IMPARARE DIVENTA FACILE

Edizione speciale Netskope

Soluzioni moderne di Data Loss Prevention (DLP)

for dummies®

- Scopri le tecniche DLP moderne
- Usa i principi Zero Trust per proteggere i dati in movimento
- Ottieni una migliore protezione del cloud

Edizione targata

netskope

Carmine Clementelli

Informazioni su Netskope

Netskope, leader globale delle soluzioni SASE, sta ridefinendo la protezione di cloud, dati e reti per aiutare le aziende ad applicare principi Zero Trust alla protezione delle informazioni. La sua piattaforma, facile e veloce da usare, fornisce un accesso ottimizzato e una protezione in tempo reale per utenti, dispositivi e dati ovunque. Netskope aiuta i clienti a ridurre il rischio, accelerare le prestazioni e ottenere una visibilità senza precedenti su qualsiasi attività svolta nel cloud, su web o in applicazioni private. Migliaia di clienti, tra cui più di 25 aziende Fortune 100, si affidano a Netskope e alla sua potente rete NewEdge per rispondere a rischi e minacce in continua evoluzione, a nuovi requisiti normativi e a cambiamenti a livello di tecnologia, reti e organizzazione. Per scoprire come Netskope aiuta i clienti a prepararsi alla transizione a una soluzione SASE, visita netskope.come

Desideriamo ringraziare tutti coloro che hanno contribuito alla pubblicazione di questo volume:

In Netskope: Amanda Anderson, Chad Berndtson, Jason Clark, Scott Hogrefe, Kathy Jacobsen, Naveen Palavalli, Stephenie Pang, Lauren Polito, Carolyn Robinson, Neil Thacker

In Evolved Media: David Penick, Karen Queen, Evan Sirof, Lauren Wagner, Dan Woods

Soluzioni moderne di Data Loss Prevention (DLP)

Edizione speciale Netskope

by Carmine Clementelli

for dummies®

Soluzioni moderne di Data Loss Prevention (DLP) For Dummies®, Edizione speciale Netskope

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

ISBN 978-1-394-20800-5 (pbk); ISBN 978-1-394-20801-2 (ebk)

Per informazioni generali sugli altri nostri prodotti e servizi o su come realizzare un libro *For Dummies* personalizzato per la propria attività o azienda, contattare il nostro reparto di Business Development negli Stati Uniti chiamando il numero 877-409-4177, scrivendo un'e-mail all'indirizzo info@dummies.biz, o visitando www.wiley.com/go/custompub. Per informazioni sulle licenze relative al marchio For Dummies per prodotti o servizi, contattare BrandedRights&Licenses@Wiley.com.

Ringraziamenti dell'editore

Fra coloro che hanno contribuito alla pubblicazione di questo libro, si ringraziano:

Editore di progetto: Elizabeth Kuball
Direttore acquisizioni: Traci Martin
Responsabile editoriale: Rev Mengle
Client Account Manager: Jeremith Coward
Direttore di produzione: Mohammed Zafar Ali
Assistenza speciale: Nicole Sholly

Introduzione

Il concetto di "protezione dei dati" non è affatto nuovo nel mondo della sicurezza informatica, ma nell'ultimo decennio le aspettative verso i sistemi di protezione tradizionali si sono nettamente evolute. 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 la buona notizia) e di difficoltà sul fronte della sicurezza, soprattutto a livello di protezione dei dati (la 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. La protezione dei dati rappresenta oggi una componente fondamentale dei requisiti di compliance, con regolamenti di settore e norme in materia di privacy che specificano le responsabilità delle aziende e introducono sanzioni significative in caso di inadempienza.

Le aziende devono adottare un approccio nuovo e applicare le policy di protezione dei dati in modo coerente ovunque vengano trasferite le informazioni. In un mondo ideale, la protezione dei dati sostiene gli obiettivi commerciali e al tempo stesso tutela l'azienda; ma la gestione delle policy e degli strumenti di protezione si rivela spesso complessa e costosa. Alle aziende servono soluzioni in grado di semplificare il rispetto delle policy pur garantendo la loro efficacia. Una possibile risposta è data da una nuova generazione di soluzioni DLP (*Data Loss Prevention*) erogate dal cloud, che sono meno complesse, altamente scalabili e più efficienti in termini di costi. Esse hanno la capacità di proteggere i dati in modo più affidabile e accurato e di ridurre 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 volume

Questo libro può preparati a prendere decisioni informate su come valutare l'attuale approccio alla protezione dei dati dell'azienda ed esplorare le nuove soluzioni disponibili per trovare quella più adatta ai tuoi bisogni, basata sui principi Zero Trust per applicare i parametri di sicurezza in modo coerente e a seconda del contesto. Spiegando come funzionano i moderni sistemi DLP erogati dal cloud, l'autore si mantiene a debita distanza dagli slogan promozionali per aiutarti a identificare 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.

Le icone nel 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 semplificarti la vita.

RICORDA

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

COSE DA TECNICI

Si tratta di informazioni molto tecniche che puoi anche permetterti di saltare.

ATTENZIONE

Leggi con attenzione per evitare potenziali grattacapi in futuro.

Oltre questo volume

Le informazioni che abbiamo fornito non bastano? 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 significa all'atto pratico "protezione dei dati"**
- **Imparare cosa si intende per *Data Loss Prevention (DLP)***
- **Valutare perché le soluzioni DLP tradizionali non sono più una strada percorribile**
- **Passare a una strategia *cloud-first* adottando una soluzione DLP all'avanguardia**
- **Sfatare i miti più comuni sulle soluzioni DLP**

Capitolo 1
I dati sensibili sono ovunque eppure è sempre più difficile trovarli

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

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, di patenti di guida, informazioni sanitarie e indirizzi postali personali;

- proprietà intellettuale 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. Molte aziende, soprattutto dopo la pandemia di COVID-19, hanno un ambiente di lavoro ibrido.

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 le informazioni su piattaforme multiple, il che le rende accessibili praticamente da qualsiasi dispositivo in remoto. Con questo aumento esponenziale della quantità, della varietà e della velocità di trasferimento delle informazioni, diventa sempre più difficile identificare e tutelare 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 nuove minacce.

Uno tsunami di dati

Secondo IDC, entro il 2025 il mondo sarà sommerso da ben 181 zettabyte di dati! In grandissima parte verrano creati e salvati direttamente nel cloud, e ogni anno saranno sempre di più. I sistemi di protezione dei dati e i relativi operatori si trovano quindi ad affrontare sfide come:

- **Troppe 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 numeri di carte d'identità, carte di credito, piani finanziari, conti correnti, contratti, dichiarazioni fiscali, password, dati sanitari protetti,

e-mail confidenziali e informazioni sul genere. Le categorie di dati sensibili possono cambiare da un Paese all'altro.

- **Troppi formati e tipi di dati:** PDF, immagini (come JPG, PNG e BMP), 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.
- **Troppo 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. Il motivo? 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 protezione dei dati non si ferma "solo" ai dati

Le aziende hanno bisogno di strategie automatizzate in grado di identificare, monitorare e tutelare efficacemente le informazioni più importanti. Allo stesso tempo la protezione dei dati si trova sempre di fronte a nuove sfide, che a loro volta aggiungono ulteriori livelli di complessità. Tra queste

- **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 di informazioni sensibili 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 manda i dati su un'app di archiviazione personale di tipo *Software as a Service* (SaaS) o che usa l'istanza personale di un

account di posta elettronica aziendale (come un account Gmail personale invece di quello di lavoro).

- *Esposizione accidentale:* un dipendente che inavvertitamente manda 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, compresi 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 o a esso sconosciute o 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. Il panorama è cambiato drasticamente da 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 varietà di ambienti digitali o 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 dei regolamenti e le sanzioni sempre più severe poste dalle leggi sulla privacy o i rischi di incorrere in azioni legali, ogni azienda dalla più

grande alla più piccola è sotto pressione per garantire il rispetto degli standard e la tutela dei dati sensibili. 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 a un ampio ventaglio di leggi e regolamenti, 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 in tutto il mondo che hanno introdotto norme sulla privacy, ci sono Brasile, Singapore, Giappone 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 con le competenze necessarie per attuare complessi programmi di protezione dei dati sono merce rara. Le tecnologie per la protezione 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 una soluzione DLP e a cosa serve?

Le tecnologie di sicurezza DLP sono sistemi progettati per identificare e proteggere automaticamente l'archiviazione, il flusso e l'uso di dati sensibili distribuiti su tutte le reti, gli utenti e i servizi di un'azienda. Questi sistemi vengono implementati 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 oggi le tecnologie DLP tradizionali sono tristemente inadeguate

Le soluzioni DLP tradizionali vengono usate da oltre dieci anni per proteggere i 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 fornire 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 per quello che sono stati progettati, ma oggi sono chiamati a fare tutt'altro lavoro, e cioè garantire la sicurezza di dati archiviati nel 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 distribuire 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 smartworking, le applicazioni cloud e la flessibilità di usare i dispositivi personali.

Le tecnologie DLP tradizionali richiedono poi lunghi aggiornamenti software e continue correzioni che interrompono concretamente le normali attività aziendali. Proprio per queste interruzioni, spesso le aziende decidono di evitare gli upgrade, trovandosi poi con versioni

vecchie di mesi o anni rispetto alle più recenti. Così, non usano protezioni aggiornate in linea con i requisiti più recenti in termini di gestione dei dati, conformità e contenimento dei rischi.

Senza gli aggiornamenti e i 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 il modo "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. Poco fa abbiamo accennato alla pressione dei falsi positivi sui team di sicurezza, ma vale la pena approfondire l'argomento.

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. Gli specialisti si ritrovano con una miriade di allarmi che spesso non corrispondono neppure a problemi effettivi, e che non forniscono alcun contesto per stabilire un livello di rischio. In pratica, gli allarmi vengono generati con molto ritardo rispetto all'incidente. Quindi, oltre a non avere contesto, i team devono anche risalire a eventi passati che spesso i diretti responsabili non ricordano nemmeno. 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 ignorarle se vogliono solo 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*, 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*), in modo da facilitare la gestione degli allarmi e consentire interventi più rapidi. Tuttavia, se il sistema DLP non è accurato, non permette di individuare il contesto di business e il livello di rischio, e i modelli UEBA non potranno funzionare bene.

Per garantire una protezione efficace dei dati sensibili, un sistema DLP deve essere integrato e automatizzato in modo da monitorare e verificare costantemente l'identità dei singoli individui e dispositivi autorizzati, i relativi comportamenti, come collaborano tra loro e come condividono dati all'esterno, le applicazioni usate e il loro livello di rischio, oltre a molti altri fattori contestuali. Questo approccio *Zero Trust* (v. Capitolo 3) permette di applicare precisi 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. Un tale approccio non perturba le moderne prassi di lavoro ma le agevola rendendole più sicure.

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

La tecnologia DLP tradizionale è fondata su un modello di sicurezza sviluppato per proteggere solo i dati archiviati nella rete aziendale e in ambienti gestiti. Un modello simile non è più adatto all'era attuale, in cui i dati sono dislocati in moltissime applicazioni cloud e accessibili da utenti e dispositivi al di fuori della rete aziendale. Inoltre, non è sempre detto che i sistemi DLP tradizionali siano progettati per integrarsi con l'ampia gamma di servizi e infrastrutture cloud attualmente in uso, il che rende difficile o impossibile fornire una protezione completa per i dati nel cloud.

Aggiungendo ai sistemi DLP on-premise altre tecnologie, come le soluzioni CASB (*Cloud Access Security Broker*) o SWG (*Secure Web Gateway*) in cloud, è possibile aumentare la copertura per i repository cloud, ma non si superano le limitazioni intrinseche dei sistemi tradizionali. In questo modo, i team devono districarsi tra più console di gestione e policy di sicurezza scorrelate, due effetti collaterali molto comuni quando si aggiungono strumenti CASB e SWG a sistemi DLP tradizionali.

In altre parole, aggiungere tecnologie a un approccio DLP obsoleto non serve a mettere in sicurezza il cloud ma solo ad aumentare la complessità. Un sistema DLP 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. Le soluzioni DLP tradizionali sono on-premise. Punto.

RICORDA

Per proteggere i dati negli ambienti cloud, i sistemi DLP tradizionali devono essere ben integrati con soluzioni di *cloud security*. I dati nel cloud hanno bisogno di meccanismi di protezione ad hoc.

COSE DA TECNICI

Oggi, la maggior parte delle aziende usa due soluzioni di *cloud security* solitamente integrate in un sistema DLP tradizionali, e cioè: CASB per il traffico su applicazioni cloud e SWG per il traffico web generato dai dipendenti che lavorano da remoto o da altre sedi aziendali. Anche se queste soluzioni sono state appositamente progettate per il cloud, spesso hanno limitate capacità di protezione dei dati. La speranza è che tali integrazioni forniscano 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. Ma c'è un problema: integrare questo tipo di soluzioni è estremamente difficile, e richiede reindirizzamenti del traffico di rete basati sul complicatissimo protocollo ICAP (*Internet Content Adaptation Protocol*), di cui per nostra fortuna non parleremo qui.

E anche una volta terminata l'integrazione, questo approccio non risulta sostenibile. Innanzitutto, le soluzioni CASB usano API (*Application Programming Interface*) per collegarsi ad applicazioni cloud aziendali come Microsoft 365, Salesforce, Slack, Zoom, Teams, Google Workspace, Amazon Web Services (AWS) e Box. Le API servono a fornire al sistema DLP tradizionali la necessaria visibilità sulle applicazioni cloud in questione. Ad esempio, se sono stati salvati dati sensibili in Salesforce, il DLP è in grado di riconoscerli e garantire la protezione. I CASB si servono inoltre di funzioni di

rilevamento per monitorare attività di upload e download di dati in migliaia di applicazioni SaaS.

Poi c'è il problema di consolidare le policy di sicurezza usate da sistemi locali e su cloud perché spesso le soluzioni CASB non sono in grado di replicare i parametri come fanno i sistemi DLP tradizionali. Proprio a causa di questa differenza, le console di gestione e i criteri di sicurezza risultano frammentati e non sincronizzati.

Il problema di un'architettura simile è che integrare tecnologie DLP on-premise con applicazioni su cloud attraverso una soluzione CASB genera anche un ritardo, chiamato *latenza*. Questa latenza implica che, anche quando il sistema DLP tradizionali identifica una violazione dei dati in un ambiente cloud, serviranno minuti, ore o addirittura di più per innescare una risposta. Facciamo un esempio: c'è stata una violazione che è stata identificata, ma non fermata 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 (il CASB) si occupa di servizi cloud, mentre l'altro (DLP tradizionali) è una complessa architettura on-premise fatta di componenti hardware e software. Il risultato è un sistema di difesa fragile, facile da aggirare, che genera parecchia latenza ed è estremamente complesso da ottimizzare e mantenere. Meglio eliminare la complessità e semplificare l'intero processo, riducendo il rischio di altri problemi.

Essere vincolati a un'architettura on-premise, priva dei mezzi per scalare in tempi rapidi, limita notevolmente l'efficacia delle tecnologie DLP tradizionali negli ambienti cloud. Un approccio come questo non è più sostenibile.

RICORDA

Per assicurare l'efficacia dei sistemi DLP, bisogna spostare l'attenzione dal perimetro esterno del dataset ai dati in sé e a dove e come viaggiano. Le aziende non possono più permettersi di affidarsi a strategie basate su sistemi DLP tradizionali se vogliono proteggere efficacemente le informazioni archiviate nel cloud.

DLP per l'era del cloud

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 DLP deve passare a una strategia *cloud-first* in modo da assicurare più copertura, efficienza e scalabilità, oltre a solide capacità di elaborazione e misure di prevenzione del rischio ancora più efficaci. Con un modello DLP rinnovato, le aziende moderne possono gestire al meglio le sfide poste dal lavoro ibrido e dotarsi di strumenti indispensabili per il futuro. Rinnovare l'architettura DLP dell'azienda non è un'impresa da poco, ma con il continuo evolversi dei rischi e i progressi delle soluzioni DLP *cloud-ready*, è il momento giusto per prendere in considerazione l'idea.

Le soluzioni di Cloud DLP non richiedono implementazioni complesse, ma solo l'attivazione di un servizio cloud. Non ci sono una miriade di componenti e soluzioni software da aggiornare e mantenere manualmente, né database DLP da gestire o esperti da assumere. E sarà possibile dire addio ai server DLP, che prima o poi diventano obsoleti e devono essere cambiati, o ai proxy hardware da aggiornare.

Le piattaforme di protezione 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 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 basata sul cloud collegata ad alcuna infrastruttura e programma preesistente, il sistema DLP riceve sempre aggiornamenti in tempo reale ovunque. Questo approccio è molto più efficiente per proteggere i dati sensibili della tua organizzazione.

Miti da sfatare

Quando si parla di servizi DLP *cloud-ready*, si sa di entrare in un mercato pieno di paroloni, slogan e promesse irrealistiche, con utenti bombardati di informazioni e spesso confusi sulle opzioni possibili. Ma la realtà è che le soluzioni DLP non sono tutte uguali. In

questo volume, spiegherò le differenze tra fatti e stratagemmi promozionali analizzando le caratteristiche e funzionalità più importanti dei vari sistemi.

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

Mito: le soluzioni DLP più recenti sono anche le migliori

Realtà: al momento di scegliere un programma di protezione 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 e lungo il percorso ha sviluppato tutta una serie di nuove funzioni. Per investire in un programma completo di protezione 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: i sistemi DLP tradizionali non erano accurati

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 identificare e impedire il trasferimento non autorizzato di informazioni sensibili.

Il problema non è l'accuratezza quanto il numero di falsi positivi, come ho 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. 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: le soluzioni DLP devono offrire solo un livello di protezione "accettabile"

Realtà: quando si tratta di garantire la sicurezza dei dati aziendali, meglio non prendere scorciatoie ed evitare soluzioni basate su cloud che promettono livelli di protezione appena sufficienti . Ci si potrebbe infatti ritrovare con un set di funzioni ridotto o un'attenzione limitata ai soli vettori di attacco e alle categorie di dati superficiali, con il rischio di esporre le informazioni ad attività dannose, falsi positivi e imprecisioni nel rilevamento.

Il mio consiglio è investire in un sistema DLP basato su cloud che assicura un'elevata precisione di rilevamento dei dati, offre livelli di sicurezza aggiuntivi e una protezione completa contro possibili minacce a danno dei dati aziendali o di altro materiale riservato. Meglio non essere troppo disinvolti quando si parla di protezione dei dati e investire nel sistema DLP giusto per massimizzare la sicurezza e le prestazioni.

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 basata su cloud deve essere superiore ai sistemi 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.

RICORDA

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

Mito: un pacchetto di soluzioni di protezione dei dati è efficace quanto una soluzione completa e integrata

Realtà: in fatto di protezione dei dati, può sembrare logico affidarsi a iniziative e programmi di sicurezza che raggruppano 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. Presto o tardi, però, questi programmi di protezione multiservizio sono destinati a diventare insufficienti. 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 protezione dei dati saranno costretti a fare i conti con molteplici console di gestione e parametri di sicurezza scoordinati. 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 che i dati sono sempre vulnerabili a eventuali attacchi.

Per tutelare efficacemente l'azienda, è bene puntare su soluzioni integrate che offrono funzioni complete, in grado di coprire tutte le potenziali aree di rischio su servizi cloud, sistemi locali, servizi di posta elettronica ed endpoint e ottenere così una protezione completa per molti tipi di dati e controlli.

IN QUESTO CAPITOLO

- **Capire le sfide a carico dei sistemi DLP tradizionali**
- **Prepararsi a scalare le soluzioni in vista di una crescita o di cambiamenti futuri**
- **Conoscere le realtà e le limitazioni dei sistemi DLP in cloud**
- **Comprendere in che modo i sistemi 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. In questo capitolo spieghiamo perché mettere in esercizio una protezione dei dati completa in tutta l'azienda porta risultati nell'immediato e vantaggi strategici nel lungo periodo.

Aziende senza confini

Una decina di anni fa, il concetto di azienda era fondamentalmente definito dai confini fisici di un edificio o una sede, al cui interno si trovavano dipendenti, attrezzature e risorse. Ma con il tempo si è evoluto per riflettere la natura mutevole delle tecnologie e del business; oggi, l'azienda non è più limitata a un ambiente fisico.

Con la diffusione dello smart-working, è probabile che le informazioni sensibili viaggino anche sulle reti domestiche dei dipendenti. Con l'aumento dei servizi cloud, i dati sono sparpagliati in ambienti diversi, tra cui applicazioni SaaS come Microsoft 365 e Salesforce, nonché in conversazioni online su app collaborative come Slack e Microsoft Teams (v. Figura 2-1). L'azienda ora include i numerosi endpoint usati dai dipendenti per connettersi alle risorse aziendali, oltre alle migliaia di app cloud approvate (o anche no).


ATTENZIONE

Proteggere i dati sensibili vuol dire saperli riconoscere e sapere dove vengono salvati. Sapere che ci sono ma non dove risiedono e viaggiano, non serve a proteggerli.


RICORDA

Per garantire che tutti i dati sensibili vengano individuati e protetti in qualsiasi ambiente, bisogna puntare su un approccio completo. Questo vuol dire evitare lacune o angoli ciechi che potrebbero mettere i dati a rischio di esfiltrazione o esposizione accidentale.

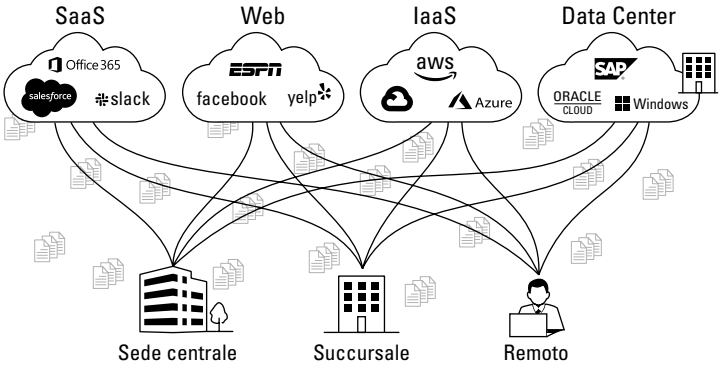

FIGURA 2-1: Nelle moderne aziende altamente distribuite, i dati risiedono e confluiscono su molti ambienti nuovi.

Le difficoltà associate all'evoluzione dei sistemi DLP

Come discusso nel Capitolo 1, i sistemi DLP si concentravano soprattutto sulla protezione dei dati archiviati *all'interno* dei data center aziendali. Oggi, però, è importante proteggere i dati ovunque possano essere trasmessi, ossia 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 le informazioni vengono trasferite e archiviate, puntando l'attenzione sui dati piuttosto che sugli ambienti in cui vengono generati e mantenuti, è possibile ottenere notevoli vantaggi in termini di flessibilità ed efficacia. Un po' come una squadra di calcio che passa da una difesa a zona a una difesa a uomo. Come vedremo nelle pagine successive, adottando un approccio completo è possibile proteggere le informazioni sensibili ed evitare che finiscano nelle mani sbagliate.

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 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 richiede una soluzione DLP completa e flessibile, in grado di adattarsi costantemente alle esigenze mutevoli delle aziende altamente distribuite.

Nei paragrafi seguenti, esamineremo 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 poi la popolarità di questi strumenti è cresciuta in modo sostanziale. Oggi non è insolito per le aziende usare centinaia di applicazioni SaaS approvate, e per i dipendenti usare migliaia di app aggiuntive di cui l'azienda non è neppure a conoscenza.

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 a garantire la continua efficacia ed efficienza dei sistemi di fronte a 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 Slack, Teams e Zoom, o di posta elettronica in cloud come Gmail. Possono anche essere sotto forma di immagini, fotografie e screenshot: le catture di informazioni importanti vengono usate 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 "Un moderno DLP in azione", più avanti in questo capitolo, spiega nel dettaglio come funzionano i sistemi DLP. Per il momento, ricordiamo che la funzionalità di base di un sistema DLP consiste nel rilevare e proteggere i dati sensibili.

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

Con le applicazioni cloud e l'espansione delle attività in nuove sedi, l'uso dei sistemi DLP tradizionali è diventato sempre più ingestibile in quanto sono stati progettati per essere installati e gestiti in loco, e cioè duplicati e reinstallati in ogni singola sede o ufficio remoto. Tutto questo aggiunge un notevole livello di complessità e richiede molte risorse, in termini di apparecchiature hardware, manutenzione e personale specializzato. Inoltre, 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.

Proprio come quando saltiamo un aggiornamento dello smartphone o del laptop per paura di compromettere la funzionalità della nostra app preferita o per evitare altri problemi, non c'è da stupirsi se le aziende preferiscono tenersi strette le vecchie versioni dei software DLP piuttosto che aggiornarle su innumerevoli server e uffici remoti, nonché che sulle migliaia di dispositivi dei dipendenti. Decisamente meglio che tentare la sorte!

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, poiché 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 *machine learning* (ML) e la corrispondenza esatta dei dati (vedi paragrafo seguente). 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, di cui abbiamo già parlato nel Capitolo 1, è l'inaccuratezza dei sistemi DLP tradizionali. Ma il problema vero non è l'accuratezza, o almeno non è quello principale. Il problema principale sono i falsi positivi (già discussi nel Capitolo 1), dovuti soprattutto all'assenza di contesto. Certo, 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 possono tenere il passo ed è naturale che l'accuratezza non sia più quella di una volta. Ma il vero problema 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 fondamentale per lavorare, queste false segnalazioni sono diventate troppe.

È importante che la soluzione DLP non introduca problemi per l'azienda né interrompa 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 principali problemi dei sistemi DLP tradizionali, ma lo sono per le soluzioni su cloud meno mature. Gli aspetti da considerare sono due:

- Se le funzioni di rilevamento sono inaccurate possono portare a identificare e proteggere troppi dati non sensibili, con il rischio di compromettere comunicazioni legittime.
- Se mancano metodi per identificare i dati effettivamente sensibili, possono rimanere esclusi dal rilevamento tipi di file specifici (come immagini o formati compressi) o determinate informazioni (ad es. numeri di passaporto, informazioni sanitarie, coordinate bancarie o carte d'identità nazionali), perché il sistema non ha la capacità di identificarli.

RICORDA

Per mantenere la fiducia, i sistemi DLP devono essere accurati e precisi, segnalando e bloccando solo i trasferimenti dannosi senza generare troppi falsi positivi.

Ingrediente principale n° 1: 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 (*regex*); sono uno strumento utile che aiuta i sistemi DLP a riconoscere automaticamente specifici tipi di dati 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. 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 (Word, 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. il Capitolo 1).
- È essenziale avere il 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 con precisione e segnalare informazioni potenzialmente sensibili, indipendentemente dallo stato, dalla regione e dal Paese in cui si trovano.

Ingrediente principale n° 2: Corrispondenza esatta dei dati (EDM)

L'EDM è un modo per trovare specifiche informazioni strutturate a partire da fonti come fogli di calcolo e database. Esso permette 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 suo codice fiscale, il suo indirizzo e altri codici identificativi. 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 persino per le informazioni sanitarie, i prodotti o informazioni sui prezzi. 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.

Ingrediente principale n° 3: 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 protezione dei dati. Oggi, gli utenti scattano facilmente fotografie di documenti, moduli, carte d'identità, lavagne e di altre fotografie. 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 più comuni tipi di file e documenti (come carte di credito, moduli fiscali, accordi di non divulgazione, moduli per fusioni e acquisizioni e brevetti), senza necessariamente

estrarre 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 considerare anche il 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 di e-mail 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.

Ingrediente principale n° 4: 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. 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. In altre parole, devono *capire il contesto*. Questa agilità permette di proteggere efficacemente i dati sensibili, minimizzare i rischi di violazione dei dati e garantire la conformità alle normative senza alcun impatto negativo 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 possono essere usate per identificare con precisione le circostanze specifiche dell'accesso di un utente a dati sensibili, il contesto aziendale e i potenziali rischi connessi a tale azione, per poi stabilire il livello di accesso e la risposta più adatti; il tutto sulla base di fattori come l'identità, la posizione e il comportamento della persona, ma anche la sicurezza del dispositivo, l'affidabilità della rete, la reputazione dell'applicazione usata, la destinazione finale di un trasferimento di dati e così via.

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.

Ciò 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 permette al sistema DLP di fare scelte informate su quando autorizzare o meno le attività legate ai dati.

RICORDA

Lavorare con soluzioni di sicurezza integrate, in associazione a tecnologie di protezione dei dati, è la differenza tra uno *strumento* e una *piattaforma* di protezione dei dati.

Soluzione DLP moderna 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:

- **identificare i dati sensibili ovunque risiedano e vengano trasferiti:**
  - *Dati in movimento*, ossia 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*, cioè i dati usati attivamente, anche per collaborazioni, e che, ad esempio, vengono trasferiti su periferiche USB, stampati o inviati via fax (esistono ancora i fax?!).
- **monitorare l'ambiente dei dati** per rilevare chi accede alle informazioni e come vengono usate. Monitorando le azioni, il sistema può individuare incidenti (come la condivisione non autorizzata di informazioni riservate) che potrebbero violare le policy aziendali 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 download massivi sospetti di grandi quantità di file), assicurando di identificare e correggere tempestivamente le potenziali violazioni di sicurezza.
- **intervenire automaticamente per attuare le 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.
- **educare gli utenti** visualizzando automaticamente notifiche sulle violazioni e spiegando perché una determinata azione è un comportamento a rischio, e allo stesso tempo promuovere prassi di gestione dei dati sicure. 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 buona

soluzione DLP deve avvisare gli utenti immediatamente, senza ritardo, 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 abbiamo detto in precedenza, 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, e molte altre affrontate nei paragrafi precedenti, hanno intaccato la popolarità delle soluzioni DLP tradizionali, spingendo molte aziende a cercare alternative. Ora che i dati vengono trasferiti sempre più sul cloud, servono sempre più sistemi DLP in cloud capaci di riconoscere i cambiamenti a livello dei contesti e dei rischi associati 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 il cambiare dei rischi e del contesto.

IN QUESTO CAPITOLO

- **Capire come le vecchie soluzioni di protezione dei dati possono compromettere le attività aziendali**
- **Scoprire i tipi di contesto delle informazioni 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 di Zero Trust nelle soluzioni DLP moderne

Un concetto chiave nel campo della sicurezza informatica (DLP 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, siano 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 bensì 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 autorizzare l'accesso ai dati sensibili o un certo uso degli stessi. Anche se un dipendente è già stato autorizzato in precedenza, deve essere sottoposto a una

valutazione accurata, che può includere la verifica dell'identità, il controllo del dispositivo e della connessione di rete, un esame dei rischi correlati alle applicazioni a cui tenta di accedere e il monitoraggio del suo comportamento per accertarsi che sia *sempre* 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.

La strategia Zero Trust punta a creare un ambiente sicuro e controllato per accedere ai dati e trasferirli, riducendo il rischio di violazioni e tutelando i dati sensibili. Per farlo, implementa rigidi controlli degli accessi, monitora e verifica su base continuativa le azioni degli utenti, i rischi contestuali e i comportamenti. Nei sistemi DLP, un modello di sicurezza Zero Trust aiuta a minimizzare i rischi di violazione dei dati, offre risultati più accurati in termini di protezione dei dati e ottimizza i cicli di *incident response*, sulla base del contesto e dei rischi dell'azienda. Concedendo l'accesso e l'uso sicuro dei dati sensibili solo agli autorizzati, e impedendo qualsiasi tentativo di accesso o trasferimento delle informazioni pericoloso, sospetto, disattento o rischioso, le aziende possono proteggere meglio le proprie risorse.

I rischi associati ai sistemi di sicurezza obsoleti

I sistemi DLP sono stati creati per impedire la fuga di informazioni sensibili dall'azienda. Le versioni tradizionali gestiscono un numero limitato di scenari; il loro scopo principale è identificare i dati sensibili e mantenerli dentro l'azienda, usando un approccio basato sul perimetro che tiene sotto controllo il flusso di dati in entrata e in uscita dalla rete aziendale.

Basandosi su una strategia di *sicurezza implicita*, esse si limitano a individuare 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 cercare i codici fiscali e impedire che vengano trasmessi al di fuori del perimetro dell'azienda o può impedire il caricamento di dati sensibili su un'applicazione SaaS (come Microsoft Team), senza distinzioni tra un'istanza

aziendale approvata e una personale. 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 stabilire se un'attività è autorizzata o meno. La fiducia implicita è un concetto che inibisce una comunicazione efficiente e lo scambio di dati necessario allo sviluppo 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 vengano 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 sistema DLP moderno erogato nel cloud che si basa sui principi Zero Trust monitora e controlla qualsiasi posizione usata per connettersi e accedere alle informazioni, e ovunque queste vengano archiviate e trasferite (nei repository delle applicazioni cloud e anche 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 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 sono affidabili e attenti alla sicurezza, e non mettono 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 della 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, una soluzione con approccio Zero Trust non parte da alcun presupposto, ma protegge i dati sensibili (come le informazioni di pagamento) chiedendo a tutti gli utenti di completare un processo di autenticazione a prescindere dal livello di autorizzazione riconosciuto. La procedura può includere l'autenticazione a più fattori, 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 la 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 dare l'autorizzazione, e minimizza i rischi ai 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 abbiamo parlato nel paragrafo "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 chi è il destinatario di quell'azione. Queste informazioni aiutano a stabilire se il comportamento di un utente va bene oppure no. 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 rimangano protetti e

solo gli utenti autorizzati possano accedere alle informazioni e condividerle con destinatari autorizzati, e solo verso applicazioni ritenute sicure.

- **Contesto del dispositivo:** Il dispositivo che tenta di accedere ai dati. È necessario considerare se il dispositivo è personale o aziendale, la postura di sicurezza e se è stato 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 tutte queste variabili, è possibile determinare i privilegi da applicare al dispositivo sulla base del 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. Ciò può aiutare a stabilire se l'app pone un rischio, ad esempio viola il Regolamento generale sulla protezione dei dati (GDPR) esponendo troppo 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 Slack e Microsoft Teams, 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 livello di sensibilità, il formato, la dimensione di una determinata informazione e altri fattori, nonché dove vengono usati i dati e se l'uso è legittimo. Ciò aiuta a capire a quali tipi di dati accedono gli utenti, quali vengono trasferiti e se devono essere usati in quella particolare destinazione. 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 le informazioni siano accessibili e gestibili solo da parte di utenti autorizzati e in destinazioni 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. Un moderno sistema DLP basato su principi Zero Trust prende in considerazione tutti i rischi, dagli utenti ai dati, alle reti, ai dispositivi e alle 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 usa tutte le informazioni di contesto disponibili per prendere decisioni informate. Esso ha bisogno dell'aiuto e dell'input di altre soluzioni per raccogliere tutto il contesto necessario in relazione all'utente, al dispositivo, all'applicazione e ai dati. Per questo, un sistema con filosofia 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 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 *Security Service Edge* (SSE) 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:

- **SWG:** Un SWG è una soluzione di sicurezza che 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. Esso individua, monitora e protegge i dati aziendali sensibili dalla perdita e dall'esposizione su qualsiasi connessione web (reti domestiche, pubbliche o remote).
- **CASB:** Il componente CASB della piattaforma Netskope DLP individua, monitora e protegge i dati sensibili su applicazioni SaaS, IaaS, 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 es. 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.
- **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 *machine learning*, 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.
- **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 a più fattori, Single Sign-On e 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 che aiuta a proteggere le risorse e ad assicurare il 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, sia per i dati in movimento che a riposo. La soluzione protegge in tempo reale le e-mail sensibili in uscita attraverso proxy SMTP 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.
- **ZTNA (*Zero Trust Network Access*):** Netskope DLP, erogata 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 connettano 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 da un'ampia serie di minacce.

Applicare i principi Zero Trust a una soluzione DLP

RICORDA

Lo scopo della protezione Zero Trust non è 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, e senza 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 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 le informazioni sono protette e accessibili solo a utenti autorizzati.

Approccio Zero Trust adattivo

Un approccio Zero Trust adattivo si fonda sul fatto che le cose cambiano nel tempo. Questo significa che la protezione Zero Trust deve continuamente valutare il contesto di business, il rischio e il comportamento degli utenti per garantire la sicurezza dei dati.

Prendiamo come esempio il buttafuori all'ingresso di una discoteca: una sera arriva un gruppo di persone, il buttafuori controlla i documenti d'identità e, se tutto è in ordine, le lascia passare. Più tardi, però, inizia a notare un comportamento strano da parte di una persona di quel gruppo, che si mostra aggressiva o tenta di entrare in un'area del locale non autorizzata. Con un approccio Zero Trust adattivo, il nostro buttafuori può riconoscere questo comportamento e agire per proteggere gli altri clienti. Può decidere di tenere d'occhio quella persona per assicurarsi che non causi problemi o anche chiederle di andarsene. In questo modo, è possibile 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. Grazie a un approccio Zero Trust adattivo, il sistema riconosce questo nuovo comportamento e correggere di conseguenza i suoi 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 al bisogno. 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 e se serve modifica i privilegi di accesso. 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'UE 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 serve. 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 e modifica i privilegi se serve. 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 e quindi proteggere i dati sensibili e la reputazione dell'azienda.

Esso offre una maggiore protezione 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.

Protezione dei dati Netskope con approccio Zero Trust adattivo

La protezione dei dati con approccio Zero Trust adattivo messa a punto da Netskope si basa interamente 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 saranno verificati dal *Netskope Cloud Confidence Index* (CCI), un database in continua crescita che oggi conta quasi 60.000 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

Il *Security Service Edge* (SSE) è alla base del sistema di protezione dei dati di Netskope, e fa parte della più ampia piattaforma Netskope *Secure Access Service Edge* (SASE). 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 vuol dire più che semplicemente applicare 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

- **Confrontare le soluzioni DLP tradizionali e moderne**
- **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 DLP**

Capitolo 4
Perché scegliere Netskope come soluzione DLP moderna

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 in cloud, più facili da distribuire, ma probabilmente senza i livelli di accuratezza e applicabilità necessari? In questo capitolo rispondiamo alla domanda iniziando da quali sono i principali vantaggi delle soluzioni DLP in cloud:

- **Fornire una protezione completa.** Una soluzione DLP in cloud può proteggere le informazioni indipendentemente da dove sono salvate, dalla destinazione del trasferimento o dalla modalità di accesso.
- **Garantire la protezione in ambienti cloud.** Applicazioni SaaS, servizi cloud pubblici di tipo IaaS, accesso Web... nell'azienda moderna incentrata sul lavoro ibrido, la protezione è assicurata a prescindere da dove si connettono gli utenti.

- **Eliminare il bisogno di configurare infrastrutture aggiuntive perché possono essere distribuite in modo facile e veloce come servizi cloud.**
- **Proteggere i dati sensibili senza sovraccaricare la rete o le risorse di endpoint.** Un sistema DLP in cloud può gestire tutte le attività di scansione dei dati e gli algoritmi di rilevamento alla massima capacità.
- **Offrire un'integrazione più agevole con un'ampia gamma di altri strumenti di sicurezza.**
- **Fornire più visibilità sui dati trasferiti e archiviati al di fuori delle sedi aziendali.**
- **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 per prendere decisioni informate sul sistema DLP in cloud più adatto. I paragrafi seguenti forniscono informazioni sulle caratteristiche distintive della piattaforma Netskope.

Capire le differenze tra le soluzioni DLP in cloud

Le soluzioni DLP moderne devono essere erogate su cloud, e sono di due tipi diversi. Le soluzioni DLP native in cloud sono generalmente integrate in piattaforme IaaS e 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 DLP e soluzioni native in cloud a confronto

Netskope DLP offre una serie di vantaggi rispetto alle più limitate soluzioni native in cloud. Uno dei principali è la maggiore copertura attraverso un singolo motore di policy DLP, che assicura la protezione dei dati sensibili su una più ampia gamma di formati, canali di comunicazione e ambienti, tra cui applicazioni SaaS, servizi IaaS, applicazioni private, servizi di posta elettronica, condivisioni di file e transazioni web, indipendentemente dalla posizione degli utenti.

Netskope DLP include anche 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.

Un altro vantaggio di Netskope DLP è un'accuratezza di livello superiore. La soluzione esamina qualsiasi tipo di file e formato di dati, e usa un'ampia gamma di algoritmi di rilevamento e il *machine learning* (ML) 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 persino incorporati nelle immagini. Questo è importante perché aiuta a impedire la perdita o l'esposizione accidentale dei dati sensibili, con le relative conseguenze per l'azienda, e garantisce di segnalare eventi di sicurezza veri e propri invece di falsi positivi.

Infine, Netskope DLP integra la filosofia Zero Trust per l'analisi del contesto; questo significa che la soluzione è progettata per lavorare in un'architettura di sicurezza Zero Trust completa. Ciò aiuta a garantire che tutti gli accessi ai dati sensibili vengano 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 non la tecnologia e le funzioni necessarie per proteggere i dati sensibili 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 mancano della copertura necessaria a proteggere i dati sensibili in modo completo.

ATTENZIONE

Alcune delle più recenti soluzioni DLP erogate su cloud si presentano bene su carta ma sono lontane anni luce dalle più sofisticate e mature piattaforme tradizionali 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. Bisogna valutare fattori come il livello di maturità e sofisticazione delle capacità di rilevamento dei dati (ad esempio, quanti tipi di file può esaminare e quanti identificativi di dati usa, compresi i tipi di dati localizzati specifici per Paese), la varietà di canali che copre, la sua capacità di adattarsi a rischi e ambienti in continua evoluzione e il livello di integrazione e personalizzazione offerto.

Per adottare una soluzione DLP erogata dal cloud bisogna capire qual è la più adatta. Vediamo quali aspetti è bene considerare:

- **Ampiezza della copertura:** Le soluzioni DLP integrate generalmente fanno parte di SWG, CASB o NGFW, e spesso di un servizio ZTNA (*Zero Trust Network Access*). Esse sono erogate dal cloud e integrate in un servizio di sicurezza di rete. Il loro ambito di applicazione è limitato. Ad esempio, mancano funzioni di protezione dei dati per e-mail in uscita, endpoint e una più ampia gamma di applicazioni SaaS e le loro istanze specifiche (cioè, account aziendali vs personali).
- **Limiti delle soluzioni:** Soluzioni di questo tipo possono non coprire 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. E soprattutto, possono avere capacità di rilevamento e funzioni IA e ML deludenti.

- **Accuratezza del rilevamento dei dati sensibili:** Molte soluzioni DLP in cloud più recenti non sono in grado di rilevare i dati sensibili con la necessaria precisione e granularità. 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 si concentrano su una o due funzioni particolarmente "appariscenti", senza tuttavia fornire una protezione dei dati davvero completa.

  Una soluzione matura offre migliaia di identificativi di dati predefiniti, 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 predefiniti 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 nell'intero 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, gli SWG di prossima generazione, il CASB e lo ZTNA per comprendere a fondo la postura di sicurezza di un'azienda e i rischi associati a ogni singola interazione con i dati sensibili. Questo vuol dire essere consapevoli delle istanze specifiche di applicazioni SaaS e 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

Non tutte le soluzioni di protezione dei dati sono uguali, e molte non hanno il livello di maturità e sofisticazione necessario per sostituire in modo efficace le soluzioni tradizionali. 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. È bene testare tutti i prodotti esaminati per verificare se supportano tutti i volumi e tipi di dati e se coprono tutti i dati in uscita (on-premise e non) senza compromessi.

Bisogna valutare con attenzione le capacità delle varie soluzioni DLP e scegliere quella che soddisfa meglio le esigenze attuali e future dell'azienda. 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 un decennio di innovazione e impegno costanti sul fronte della protezione dei dati, Netskope è considerata lo standard di riferimento rispetto ad altri fornitori di piattaforme SASE e SSE. Nei paragrafi successivi, approfondiamo le caratteristiche e le funzioni che contraddistinguono Netskope DLP.

Cosa fa Netskope DLP per proteggere l'azienda

Netskope DLP 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 DLP è *completamente integrata* nella soluzione completa Netskope SSE, descritta nel Capitolo 3, ed erogata come parte della piattaforma SASE. 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 DLP 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 60.000 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* e *Microsoft Azure*

- applicazioni private ospitate nel data center o nel cloud pubblico
- reti aziendali e uffici remoti
- forza lavoro remota
- tutti i servizi di posta elettronica, on-premise e nel cloud, compresa la posta sul web
- tutti gli endpoint dei dipendenti, on-premise e non

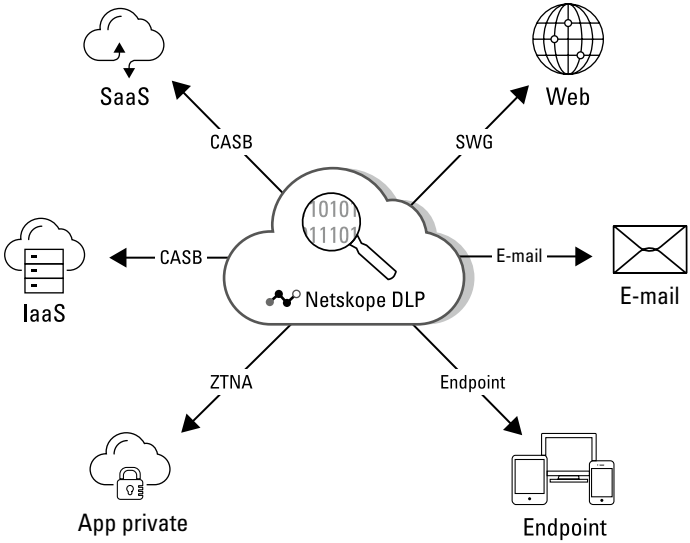

FIGURA 4-1: Netskope DLP è in grado di proteggere tutti i dati, indipendentemente da dove si trovano.

Principali elementi differenzianti

Le soluzioni DLP tradizionali sono spesso considerate inaccurate; in realtà, il vero problema sono i falsi positivi, e per risolverlo serve molta più precisione. Ne abbiamo parlato nel Capitolo 2, dove abbiamo anche presentato e spiegato gli "ingredienti chiave" che possono aiutare i sistemi DLP a essere più precisi. Nei prossimi paragrafi, spieghiamo come Netskope è riuscita a trasformare questi "ingredienti" in elementi differenzianti, creando una soluzione DLP moderna personalizzabile e automatizzata per 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 tradizionale sede dell'azienda diventano sempre più difficili da monitorare e proteggere, e sono quindi più soggetti a esposizione intenzionale e non. Netskope DLP, erogata dal cloud, scopre, monitora e protegge i dati sensibili in movimento, a riposo e in uso nell'intero ecosistema aziendale, compresi applicazioni SaaS, ambienti IaaS cloud pubblici, reti aziendali, uffici remoti, forza lavoro remota, servizi di posta elettronica ed endpoint dei dipendenti.

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

La singola console, con controllo degli accessi basato sui ruoli, garantisce che la configurazione delle policy, il monitoraggio e le attività di segnalazione e *incident response* per tutti i canali possano essere gestite attraverso un unico pannello dagli specialisti della sicurezza.

Capacità superiori di rilevamento e protezione dei dati sensibili

Gli identificativi di dati sono fondamentali per aiutare una soluzione DLP a identificare i dati sensibili sulla base di caratteristiche specifiche come parole chiave descrittive, espressioni regolari, numero di cifre, caratteri speciali, modelli o analisi di prossimità. Quando si ricerca una soluzione DLP, è bene assicurarsi 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 le più ampie varietà e la minima variazione dei dati sensibili. Questo aspetto è importante soprattutto per le aziende globali che devono avere identificativi per molti Paesi. Netskope offre tutte queste caratteristiche facendo leva sull'apprendimento automatico (ML) 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 che non sono ancora stati inventati. 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, come le cartelle compresse (ZIP, RAR, ISO ecc.), le presentazioni, le e-mail, le immagini (BMP, JPG o PNG), i fogli di calcolo, i file CAD, i post sui social, i moduli online, i messaggi di chat, gli allegati e gli 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 facilmente; per questo i moderni strumenti in cloud, come Netskope, 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 e molto altro saranno completamente protetti.

TESORO, MI SI È RISTRETTA LA SUPERFICIE DI ATTACCO

SUGGERIMENTO

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 intenzionale o malevolo. Limitare la superficie di attacco può rendere più difficile identificare 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, bisogna cercare una soluzione DLP con capacità di rilevamento avanzate (OCR, IA, ML, fingerprint dei file e strategie Zero Trust), tutte incluse in Netskope DLP (e approfondite nel Capitolo 2).

Netskope DLP 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 sull'apprendimento automatico (ML), la soluzione è in grado di riconoscere immagini sensibili come patenti di guida, carte di credito, documenti d'identità, contratti, brevetti, documenti di M&A e assegni, anche nel caso di immagini non chiare, sfocate, distorte e danneggiate. Netskope DLP protegge attivamente le informazioni sensibili per garantire la loro sicurezza anche nel mutevole universo del cloud. Questo approccio riduce inoltre il carico di lavoro dei team specializzati grazie all'identificazione e alla protezione automatica dei dati sensibili.

Netskope DLP ha una serie di strumenti di classificazione avanzati basati su ML, tra cui migliaia di identificativi di dati. Inoltre, analizza più di 1.600 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.

Protezione basata sulla conoscenza del rischio e del contesto

Il contesto è l'ABC di una protezione dei dati efficace. Monitorando il traffico tra utenti e app, è possibile esercitare un controllo granulare e autorizzare o bloccare un uso rischioso 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.

Con Netskope DLP, la fatica connessa all'*incident response* e le interruzioni delle attività aziendali sono problemi superati. La soluzione va oltre l'approccio statico di individuare le informazioni sensibili e rispondere sulla base di policy di violazione predefinite; essa tiene invece conto del contesto organizzativo e dei rischi per la sicurezza per attivare dinamicamente la protezione adeguata in base a condizioni in costante evoluzione.

Netskope DLP è integrata nativamente nella soluzione completa Netskope SSE, una piattaforma di sicurezza nativa in cloud che consolida e riunisce tecnologie come SWG, CASB e UEBA. 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 costantemente al corrente del comportamento, della posizione e della postura di sicurezza degli utenti, dei rischi a livello di dispositivo, della reputazione delle applicazioni e delle istanze personali di app, ecc. e permette alla soluzione DLP di limitare le attività di risposta ai soli incidenti effettivi, minimizzando i falsi positivi, la valutazione manuale degli incidenti e le interruzioni alle attività di business.

Con una soluzione SASE integrata, basata sui principi Zero Trust e su controlli avanzati di protezione dei dati, si può 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. Netskope DLP offre programmi di coaching e sensibilizzazione degli utenti in tempo reale ad hoc. In più, può essere integrata con i maggiori sistemi di gestione della formazione e ha un portale utente personalizzabile per l'autoapprendimento.

Lavora in modo più smart con una soluzione DLP

Netskope DLP è erogata dal cloud, quindi non si affida a componenti on-premise. In più offre una protezione sempre attiva e aggiornata, eliminando il bisogno di aggiornamenti manuali, come con le soluzioni DLP tradizionali.

Puntando su policy unificate di protezione dei dati, su una sola console e sul controllo degli accessi basato sui ruoli (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 DLP 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. In questo modo si può creare la policy una sola volta, senza doverla perfezionare e replicare continuamente in base all'uso.

SUGGERIMENTO

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, complicando di più le cose. Netskope DLP permette di visualizzare tutte le violazioni in un unico posto, mentre il rilevamento dei dati sensibili e le attività di *incident response* vengono eseguite sempre in modo coerente e in tempo reale, garantendo una risposta rapida ed efficace 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*.

Capitolo **5**

Dieci mosse per passare senza problemi a un DLP moderno erogato dal cloud

Sostituire i sistemi tradizionali e consolidati, soprattutto nel caso delle soluzioni DLP può sembrare un'impresa ardua. L'iterazione in uso è 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, puoi arrivare a una soluzione completa capace di proteggere le informazioni sensibili in tutte le piattaforme, on-premise e nel cloud.

- **Valuta i bisogni dell'azienda.** Prenditi il tempo di valutare attentamente il contesto tecnologico dell'azienda: quali sono le informazioni da proteggere, quali servizi e repository vengono usati per archiviare ed elaborare le informazioni

sensibili e come. 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 *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 quanta priorità deve essere data alla protezione dei vari tipi di dati. 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 più alti.** Nel valutare il passaggio 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. La soluzione leader di mercato Netskope CASB ha al centro la DLP per garantire la sicurezza dei dati, sia con le applicazioni cloud autorizzate dall'azienda sia con le app non autorizzate (che continuano a essere usate, è inutile negarlo).
- **Scegli attentamente il fornitore.** Assicurati di scegliere un fornitore che soddisfa le esigenze dell'azienda, attuali e future, in ogni singolo ambiente. Netskope DLP è l'unica soluzione che offre una protezione completa per tutte le esigenze cloud e non solo. Parliamo di protezione dei dati a riposo, in movimento e in uso in ambienti in cloud e on-premise, protezione DLP di endpoint, servizi di posta elettronica e reti per il traffico web ed e-mail, nonché protezione DLP per SaaS e IaaS e per le 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 protezione dei dati che rischiano più di creare problemi che di 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 DLP. Questa soluzione DLP completa è progettata per proteggere 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 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 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, alla protezione delle informazioni scambiate tramite istanze di posta elettronica personali, puoi avere la certezza che i dati aziendali sono protetti in ogni circostanza. Con Netskope, puoi gestire la migrazione dei servizi e-mail al cloud a mente serena.
- **Proteggi i dati in movimento.** I dati trasferiti tra posizioni, connessioni, servizi e dispositivi diversi (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. Netskope mette a disposizione un servizio DLP unificato ed erogato attraverso tutta la sua piattaforma SSE intelligente

che è progettato per proteggere i dati sensibili da qualsiasi postazione di lavoro. Questo approccio offre i massimi livelli di sicurezza per le transazioni dei dati, anche grazie a tutti i vantaggi della filosofia Zero Trust e del contesto di rischio disponibile, senza il problema di gestire oscure configurazioni hardware. L'innovativa soluzione DLP Netskope garantisce la sicurezza dei dati sempre e ovunque.

- **Proteggi i dati sui dispositivi di 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. Non importa se i dati vengono creati sull'endpoint stesso o scaricati dal cloud, Netskope DLP offre la soluzione ideale. Questa leggera soluzione di endpoint 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. Essa 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 garantire 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 di recente hai investito in una soluzione DLP offerta da un fornitore di servizi cloud o SaaS, nel breve periodo ti 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. Ma fai attenzione a capire quando stai gestendo 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. Netskope 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 DLP offre un approccio moderno alla protezione dei dati più efficiente ed efficace che mai. La soluzione usa avanzate tecnologie di rilevamento, come ML, *fingerprint* dei dati e riconoscimento

delle immagini su una scala senza precedenti e a pieno potenziale persino sugli endpoint perché la capacità di elaborazione è 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 DLP di valutare ogni interazione che contiene dati sensibili, per adattare dinamicamente la risposta in base a ogni singola violazione delle policy. Questo nuovo approccio supporta una collaborazione sicura e le moderne prassi di condivisione dei dati, non ostacola la produttività, minimizza i falsi positivi e genera risultati più accurati sul fronte della protezione dei dati. Netskope DLP è integrata nativamente nella soluzione completa Netskope SSE, e quindi sempre consapevole dei rischi, dei comportamenti e delle vulnerabilità della sicurezza in azienda. Netskope DLP è completamente integrata in Netskope SSE, il che permette alle aziende di essere 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 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. Netskope DLP aiuta a ridurre i requisiti a carico del team DLP, che quindi può passare meno tempo a gestire gli incidenti e più a concentrarsi su iniziative attive per garantire la sicurezza dell'azienda.
- **Preferisci la maturità al clamore.** Le conoscenze tecniche non bastano a garantire 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 rendere utile la fatica!

Sicurezza pronta a tutto

Protezione dei dati

Netskope, leader SASE globale, sta ridefinendo la sicurezza del cloud, dei dati e delle reti per aiutare le organizzazioni ad applicare i principi zero trust per proteggere i dati. Veloce e facile da usare, la piattaforma Netskope offre un accesso ottimizzato e sicurezza in tempo reale per persone, dispositivi e dati ovunque si trovino. Netskope aiuta i clienti a ridurre i rischi, accelerare le prestazioni e ottenere una visibilità impareggiabile su qualsiasi attività cloud, web e delle applicazioni private. Migliaia di clienti, tra cui più di 25 delle aziende Fortune 100, si affidano a Netskope e alla sua potente rete NewEdge per affrontare minacce in evoluzione, nuovi rischi, cambiamenti tecnologici, requisiti organizzativi e di rete, modifiche e normative. Scopri come Netskope aiuta i clienti a essere pronti a tutto nel loro percorso SASE, **visita netskope.com.**

netskope

Preparati a un futuro *cloud-first* con le moderne tecnologie DLP

La rapida adozione del cloud e la tendenza al lavoro remoto hanno reso inadeguati i sistemi di protezione dei dati un tempo considerati innovativi. I sistemi di sicurezza devono garantire una protezione costante delle informazioni, indipendentemente dalla posizione dei dati e degli utenti. La soluzione di *Data Loss Prevention* (DLP) ideale deve essere sviluppata appositamente per il cloud, e non riadattata sulla base dei nuovi casi d'uso. Inoltre, deve poggiare su tecniche Zero Trust, ridurre la complessità e garantire un'applicazione coerente delle policy. Ovunque.

All'interno...

- Valutare l'approccio dell'azienda alla protezione dei dati
- Proteggere i dati sensibili supportando gli obiettivi commerciali
- Scoprire il funzionamento dei sistemi DLP moderni
- Ridurre gli accessi non autorizzati ai dati
- Semplificare le policy di sicurezza senza rinunciare alla loro efficacia
- Trasferire in modo sicuro i dati nel cloud e tra diverse applicazioni cloud

Carmine Clementelli è un esperto di sicurezza informatica e technology leader in materia di sicurezza dei dati, protezione del cloud, Zero Trust e *Security Service Edge* (SSE) in Netskope. Ha alle spalle decenni di esperienza come autore, oratore e consulente per Palo Alto Networks, Symantec e altre aziende globali.

Visitate il sito Dummies.com®
per trovare video, esempi passo passo e guide, o per i vostri acquisti!

ISBN: 978-1-394-20800-5
Non in vendita

for dummies®

WILEY END USER LICENSE AGREEMENT

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