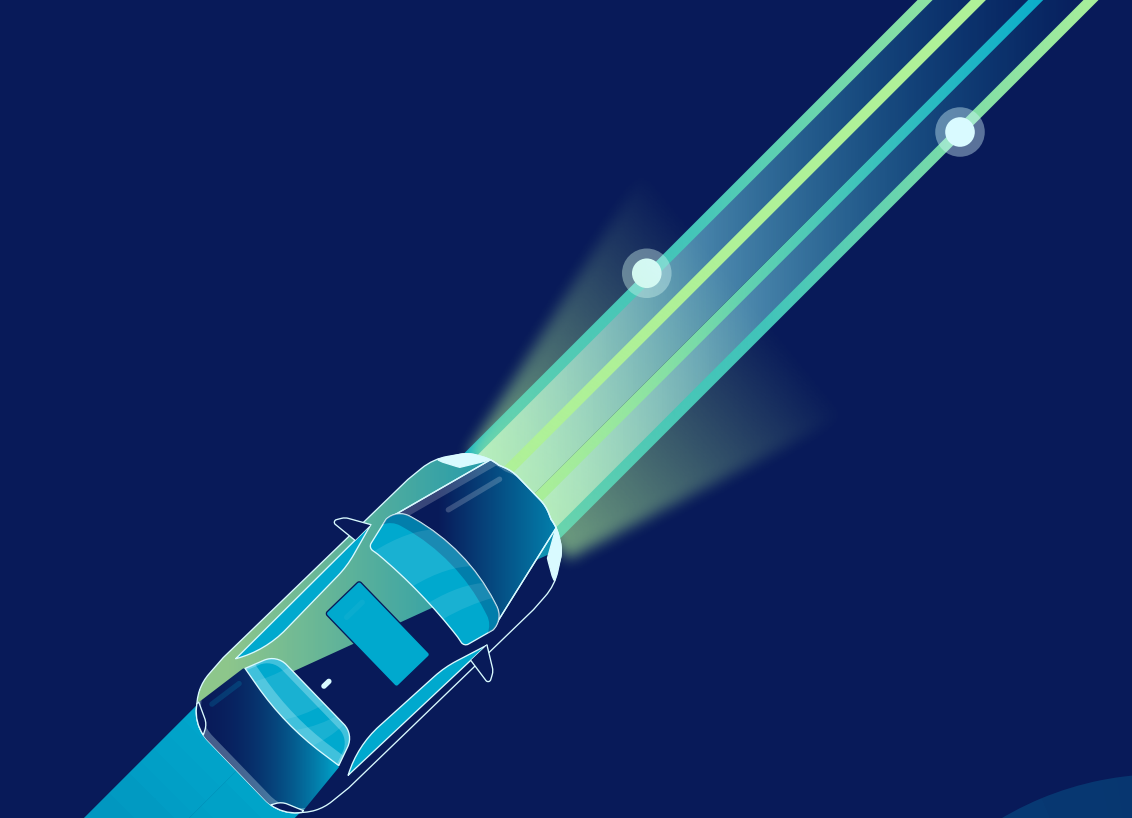
netskope

Il manuale per la sicurezza dei dati unificata



Protezione dei dati al massimo livello grazie alla combinazione di DSPM e DLP in un'unica soluzione

Il manuale per la sicurezza dei dati unificati

Indice

Sintesi

I team di sicurezza aziendale, gestione dei rischi e compliance hanno la sensazione di partecipare a una corsa infinita, cercando di stare al passo con gli autori delle minacce. E non si sbagliano. Le violazioni dei dati diventano sempre più frequenti ogni anno e nessuna organizzazione ne è immune. Il problema riguarda società di qualsiasi dimensione, settore e area geografica.

Gli utenti possono essere a conoscenza del rischio, ma si aspettano che le aziende con cui hanno a che fare proteggano le loro informazioni. Pochi eventi hanno un impatto così grande sulla reputazione del marchio di un'azienda come un attacco informatico su larga scala.

Il panorama delle minacce ha indotto le autorità di regolamentazione a innalzare le aspettative in merito alla privacy dei dati aziendali. Le violazioni spesso sono frutto dell'inosservanza da parte delle organizzazioni di regole volte a proteggere i dati sensibili. Quando le autorità di regolamentazione scoprono che un'azienda presa di mira non ha rispettato le normative obbligatorie, esse tendono a reagire con forza, imponendo sanzioni pecuniarie.

Garantire la sicurezza e la conformità era già una sfida quando le informazioni preziose di un'azienda risiedevano tutte all'interno del proprio perimetro aziendale. Oggi, ciò è ancora più difficile perché il 60% dei dati dei clienti di un'azienda media si trova nel cloud. [1] Queste preziose informazioni si trovano al di fuori del tradizionale ambito di controllo del reparto IT.

Proteggere le risorse digitali nelle aziende di oggi richiede un nuovo modo di pensare. La sicurezza unificata dei dati combina le funzionalità di rilevamento, classificazione, governance degli accessi e valutazione del rischio (quelle presenti negli strumenti di gestione del livello di sicurezza dei dati [DSPM]) con le protezioni in tempo reale delle tecnologie di prevenzione della perdita dei dati (DLP). Completamente integrate, queste soluzioni bloccano i dati di un'azienda, anche i dati memorizzati nel cloud e nelle applicazioni ombra non gestite da IT aziendale, attraverso sei funzionalità chiave.

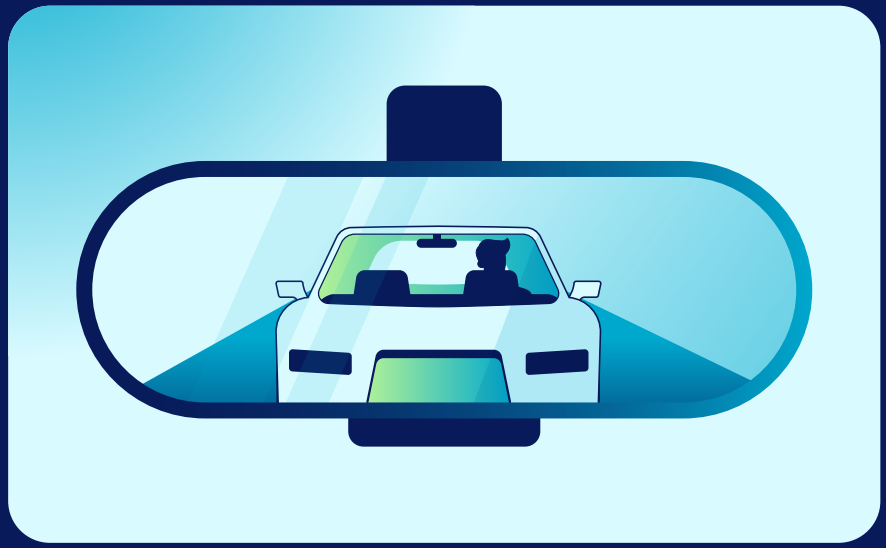
[1] Fonte: Statista. "Quota di dati aziendali archiviati su cloud nelle organizzazioni di tutto il mondo", marzo 2022.

Fondamenti sulla sicurezza dei dati nell'era dell'IA

Le aziende devono riconoscere i propri punti ciechi sulla sicurezza per bloccare in modo efficace i tentativi da parte degli attacchi informatici per ottenere misure di salvaguardia passate. Per assicurarsi di avere una chiara visione di tutte le applicazioni e dei dati a cui gli utenti accedono, i team IT devono porsi alcune domande chiave:

- Dove sono tutti i nostri dati?
- Qual è la natura di questi dati?
- Chi ha accesso ai dati sensibili?
- Quanto sono rischiose le nostre interazioni con i dati?

Lo scopo di questo esercizio è semplice: Se una soluzione, o un database, basati su cloud contiene informazioni personali identificabili (PII) dei clienti, come indirizzi o codici fiscali, o qualsiasi altra informazione aziendale sensibile, l'organizzazione ha bisogno di capire quali misure di protezione sono state messe in atto per tenere sotto controllo il rischio dei dati.



Consiglio del professionista

Se una soluzione basata su cloud contiene PII dei clienti o altre informazioni aziendali sensibili, l'organizzazione ha bisogno di capire quali misure di protezione sono state messe in atto per tenere sotto controllo il rischio dei dati.

Gestione del rischio attraverso i dati

La sfida nell'identificare i punti ciechi dei dati è che le aziende devono proteggere tantissime informazioni differenti che, non sempre, viaggiano in modo ordinato. I team addetti alla sicurezza potrebbero dover gestire i dati in un'ampia gamma di endpoint, siti Web e sistemi di posta elettronica. I dati sensibili possono risiedere anche in database, data lake e/o data warehouse, nonché in una serie di sistemi basati su cloud: non solo software-as-a-service (SaaS), ma anche infrastructure-as-a-service (IaaS) e platform-as-a-service (PaaS).

Alcuni di questi dati sono presenti in loco; altri sono presenti su cloud. Tutti devono essere protetti mentre sono in movimento, mentre sono in uso e mentre sono a riposo.

Giusto per complicare ulteriormente la sfida, circa il 90% dei dati aziendali non è strutturato.[2] Le informazioni cruciali si trovano nei documenti Word, PDF, file di immagini e altri formati. Anche se questi dati potrebbero non essere facilmente ricercabili, essi richiedono la stessa protezione dei dati contenuti nei database e in altre applicazioni strutturate.

Infine, sebbene i dati critici per l'attività debbano risiedere nelle applicazioni gestite dall'IT aziendale, l'IT ombra è un problema costante. Le unità aziendali spesso impiegano tecnologie non gestite per uno scopo specifico senza ottenere l'approvazione dell'IT. Il 97% delle applicazioni cloud che i dipendenti di un'azienda standard utilizza esiste senza che l'IT ne sia a conoscenza. [3]

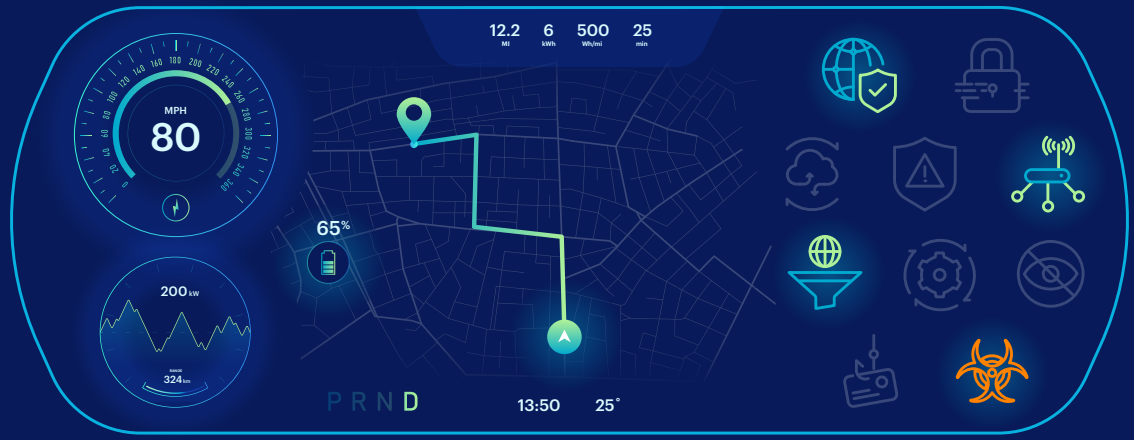
Circa

90%

dei dati aziendali non sono strutturati.

88%

degli utenti che interagiscono con applicazioni cloud personali - Shadow IT [4]



[2] IDC. "Valore non sfruttato: ciò che ogni dirigente deve sapere sui dati non strutturati", agosto 2023.

[3] Netskope Threat Labs Cloud and Threat Report: 2025.

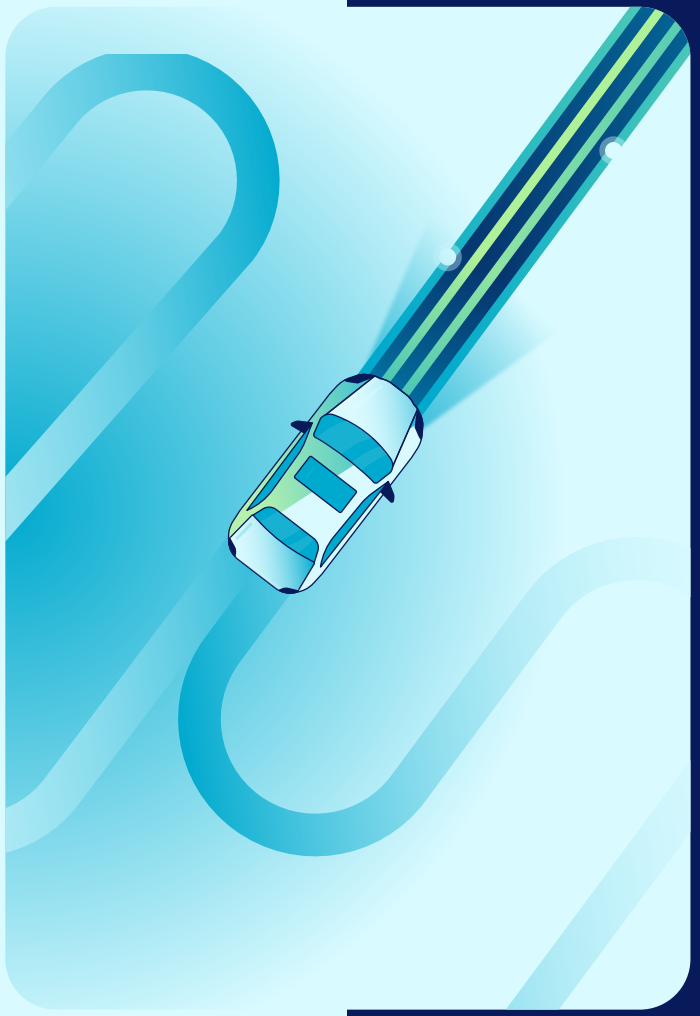
[4] Netskope Threat Labs Cloud and Threat Report: Generative AI, 2025.

Tecnologie frammentate incapaci di rispondere alla sfida

Le aziende non mancano di opzioni per proteggere i singoli tipi di dati, ma di solito necessitano di un assortimento di soluzioni per assicurare la totalità dei loro dati. I team dedicati alla sicurezza hanno dovuto aumentare il livello di protezione nel corso degli anni, e si prevede che questa tendenza continuerà con l'emergere di nuove tecnologie e vulnerabilità.

I sistemi endpoint DLP svolgono un ottimo lavoro per proteggere i dati sugli endpoint aziendali. Tuttavia, per proteggere le informazioni sensibili contenute nelle e-mail, un'azienda ha bisogno di un'e-mail DLP o di un'altra soluzione. Alcune organizzazioni dispongono di una soluzione separata per garantire l'utilizzo dell'IA generativa (genAI) all'interno del proprio ambiente. La funzionalità di questa soluzione potrebbe includere la prevenzione della fuga accidentale dei dati aziendali nel dominio pubblico, ma potrebbe non coprire le esigenze di conformità normativa dell'azienda. Per le minacce interne, l'organizzazione potrebbe procurarsi uno strumento di analisi comportamentale per prevenire il sabotaggio. E per la scoperta e la classificazione dei dati sensibili, DSPM è la scelta migliore.

Il problema è che l'implementazione di tutte queste svariate soluzioni crea un paesaggio di tecnologie disparate complesso che sollecita le risorse IT e può rendere i dati aziendali meno sicuri.



"È il momento di reinventare la sicurezza dei dati se DSPM e DLP sono stati gestiti come silos separati. Possono lavorare insieme per formare il fulcro di un approccio completo che non solo protegge i dati, ma posiziona in modo competitivo l'organizzazione per essere leader nell'economia odierna basata sui dati".

Ankur Chadda

Leader di marketing per la sicurezza dei dati Netskope

Sicurezza unificata dei dati

I team di IT necessitano di una piattaforma di sicurezza in grado di proteggere tutti i tipi di dati e, al tempo stesso, offrire una visibilità totale. Questo è l'obiettivo delle piattaforme unificate per la sicurezza dei dati, che uniscono le funzionalità DSPM e DLP in un'unica soluzione.

Riunire tutti i dati di un'azienda in una stessa soluzione comporta diversi vantaggi:

- **Visibilità migliorata.** Il personale IT può visionare un'unica dashboard per comprendere i problemi di sicurezza dei dati che possono esistere in loco o sul cloud, nei dati gestiti e non gestiti in movimento, in uso o a riposo.
- **Migliore sicurezza.** I sistemi disparati spesso comportano una risposta frammentata a qualsiasi minaccia. Al contrario, una piattaforma strettamente integrata assicura che le informazioni su rischi o minacce raccolte da una soluzione saranno condivise con altre soluzioni, consentendo una risposta coordinata ovunque l'azienda memorizzi i dati.
- **Facilità di gestione.** L'amministrazione dell'infrastruttura di sicurezza richiede meno tempo del personale, spostando il team di sicurezza da un approccio reattivo costante alla correzione della vulnerabilità, alla pianificazione a lungo termine e ad altre iniziative strategiche.

"Capisco che come si presenta il mio set di politiche attraverso più funzioni e applicazioni, rispetto ad alcune delle nostre applicazioni legacy in cui ho avuto quattro diversi luoghi per gestire una singola applicazione e le sue caratteristiche".

Vicepresidente dell'infrastruttura

Tecnologia

L'approccio di Netskope One alla sicurezza unificata dei dati

Netskope One assiste le organizzazioni nel passare a un livello superiore fornendo una piattaforma unificata per la sicurezza completa dei dati. Unisce DSPM e DLP con l'obiettivo di portare precisione e accuratezza al rilevamento dei rischi e a un controllo delle minacce.

Un fattore chiave la differenzia rispetto alle soluzioni alternative è la capacità della piattaforma Netskope One di proteggere i dati a riposo, in movimento e in uso attraverso tutti i principali vettori di minaccia. Consolidando così tante funzionalità, consente a tutti gli strumenti di protezione delle informazioni sensibili di condividere il contesto tra utenti, applicazioni e azioni.

Questo approccio rafforza la sicurezza in cinque modi principali:

1. Riducendo la superficie di rischio della società: Netskope One controlla l'accesso a tutte le applicazioni Web, SaaS e private in cui risiedono i dati
2. Accelerando la scoperta dei dati
3. Supportando una migliore comprensione dei dati aziendali, inclusi lignaggio e movimento dei dati
4. Consentendo il controllo automatizzato e in tempo reale del rischio dei dati
5. Supportando la scalabilità: Le politiche e i profili dei dati possono essere creati una sola volta e, successivamente, sfruttati ovunque

Netskope One offre maggiore ampiezza e profondità di copertura ovunque risiedano i dati di un'azienda. Ora diamo un'occhiata alle tre domande che vi aiuteranno a valutare il contesto della vostra organizzazione:

Domanda 1: Qual è il rischio rappresentato dalla superficie?

Domanda 2: Quanto velocemente le soluzioni di sicurezza rispondono a comportamenti rischiosi?

Domanda 3: In che modo vengono applicati i criteri DLP al traffico rimanente?

"Netskope ci permette di quantificare l'esfiltrazione dei dati e collegare i comportamenti a rischio agli individui, consentendoci di agire tempestivamente".

Senior Director

Global Insider Risk Program, di un'importante società di servizi finanziari

Domanda 1: Qual è il rischio rappresentato dalla superficie?

Netskope One prende decisioni politiche continue, adattive e basate sulla fiducia in tempo reale. Ogni volta che un utente tenta di memorizzare, spostare o manipolare i dati, la piattaforma valuta il rischio attraverso quattro vettori:

- **Rischio per l'utente:** I dati sono protetti da tentativi di impersonificazione? Si è in grado di verificare che gli utenti siano chi dicono di essere?
- **Rischio del dispositivo:** L'individuo è su un dispositivo gestito, in una posizione nota e attendibile?
- **Rischio delle applicazioni:** Il software fa parte di un'applicazione gestita dal l'IT? E si tratta di un'istanza aziendale o personale del software?
- **Rischio dei dati:** Si tratta di dati aziendali riservati o sensibili?

Netskope ha analizzato e valutato più di 80.000 applicazioni e sviluppato 130 categorie per gli URL. La piattaforma Netskope One classifica il traffico di conseguenza, per accelerare la gestione delle minacce. La piattaforma può inoltre fare la differenza tra migliaia di istanze SaaS.

Netskope One raccoglie tutti questi dati, sfruttando così l'analisi del comportamento degli utenti e delle entità (UEBA), insieme all'intelligence sulle minacce in tempo reale, per valutare il tentativo di attività da parte dell'utente su una scala di comportamenti rischiosi.

Domanda 2: Quanto velocemente le soluzioni di sicurezza rispondono a comportamenti rischiosi?

Dopo aver completato l'analisi del rischio, l'applicazione della politica sulla sicurezza dei dati di Netskope One interrompe il traffico sospetto mentre l'utente esegue la ri-autenticazione o fornisce una giustificazione per il suo comportamento. In alternativa, nel peggiore dei casi, può bloccare automaticamente il traffico, isolando l'utente e/o il dispositivo fino a quando un'azione umana non ne possa valutare l'attività.

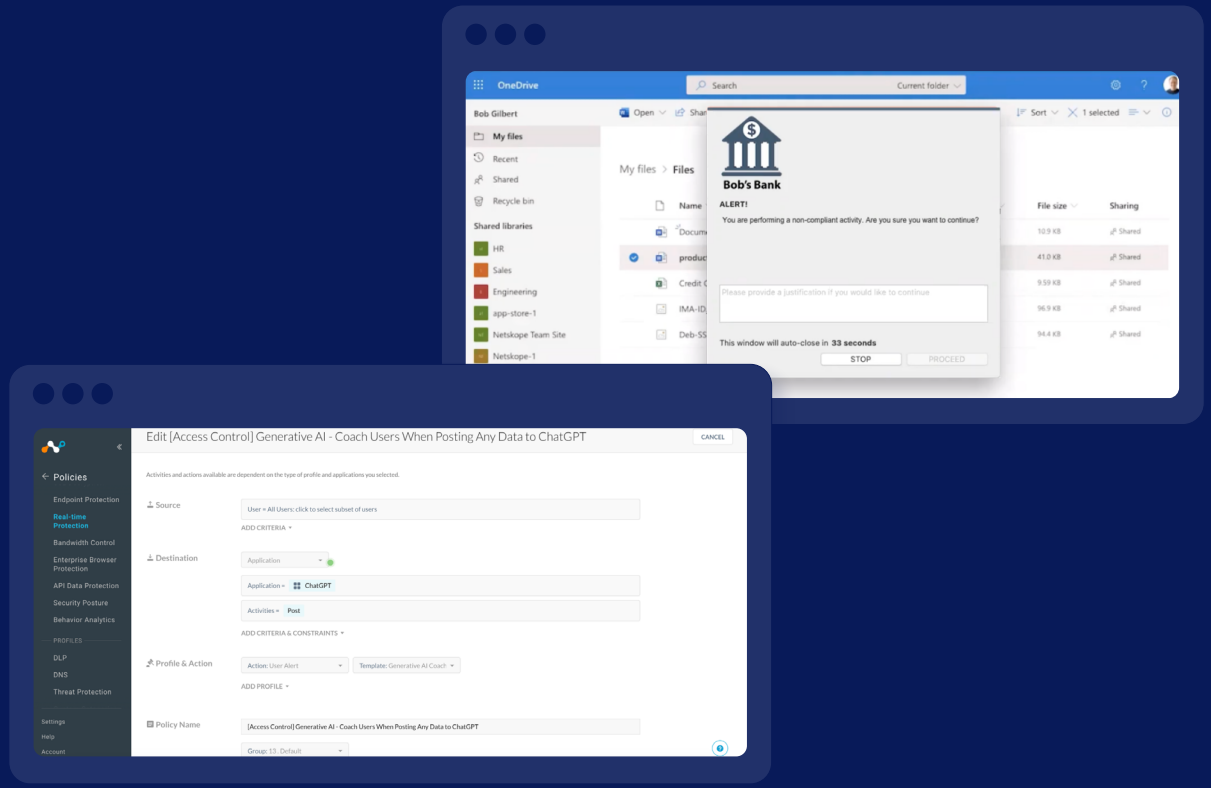
Le aziende possono utilizzare Netskope One Data Security per introdurre controlli granulari che, tra l'altro:

- Bloccano malware e contenuti che violano la politica di utilizzo accettabile (AUP)
- Interrompono attività basate su cloud e/ o applicazioni note come rischiose
- Impediscono il caricamento su qualsiasi applicazione cloud, o applicazione, che l'IT non gestisce
- Limitano le attività di condivisione a determinati domini Web
- Limitano il traffico in base a informazioni aggiuntive, come le caratteristiche dell'utente

Una caratteristica unica di Netskope One Data Security è che può essere configurato per fornire coaching in tempo reale per educare gli utenti il cui comportamento viola la politica sui dati aziendali.

"Siamo molto preoccupati per l'aggressività di [attori di minacce avanzate persistenti] alla ricerca dei nostri dati. La soluzione SSE di Netskope ci aiuta a gestire questo problema in modo molto più efficace".

Vicepresidente dell'infrastruttura,
Società in ambito tecnologico



Domanda 3: In che modo vengono applicati i criteri DLP al traffico rimanente?

Per il traffico che supera l'analisi DSPM, Netskope One Data Security applica tecniche DLP per garantire che gli utenti non esfiltrino i dati. Le funzionalità della piattaforma esaminano i dati su e-mail, endpoint, siti Web e vari formati di archiviazione dei dati, sia a livello locale che su cloud.

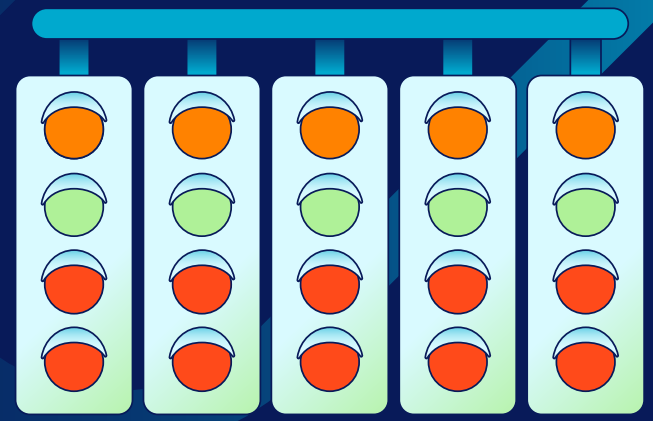
Come le precedenti iterazioni di DLP, Netskope One Data Security utilizza espressioni regolari personalizzate, parole chiave, dizionari e corrispondenza dati esatta (EDM) e corrispondenza documenti indicizzati (IDM) per identificare i dati. Raccoglie indizi di contesto sia dai fattori della piattaforma, come il rischio utente o le informazioni dal cloud access security broker (CASB) o SaaS security posture management (SSPM), sia da fonti esterne, come single sign-on (SSO) o integrazioni di secure email gateway (SEG). Come il DSPM, Netskope One DLP sfrutta l'ispezione dei contenuti utilizzando modelli ML per trovare PII, PHI e altri tipi di dati.

Per l'84% delle organizzazioni che devono rispettare un qualche tipo di quadro di conformità esterno, [5] queste capacità sono cruciali. Netskope One è dotata di 38 modelli predefiniti di conformità legale e normative, che supportano le unità aziendali in tutto il mondo nel soddisfare i requisiti locali. Soprattutto, nonostante la piattaforma migliori la conformità, essa riduce l'attrito di sicurezza per gli utenti in modo da non ostacolare la produttività del business.

"Netskope ci fornisce gli strumenti e le funzionalità per abbracciare in modo sicuro le tecnologie cloud, pur mantenendo il controllo e la conformità".

Responsabile della sicurezza

Apex Group



[5] Fonte: Coalfire. "Securealities Report: Compliance 2023", maggio 2023.

Il Machine Learning (ML) di Netskope One interpreta i dati sia strutturati che non strutturati

Netskope One utilizza il Machine Learning sia per determinare il contenuto dei dati non strutturati che per categorizzare i dati. Ad esempio, il processo di classificazione delle immagini della piattaforma utilizza un algoritmo di ML addestrato per identificare documenti sensibili come passaporti o patenti di guida senza esaminarne il testo. Nel frattempo, la tecnologia di riconoscimento ottico dei caratteri (OCR) della piattaforma è in grado di estrarre il testo dalle immagini per analizzarlo.

Le funzionalità di ML integrate in Netskope One utilizzano gli attributi dei dati sia strutturati che non strutturati per etichettarli come PII, informazioni personali sulla salute (PHI), soggetti al regolamento generale sulla protezione dei dati (GDPR) o alla legge sulla portabilità e responsabilità delle assicurazioni sanitarie (HIPAA), ecc. La piattaforma è dotata di oltre 3.000 classificatori del rischio dati integrati e le aziende possono sviluppare anche i propri classificatori basati sul ML.

Inoltre, Netskope One può essere addestrato per cercare combinazioni di identificatori, come i numeri di previdenza sociale nei documenti fiscali o per eseguire un'analisi dei privilegi confrontando dati e caratteristiche dell'utente. Sfruttando il Machine Learning in questo modo, si riduce il sovraccarico operativo della sicurezza riducendo al minimo il coinvolgimento umano nel processo decisionale di routine, migliorando al contempo l'efficacia delle decisioni eliminando la possibilità di errori umani.

Consiglio del professionista

Il Machine Learning riduce il sovraccarico operativo della sicurezza riducendo al minimo il coinvolgimento umano nel processo decisionale di routine, migliorando al contempo l'efficacia delle decisioni.

Netskope One: La scelta giusta per la sicurezza unificata dei dati

Netskope One è in vantaggio rispetto ai potenziali aggressori combinando le funzionalità DSPM con un motore DLP unificato che gestisce tutte le fonti di dati, sia in loco che su cloud. La piattaforma fornisce un dashboard a pannello singolo che mostra le preoccupazioni, i controlli e la risposta alle minacce per l'intero ciclo di vita dei dati. E le informazioni che essa produce sostengono l'applicazione delle politiche in tempo reale.

La piattaforma Netskope One protegge tutti i dati di un'azienda, sia strutturati che non strutturati, gestiti o meno, all'interno del data center o nel cloud. Uno studio sull'impatto economico totale di Forrester ha rilevato che il tipico cliente Netskope raggiunge i seguenti risultati aziendali: [6]

> "Direi sicuramente che il livello di rischio si è abbassato [grazie all'implementazione di Netskope SSE] perché non stiamo cercando di spegnere incendi di continuo e possiamo concentrarci sulle vulnerabilità e sul lavoro effettivo".
>
> **Vicepresidente dell'Esperienza digitale**
>
> Società di servizi finanziari

Risultati aziendali

- **Riduzione dell'80% del rischio di una grave violazione dei dati da parte di attacchi esterni**
- **Riduzione del 60% del tempo medio di risoluzione (MTTR)**
- **Riduzione del 10% dei costi di infrastruttura**
- **Riduzione dell'80% dei numeri di ticket dell'help desk**
- **Riduzione del 15% dei tempi di inattività non pianificati**
- **Aumento del 30% dell'efficacia delle operazioni di rete e sicurezza**
- **Miglioramento della protezione della proprietà intellettuale (PI) da DLP**
- **Maggiore disponibilità e reattività alla conformità normativa**
- **Maggiore allineamento con gli obiettivi ambientali, sociali e di governance (ESG)**

6. Forrester. "The Total Economic Impact of Netskope SSE," ottobre 2024.

Una serie di vittorie con Netskope One

Vincere la gara contro i cyberattacchi richiede strategia, preparazione ed esecuzione. Quando il pedale dell'acceleratore incontra un ostacolo, è tutto o niente.

La sicurezza dei dati unificata con Netskope One offre tutte le funzionalità di protezione necessarie per proteggere le loro macchine di grande valore:

- **Automatizzare la scoperta e la classificazione dei dati aziendali ovunque essi risiedano e si spostino**
- **Rispondere rapidamente ai rischi di esfiltrazione dei dati**
- **Ottenere la conformità e la privacy dei dati in modo efficiente**
- **Ridurre significativamente il rischio di insider malintenzionati**
- **Ridurre al minimo l'esposizione ai dati negligenti**
- **Offrire un'esperienza senza attriti all'utente finale**
- **Garantire l'uso sicuro dell'IA generativa organizzativa**
- **Gestire il ciclo di vita dei dati in modo completo**

"La sicurezza informatica è per noi un fattore di differenziazione competitivo, che ci aiuta ad attrarre nuovi clienti, in particolare da industrie che apprezzano una solida protezione dei dati".

CISO

Società globale di servizi

"Netskope SSE ci ha fatto scoprire tutti questi problemi che non sapevamo davvero di avere. Abbiamo trovato sistemi su internet che non stavano passando attraverso i nostri controlli di sicurezza ... Siamo rimasti scioccati e abbiamo risolto i problemi".

Vicepresidente dell'Esperienza digitale

Società di servizi finanziari[7]

Netskope One

Effettuare il back-up dei propri dati con Netskope One Data Security.

Saperne di più ⟶

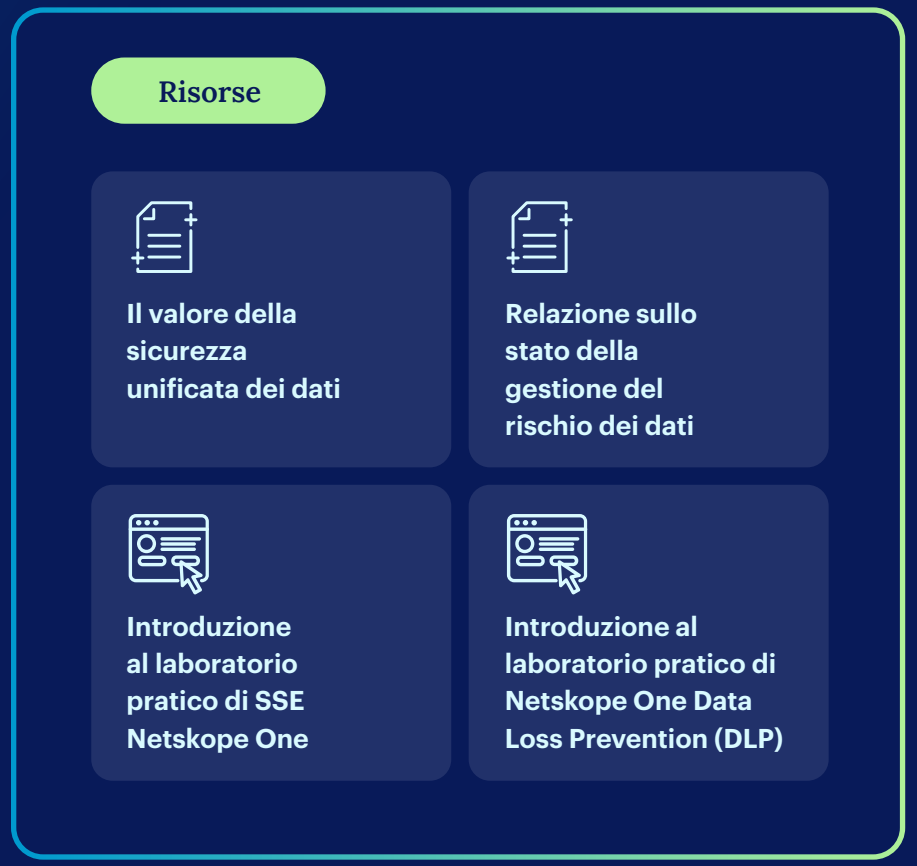
[7] Forrester. "The Total Economic Impact of Netskope SSE," ottobre 2024.

A proposito di Netskope

Netskope, leader nella sicurezza e nelle reti moderne, soddisfa le esigenze dei team di sicurezza e networking fornendo accesso ottimizzato e sicurezza in tempo reale basata sul contesto per persone, dispositivi e dati ovunque si spostino. Migliaia di clienti, tra cui più di 30 appartenenti a Fortune 100, si affidano alla piattaforma Netskope One, al suo Zero Trust Engine e alla sua potente rete NewEdge per ridurre i rischi e ottenere massima visibilità e controllo su applicazioni cloud, IA, SaaS, Web e private che offrono sicurezza e prestazioni accelerate senza compromessi.

Interessati ad approfondire?

Richiedi una demo



netskope