Dezentralisierung der Netzwerksicherheit **Die Hauptmerkmale**

open systems

Warum es Zeit wird die Netzwerksicherheit zu überdenken

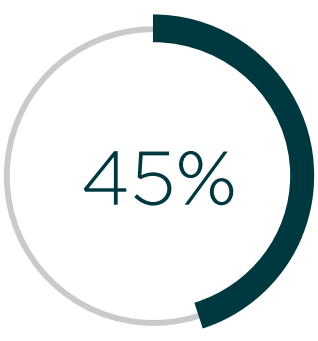
Die heutigen Unternehmensnetzwerke werden zunehmend dezentralisiert.

BISHER

- Arbeit findet in Büroräumlichkeiten statt
- Aufgaben und Anwendungen laufen über das Rechenzentrum
- Mitarbeiter arbeiten auf Geräten, die vom Unternehmen gestellt und verwaltet werden
- Sensible Daten befinden sich im Rechenzentrum
- User Traffic läuft über das Rechenzentrum
- Sicherheitsrichtlinien werden je nach Anforderungen neuer Apps und externer Benutzer zusammengeschustertt

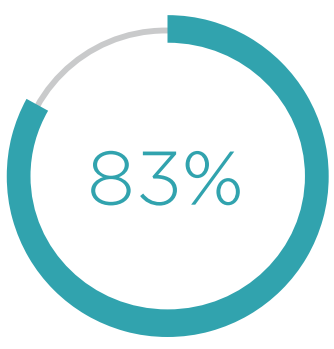
NEU

- Arbeit findet mehr und mehr ausserhalb der Büroräumlichkeiten statt
- Aufgaben und Anwendungen laufen in Hybrid- und Multi-Cloud-Umgebungen
- Mitarbeiter arbeiten auf privaten- und vom Unternehmen gestellten Geräten
- Sensible Daten werden in der Cloud gespeichert
- Mehr User Traffic in der öffentlichen Cloud und am Netzwerk Edge
- Bedarf an kontextbasierten, zentral verwalteten Sicherheitsrichtlinien



Weniger als die Hälfte der IT-Führungskräfte wissen, wie viele SaaS-Anwendungen in ihrem Unternehmen im Einsatz sind [1]

Cloud-Dienste unter IT-Governance [2]



Der Unternehmensauslastung sind Schätzungen zufolge bis 2020 in der Cloud[3]

ZENTRALISIERTE SICHERHEIT IN EINER DEZENTRALISIERTEN WELT

Da sich immer mehr Nutzer, Geräte, Anwendungen, Dienste und Daten ausserhalb des Unternehmens befinden, benötigen Unternehmen in einer **dezentralisierten Welt** eine **zentrale, Zero-Trust Sicherheitslösung**.

2/3

Der Unternehmen sehen beim Thema **Sicherheit** in der Cloud die grössten Herausforderungen.[4]

DIE ZUKUNFT IST SASE

Nach der Definition von Gartner ist **Secure Access Service Edge** (SASE) ein aufkommender, primär Cloud-basierter Service, der **umfassende WAN- und Netzwerksicherheitsservices** kombiniert, um dynamische und sichere Zugriffsanforderungen digitaler Unternehmen zu unterstützen.[5]

SASE IM TREND

Unternehmen, die bis 2023 SWG-, CASB-, ZTNA- und FWaaS-Funktionen von einem einzigen Anbieter beziehen werden, gestiegen von <5% in 2019[6]

Unternehmen, die im Jahr 2024 explizite SASE-Einführungsstrategien haben werden, gestiegen von <1% von Ende 2018.[7]

KONTROLLE ÜBER IHR NETZWERK

Endpoint Identities – Benutzer, Geräte, Zweigstellen, IoT-Geräte usw. – sind die neue Grundlage für sichere Zugriffsrichtlinien, nicht das Rechenzentrum. SASE bietet einen richtlinienbasierten, softwaredefinierten und sicheren Zugriff über eine unendlich massgeschneiderte Netzwerkstruktur.

Der Sicherheitsperimeter befindet sich dort, wo das Unternehmen ihn benötigt, während Latenzprobleme verschwinden.

Wenn Sie mehr über SASE und die Zukunft der Netzwerkverwaltung und Sicherheit erfahren möchten, laden Sie den kostenlosen Gartner Bericht herunter, *Competitive Landscape: Managed SD-WAN Services*.

GARTNER BERICHT HERUNTERLADEN

[1]Pulse Q&A, *Research Report: SaaS Application Management*, März 2019
[2]Netskope, *Cloud Bericht*
[3-4]Logic Monitor, *83% of Enterprise Workloads Will Be in the Cloud by 2020*, Januar 8, 2018
[5-7]Gartner, *The Future of Network Security Is in the Cloud*, August 30, 2019

open systems

WE'RE IN THIS TRANSFORMATION TOGETHER.

Open Systems ist Pionier im Bereich Secure Access Service Edge (SASE), der es Unternehmen ermöglicht, Netzverbindungen intern, zur Cloud und zum Rest der Welt herzustellen. Mit der Cloud-Architektur, dem Secure Service Edge, dem hybriden Cloud-Support, dem 7x24-Kontakt zu Level-3-Ingenieuren und der Predictive Analytics bietet SASE von Open Systems eine Komplettlösung für Netzwerke und IT-Sicherheit. Weitere Informationen unter open-systems.com.

open-systems.com