diverse. Scopri che priorità assegnare alla protezione dei vari tipi di dati all'interno dell'azienda. Questa fase può essere particolarmente vantaggiosa per le aziende che hanno bisogno di supporto per garantire la compliance normativa o che richiedono nuove soluzioni DLP a causa di sistemi tradizionali inefficienti.

Identifica e mitiga i rischi maggiori

Per valutare la transizione a una soluzione di protezione dei dati erogata dal cloud, stabilisci quali aree dell'attuale assetto tecnologico rappresentano il rischio più alto. Considera la condivisione accidentale dei dati, l'esfiltrazione dolosa e altre minacce informatiche tipiche degli ambienti cloud associate alle applicazioni SaaS, ai servizi di posta elettronica in cloud e IaaS.


SUGGERIMENTO

La soluzione leader di mercato Netskope CASB ha al centro la DLP per proteggere i dati sia nelle applicazioni cloud autorizzate dall'azienda sia nelle app non autorizzate (che continuano a essere usate, è inutile negarlo).

Scegli attentamente il fornitore di soluzioni di sicurezza dei dati

Assicurati di scegliere un fornitore capace di soddisfare le esigenze dell'azienda, attuali e future, in ogni singolo ambiente.

SUGGERIMENTO

Netskope è l'unico fornitore a offrire una protezione completa per tutte le esigenze di sicurezza sul cloud e oltre. Parliamo di protezione dei dati a riposo, in movimento e in uso in ambienti in cloud e on-premise, di protezione DLP su endpoint, servizi di posta elettronica e reti per il traffico web ed e-mail, nonché protezione DLP per SaaS, IaaS e applicazioni private. Questa copertura completa per tutti i trasferimenti di dati garantisce la massima visibilità sull'intero sistema aziendale, inclusi i percorsi più a rischio.

Valuta attentamente l'accuratezza delle capacità di ogni soluzione, come: quanti e quali tipi di file è in grado di analizzare, il riconoscimento dei formati di immagini e la copertura della più ampia varietà possibile di dati sensibili, inclusi identificativi internazionali e specifici per Paese. Valuta anche la capacità del sistema di tenere conto del maggior numero possibile di contesti di rischio e aziendali, e quindi di prendere automaticamente decisioni di incident response informate e adeguate a ogni uso dei dati sensibili.

In sostanza, evita approcci superficiali alla sicurezza dei dati che rischiano di creare ulteriori problemi anziché fornire soluzioni.

Proteggi i servizi di posta elettronica e le app collaborative

Scopri la forza della protezione della posta elettronica in cloud e delle applicazioni SaaS con Netskope One Data Security. Questa soluzione completa è progettata per mettere al sicuro tutte le informazioni sensibili dell'azienda, comprese le e-mail in uscita e le comunicazioni asincrone tramite app collaborative basate su SaaS, come Slack e Microsoft Teams. Grazie alle API (*Application Programming Interface*), alla protezione in tempo reale in linea, alla protezione per collaborazioni esterne e anche alla capacità di distinguere le istanze personali di servizi SaaS ed e-mail dalle istanze aziendali degli stessi servizi, puoi avere la certezza che i dati aziendali sono protetti in ogni circostanza. Con Netskope, puoi gestire la collaborazione e le comunicazione a mente serena.

Proteggi i servizi e-mail in cloud

Scopri la forza della protezione dei servizi di posta elettronica in cloud con Netskope One DLP. Questa soluzione DLP completa è progettata per proteggere tutte le informazioni sensibili dell'azienda da attacchi e condivisioni accidentali. Grazie alle API, alla protezione in tempo reale in linea e alla protezione delle informazioni scambiate tramite istanze di posta elettronica personali, puoi essere certo che i dati aziendali sono sempre protetti. Con Netskope, puoi gestire la migrazione dei servizi e-mail al cloud a mente serena.

Proteggi i dati in movimento

I dati trasferiti tra diverse posizioni e connessioni e tra diversi servizi e dispositivi (come reti domestiche, sedi aziendali, uffici remoti, dispositivi aziendali e personali) possono essere difficili da gestire e proteggere. Le tradizionali soluzioni DLP collegate a server proxy non sono sempre sufficienti quando si tratta di dati in movimento.

SUGGERIMENTO

Netskope offre la sicurezza dei dati unificata attraverso la piattaforma Netskope One, che protegge la trasmissione di dati sensibili tra sedi on-premise e/o sul cloud. Questo approccio offre i massimi livelli di sicurezza per le transazioni dei dati, anche grazie a tutti i vantaggi della filosofia Zero Trust e dell'approfondito contesto di rischio, senza il problema di dover gestire oscure configurazioni hardware. L'innovativa soluzione Netskope One Data Security garantisce la sicurezza dei dati sempre e ovunque.

Proteggi i dati sui dispositivi endpoint dei dipendenti

Anche se archivi nel cloud sempre più dati, devi assicurarti che i file sensibili non vadano persi o rubati su endpoint non sempre (o per niente) connessi a una rete aziendale.

SUGGERIMENTO

Non importa se i dati vengono creati sull'endpoint stesso o scaricati dal cloud: Netskope One DLP è la soluzione ideale. Questa soluzione endpoint ultraleggera offre tutte le capacità DLP avanzate, come classificatori basati su machine learning, riconoscimento ottico dei caratteri, fingerprint dei file, corrispondenza esatta dei dati e altro ancora. E il tutto con un uso ridotto di risorse, perché la soluzione è

erogata dal cloud. È in grado di gestire svariati casi d'uso, tra cui il rilevamento di dati trasferiti via USB, e mette a disposizione funzioni di protezione dei dispositivi USB e altre policy di controllo a livello di dispositivo per assicurare che i dati sensibili siano sempre al sicuro, indipendentemente da dove si connettono gli utenti.

Pensa al futuro tenendo solo gli strumenti che funzionano davvero

Se hai recentemente investito in una soluzione DLP offerta da un fornitore di servizi cloud o SaaS, nel breve periodo conviene senz'altro mantenere le funzioni acquistate. Ad esempio, se la protezione di cui hai bisogno per la suite di applicazioni in uso è già garantita, è inutile pensare di cambiare nell'immediato.

ATTENZIONE

Ma fai attenzione a quando gestisci troppe policy isolate e scollegate tra loro. Se hai in mente di ampliare la protezione dei dati a più cloud e applicazioni SaaS, rischi di trovarti con troppe console e policy differenti.

SUGGERIMENTO

Netskope One DLP propone una soluzione più semplice: un'unica console con policy coerenti in grado di proteggere i dati indipendentemente dal luogo di accesso o archiviazione.

Accedi a una protezione completa

Netskope One offre un approccio moderno alla sicurezza dei dati, più efficiente ed efficace che mai. La soluzione si avvale di avanzate tecnologie di rilevamento, come machine learning, fingerprint dei dati e riconoscimento delle immagini su una scala senza precedenti e a pieno potenziale persino sugli endpoint, perché la capacità di elaborazione viene erogata dal cloud. La singola console con policy unificate semplifica la gestione delle esigenze di protezione dei dati di tutta l'azienda. La raccolta e l'analisi delle informazioni contestuali e sui rischi correlate a utenti, dispositivi, dati, reti, cloud e comportamenti consente a Netskope One DLP di valutare ogni interazione che contiene dati sensibili, per adattare dinamicamente la risposta a qualsiasi singola violazione delle policy. Questo nuovo approccio supporta una collaborazione sicura e le moderne prassi di condivisione dei dati, minimizza i falsi positivi e genera risultati più accurati sul fronte della protezione dei dati, il tutto senza pregiudicare la produttività.

RICORDA

Netskope One Data Security è integrato in modo nativo nella soluzione completa Netskope One SSE, quindi è sempre consapevole dei rischi, dei comportamenti e delle vulnerabilità della sicurezza in azienda. Grazie alla piena integrazione di Netskope One nella soluzione Netskope SSE, le aziende sono sempre consapevoli dei rischi aziendali, dei comportamenti e delle vulnerabilità di sicurezza.

Mantieni le conoscenze istituzionali

Il passaggio a una nuova soluzione DLP erogata dal cloud può sembrare faticosissimo, ma non deve esserlo per forza. Affidati all'esperienza e alle competenze delle persone che si sono occupate di gestire il tuo sistema DLP tradizionale, compresi i policy administrator e il team di incident response. Le loro conoscenze possono aiutarti a garantire la replica delle best practice durante il passaggio a un sistema in cloud, oltre a permettere all'azienda di soddisfare le aspettative sul piano tecnologico generando profili di compliance alle policy e sviluppando nuovi flusso di lavoro per la rettifica degli incidenti.

SUGGERIMENTO

Netskope One DLP contribuisce alla riduzione dei requisiti a carico del team DLP, che potrà quindi dedicare meno tempo alla gestione degli incidenti per focalizzarsi maggiormente sulle iniziative proattive mirate alla sicurezza dell'azienda.

Preferisci la maturità al clamore

Le conoscenze tecniche, da sole, non assicurano la buona riuscita. Dallo sviluppo di metriche per i vertici aziendali fino all'elaborazione di linee guida e attività per il personale, sono tanti gli aspetti da considerare. Affidati al team di assistenza del fornitore per strutturare il percorso da seguire, liberare il potenziale dell'innovazione e fare sì che i tuoi sforzi non siano stati inutili!

netskope

Sicurezza Moderna e Network Performance.

Nessun Compromesso.

Proteggiamo i dati, eliminiamo la complessità e miglioriamo la User Experience.

Scopri come

Proteggi i tuoi dati ovunque si trovano e vengono trasferiti, minimizzando gli attriti aziendali

La rapida adozione del cloud e la tendenza verso il lavoro remoto hanno reso inadeguati sistemi di protezione dei dati un tempo considerati innovativi. Le misure di sicurezza dei dati devono proteggere i dati con coerenza sempre e ovunque. La soluzione ideale per una sicurezza dei dati moderna deve essere sviluppata appositamente per il cloud, e non riadattata in base a nuovi casi d'uso. Deve applicare tecniche Zero Trust, ridurre la complessità e garantire l'applicazione coerente delle policy ovunque, senza causare eccessivi attriti aziendali né sovraccaricare il personale addetto alla sicurezza con falsi positivi.

Qui scoprirai come...

- Valutare l'attuale sicurezza dei tuoi dati
- Implementare un approccio unificato che dà priorità al cloud
- Gestire le operazioni di sicurezza da un unico pannello di controllo
- Bloccare le fughe di dati non autorizzate prima che si verifichino
- Minimizzare i falsi positivi per ridurre gli attriti di business
- Applicare i principi Zero Trust per massimizzare la protezione

netskope

Sul sito Dummies.com®
puoi trovare video, immagini dettagliate, guide... o semplicemente fare acquisti!

ISBN: 978-1-394-42063-6

9 781394 420636

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.