DELL Technologies

Dell SafeData

Passerelle Web sécurisée Netskope

Sécurité Web de nouvelle génération à partir du Cloud et pour le Cloud, protection des services Cloud, des applications, des sites Web et des données pour n'importe quel utilisateur, site ou appareil.

Aperçu rapide

- Trafic Web et contrôles de règles granulaires des applications, y compris les données, l'activité et le contexte
- Alertes de coaching basées sur le risque pour l'adoption par l'utilisateur des applications et des services Cloud
- Performances et échelle Cloud destinées à protéger chaque utilisateur, appareil et site
- Prévention des pertes de données pour les applications gérées et non gérées, ainsi que pour le trafic Web
- Logiciels malveillants et défenses contre les menaces avancées, sandboxing et plus de 40 sources d'intelligence sur les menaces
- Console Cloud unique avec contrôles de règles cohérents pour les fonctions SWG, CASB et DLP
- La plateforme de sécurité Cloud répond aux exigences du Programme fédéral de gestion des risques et des autorisations (FedRAMP) et a obtenu l'autorisation FedRAMP
- Transformation fédérale avec les solutions TIC 3.0 basées sur SASE

Présentation du produit

Aujourd'hui, une organisation moyenne utilise plus de 1 295 applications et services Cloud, dont plus de 95 % ne peuvent pas être gérés sans droits d'administration IT***. Les passerelles Web sécurisées doivent aller au-delà du filtrage d'URL traditionnel des demandes Web afin de décoder le trafic API des applications pour des milliers d'applications et de services Cloud. Cela permettra de comprendre et de protéger le contenu et le contexte. Les déploiements de sécurité Web à la volée nécessitent également des performances Cloud à la demande, en vue d'inspecter le trafic Web chiffré et l'échelle du Cloud avec un accès au Cloud distribué globalement pour les bureaux distants et les utilisateurs mobiles.

La transformation numérique dirigée par le Cloud et la mobilité continue de progresser : 85 % du trafic de passerelle Web est identifié via des applications et des services Cloud dans le Netskope Cloud Confidence Index*. De plus, 83 % du trafic Web est chiffré**, ce qui crée de nouveaux angles morts permettant la fuite de données et l'entrée de menaces pour les applications, les services Cloud et le trafic Web gérés et non gérés.

La SWG de nouvelle génération de Netskope est une solution de sécurité Web basée sur le Cloud qui arrête les logiciels malveillants, détecte les menaces avancées, filtre par catégorie, protège les données et contrôle l'utilisation des applications pour n'importe quel utilisateur, site et appareil. Il unifie nos CASB, SWG et DLP leaders sur le marché avec des contrôles de règles communs, le tout accompagné de rapports personnalisés et de métadonnées enrichies pour les requêtes ad hoc.

netskope

DELL Technologies

Principales fonctionnalités du produit

Secure Access Service Edge (SASE)

Une architecture SASE (Secure Access Service Edge) permet d'identifier les utilisateurs et les appareils, d'appliquer des contrôles de sécurité basés sur des règles et de fournir un accès sécurisé aux applications ou aux données appropriées. Ces fonctionnalités s'inscrivent directement dans la lignée de la plateforme de sécurité Cloud native de Netskope, conçue pour comprendre et protéger les environnements SaaS, Web et IaaS, tout en étant accessibles depuis n'importe quel appareil. Le tout à partir d'une console unique, avec une architecture unique et des règles intégrées pour tous les services SASE, y compris CASB, SWG et Accès privé.

Surveillance et évaluation

Bénéficiez d'une visibilité à la volée pour des milliers d'applications et de services Cloud gérés et non gérés, ainsi que pour le trafic Web, et unifiez les fonctionnalités stratégiques SWG, CASB et DLP en une plateforme SWG de nouvelle génération.

Contrôle des applications Cloud

Bénéficiez d'un contrôle granulaire et en temps réel de milliers d'applications Cloud, y compris celles dirigées par les lignes de produits et les utilisateurs. Vous pouvez ainsi arrêter les problèmes et soutenir les bonnes initiatives en toute sécurité.

Utilisation acceptable

Intégrez une combinaison de filtrage Web traditionnel couvrant les catégories d'URL, les catégories personnalisées et les évaluations dynamiques de pages pour les nouveaux sites, avec une évaluation complète de l'utilisation des applications Cloud et des politiques d'utilisation acceptable qui incluent à la fois le Cloud et le Web.

Protection contre les menaces

Protégez-vous contre les logiciels malveillants et les menaces avancées avec des fonctionnalités de défense avancée, de la détection des instances d'applications Cloud aux scripts de pré-exécution, en passant par l'analyse des macros et la détection des anomalies par apprentissage automatique.

Protéger les données, où qu'elles se trouvent

Suivez et protégez les données où qu'elles se trouvent et menez une inspection exacte et précise, avec des fonctionnalités avancées allant de la correspondance exacte à l'empreinte digitale, avec analyse de la similitude.

Couverture directe sur Internet

Éliminez la liaison terrestre coûteuse et améliorez les performances des bureaux et des utilisateurs distants grâce à l'accès NewEdge, optimisé pour offrir une faible latence et une haute capacité. Fournissez un accès direct à Internet pour les bureaux distants avec des tunnels IPsec et GRE, ainsi que pour les utilisateurs distants et mobiles.

Contactez votre spécialiste Dell Endpoint Security dédié dès aujourd'hui à l'adresse endpointsecurity@dell.com pour en savoir plus sur les produits SafeData, qui peuvent vous aider à améliorer votre posture de sécurité.

Source

* Netskope Threat Research Labs, 2019

** Google HTTPS Encryption Transparency Report, septembre 2019

*** 2019 Cloud Security Report, Cybersecurity Insiders

netskope