DELL Technologies

Dell SafeData

Netskope Secure Web Gateway

Websicherheit der nächsten Generation aus der Cloud für die Cloud – Schutz von Cloud-Services, Anwendungen, Websites und Daten für alle NutzerInnen, Standorte oder Geräte

Kurzübersicht

- Granulare Policy-Kontrollen für den Webdatenverkehr und -anwendungen, einschließlich Daten, Aktivität und Kontext
- Risikobasierte Coaching-Warnmeldungen für die nutzerbasierte Einführung von Anwendungen und Cloud-Services
- Cloud-Performance und -Skalierung zur Prüfung von allen NutzerInnen, Geräten und Standorten
- Vermeidung von Datenverlust bei verwalteten und nicht verwalteten Anwendungen sowie beim Webdatenverkehr
- Malware- und Advanced-Threat-Schutz, Sandboxing und mehr als 40 Threat-Intelligence-Feeds
- Eine einzige Cloud-Konsole mit konsistenten Policy-Kontrollen für SWG-, CASB- und DLP-Funktionen
- Security Cloud Platform: Erfüllung der FedRAMP-Anforderungen (Federal Risk and Authorization Management Program) und FedRAMP-Autorisierung
- Transformation auf Bundesebene mit SASE-basierten TIC 3.0-Lösungen

Produktübersicht

Heute nutzt ein durchschnittliches Unternehmen mehr als 1.295 Anwendungen und Cloud-Services, wobei über 95 % davon nicht verwaltet und ohne IT-Administrationsrechte sind.*** Sichere Webgateways müssen über die herkömmliche URL-Filterung von Webanforderungen hinausgehen und den API-Datenverkehr für Tausende von Anwendungen und Cloud-Services entschlüsseln, um Inhalte sowie Kontext zu verstehen und zu schützen. Inline-Websicherheitsbereitstellungen erfordern ebenfalls On-Demand-Cloud-Performance für die Prüfung des verschlüsselten Webdatenverkehrs und die Cloud-Skalierung mit global verteiltem Cloud-Zugriff für Remotestandorte und mobile NutzerInnen.

Die durch Cloud und Mobilität vorangetriebene digitale Transformation schreitet weiter voran, dabei werden 85 % des Webgateway-Datenverkehrs über Anwendungen und Cloud-Services im Netskope Cloud Confidence Index* identifiziert. Rund 83 % des Webdatenverkehrs werden verschlüsselt**, was zu neuen „blinden Flecken“ für verwaltete und nicht verwaltete Anwendungen, Cloud-Services sowie den Webdatenverkehr führt, die wiederum Datenlecks und das Eindringen von Bedrohungen begünstigen.

Das Netskope SWG der nächsten Generation ist eine Cloud-basierte Websicherheitslösung, die Malware verhindert, Advanced Threats erkennt, nach Kategorie filtert, Daten schützt und die Anwendungsnutzung für alle NutzerInnen, Standorte und Geräte steuert. Es vereint unsere branchenführenden CASB-, SWG- und DLP-Lösungen in gemeinsamen Policy-Kontrollen mit nutzerdefiniertem Reporting und umfangreichen Metadaten für Ad-hoc-Abfragen.

netskope

DELL Technologies

Wichtige Produkteigenschaften

Secure Access Services Edge (SASE)

Mit einer SASE(Secure Access Services Edge)-Architektur ist es möglich, NutzerInnen und Geräte zu identifizieren, Policy-basierte Sicherheitskontrollen anzuwenden und sicheren Zugriff auf die entsprechenden Anwendungen oder Daten zu bieten. Diese Funktionen sind direkt auf die Cloud-native Sicherheitsplattform von Netskope abgestimmt, die SaaS-, Web- sowie IaaS-Umgebungen erkennt und schützt, auf die von jedem Gerät aus zugegriffen werden kann. All das erfolgt über eine einzige Konsole mit einer einzigen Architektur sowie integrierten Policies für alle SASE-Services, darunter CASB, SWG und Private Access.

Monitoring und Bewertung

Erhalten Sie Inline-Sichtbarkeit für Tausende von verwalteten und nicht verwalteten Anwendungen, Cloud-Services sowie Webdatenverkehr. Vereinheitlichen Sie kritische SWG-, CASB- und DLP-Funktionen in einer SWG-Plattform der nächsten Generation.

Kontrolle von Cloud-Anwendungen

Profitieren Sie von der fein abgestimmten Echtzeitsteuerung von Tausenden Cloud-Anwendungen, einschließlich der Anwendungen von LOBs (Lines of Business) und NutzerInnen. Damit können Sie schädigende Elemente stoppen bzw. verhindern und gute sicher nutzen.

Zulässige Nutzung

Kombinieren Sie herkömmliche Webfilter für URL-Kategorien, nutzerdefinierte Kategorien und dynamische Seitenbewertungen für neue Websites mit umfassender Cloud-App-Nutzungsbewertung und Policies für zulässige Nutzung, die sowohl für die Cloud als auch das Web gelten.

Schutz vor Bedrohungen

Stellen Sie den Malware- und Advanced-Threat-Schutz mit umfassenden Abwehrfunktionen sicher, die von der Erkennung von Cloud-Anwendungsinstanzen über Skript- und Makroanalysen vor deren Ausführung bis zur Anomalieerkennung durch maschinelles Lernen reichen.

Schutz der Daten an jedem Ort

Verfolgen und schützen Sie die Daten an jedem Ort und sorgen Sie mit fortschrittlichen Funktionen, die von einer exakten Übereinstimmung bis zum Fingerabdruck mit Ähnlichkeitsvergleich reichen, für exakte und präzise Prüfungen.

Abdeckung für Direct-to-Internet

Eliminieren Sie kostspielige Rücktransporte und verbessern Sie die Performance für Remotestandorte sowie NutzerInnen mit dem NewEdge-Zugriff, der für niedrige Latenz und hohe Kapazität optimiert ist. Bieten Sie Direct-to-Internet-Zugriff über IPsec- und GRE-Tunnel für Remotestandorte sowie für Remote- und mobile NutzerInnen.

Wenden Sie sich noch heute unter endpointsecurity@dell.com an Ihren Dell Endpoint Security Specialist, um zu erfahren, wie Sie mit SafeData-Produkten Ihren Sicherheitsstatus verbessern können.

Source

* Netskope Threat Research Labs, 2019.

** Google HTTPS Encryption Transparency Report, September 2019.

*** 2019 Cloud Security Report, Cybersecurity Insiders.

netskope