

Dell SafeData

Netskope Secure Web Gateway

La sicurezza web di nuova generazione del cloud per il cloud, che protegge i servizi cloud, le applicazioni, i siti web e i dati di qualsiasi utente, posizione o dispositivo.

Panoramica rapida

- Controlli granulari del traffico web e delle policy delle app, inclusi dati, attività e contesto
- Avvisi di coaching basati sul rischio relativi all'adozione di app e servizi cloud da parte degli utenti
- Scalabilità e prestazioni cloud per controllare tutti gli utenti, dispositivi o posizioni
- Prevenzione della perdita di dati per le app gestite e non gestite e per il traffico web
- Misure di difesa contro malware e minacce avanzate, sandboxing e oltre 40 feed di Threat Intelligence
- Unica console cloud con controlli delle policy coerenti per le funzioni SWG, CASB e DLP
- Security Cloud Platform soddisfa i requisiti del Federal Risk and Authorization Management Program (FedRAMP) e ha ottenuto l'autorizzazione FedRAMP
- Federal Transformation con soluzioni TIC 3.0 basate su SASE

Panoramica del prodotto

Oggi, un'organizzazione utilizza in media oltre 1.295 app e servizi cloud e oltre il 95% di essi non è gestito ed è privo di diritti di amministrazione IT^{***}. Per comprendere e proteggere i contenuti e il contesto, i web gateway protetti devono superare il tradizionale filtro URL delle richieste web per la decodifica del traffico API di migliaia di app e servizi cloud. I deployment di sicurezza web in linea richiedono inoltre prestazioni cloud on-demand per ispezionare il traffico web crittografato e su scala cloud con accessi al cloud distribuiti a livello globale per gli utenti di uffici remoti e dispositivi mobili.

La Digital Transformation guidata dal cloud e dalla mobilità continua ad avanzare, con l'85% del traffico dei web gateway identificato tramite app e servizi cloud nel Netskope Cloud Confidence Index*. Inoltre, l'83% del traffico web è crittografato** e questo crea nuovi punti ciechi soggetti alla perdita di dati e all'introduzione di minacce per app gestite e non gestite, servizi cloud e traffico web.

La soluzione di sicurezza web basata sul cloud SWG di nuova generazione di Netskope evita il malware, rileva le minacce avanzate, filtra per categoria, protegge i dati e controlla l'utilizzo delle app per qualsiasi utente, posizione e dispositivo. Unifica CASB, SWG e DLP leader del settore in controlli per le policy comuni con reporting personalizzato e metadati avanzati per query ad hoc.

Caratteristiche chiave del prodotto

Secure Access Services Edge (SASE)

Un'architettura SASE (Secure Access Services Edge) consente di identificare utenti e dispositivi, applicare controlli di sicurezza basati su policy e fornire un accesso protetto alle applicazioni o ai dati appropriati. Queste funzionalità si allineano direttamente con la base della piattaforma di sicurezza nativa per il cloud di Netskope, progettata per comprendere e proteggere gli ambienti SaaS, web e IaaS durante l'accesso da qualsiasi dispositivo. Tutte le attività vengono eseguite da un'unica console, con una sola architettura e policy integrate per tutti i servizi SASE, tra cui CASB, SWG e Private Access.

Monitoraggio e valutazione

Visibilità in linea per migliaia di app e servizi cloud gestiti e non gestiti, nonché per il traffico web. Unione di tutte le funzionalità critiche SWG+CASB+DLP in una sola piattaforma SWG di nuova generazione.

Controllo delle applicazioni cloud

Controllo granulare in tempo reale di migliaia di app cloud, incluse quelle gestite da linee aziendali e utenti. Consente di bloccare i contenuti pericolosi e di consentire quelli sicuri.

Uso accettabile

Integrazione di una combinazione di filtri web tradizionali, che coprono categorie di URL, categorie personalizzate e classificazioni di pagine dinamiche per i nuovi siti con una classificazione completa dell'utilizzo delle app cloud e policy per un uso accettabile che includono sia il cloud che il web.

Prevenzione delle minacce

Protezione contro malware e minacce sofisticate con funzionalità di difesa avanzate, dal riconoscimento delle istanze delle app cloud allo script di pre-esecuzione, alla macro-analisi e al rilevamento delle anomalie con apprendimento automatico.

Protezione dei dati, ovunque

Consente di seguire e proteggere i dati ovunque si trovino e garantisce un'ispezione accurata e precisa con funzionalità avanzate che spaziano dalla corrispondenza esatta alla creazione di impronte digitali con corrispondenza delle somiglianze.

Copertura dell'accesso diretto a Internet

Consente di eliminare i costosi backhaul e migliora le prestazioni per gli uffici e gli utenti remoti grazie all'accesso NewEdge ottimizzato per la bassa latenza e l'alta capacità. Fornisce un accesso diretto a Internet per uffici remoti con tunnel IPsec e GRE, oltre che per utenti remoti e mobili.

Contattare gli esperti per la sicurezza degli endpoint Dell dedicati all'indirizzo endpointsecurity@dell.com per saperne di più sui prodotti SafeData che possono migliorare il profilo di sicurezza dell'azienda

Source

* Netskope Threat Research Labs, 2019

** Google HTTPS Encryption Transparency Report, settembre 2019

*** 2019 Cloud Security Report, Cybersecurity Insiders