

Schließen der Lücke in der IT Sicherheit:

Der Stand bei Zero Trust- und SASE-Sicherheits architekturen 2023

Vermehrte hybride Arbeit, die zunehmende Nutzung des IoT und unnachgiebige Cyberangriffe: All dies führt dazu, dass Unternehmen vor größeren Sicherheitsherausforderungen stehen als je zuvor. Neue Herausforderungen erfordern die Einführung neuer Sicherheitsmodelle. Architekturen mit Zero Trust und SASE (Secure Access Service Edge) halten folgende Versprechen:



Vernetzte Sicherheit vom Edge bis zur Cloud



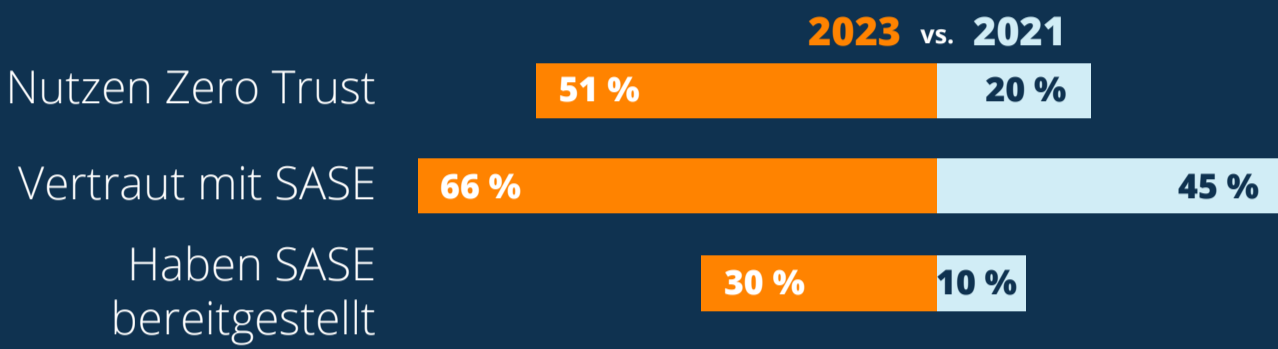
Reduzierung von Cyberrisiken durch dynamische Durchsetzung des Zugriffs auf Ressourcen nach dem Prinzip der „geringsten Privilegien“



Ermöglichung von sicherem Zugriff auf Unternehmensanwendungen von überall aus

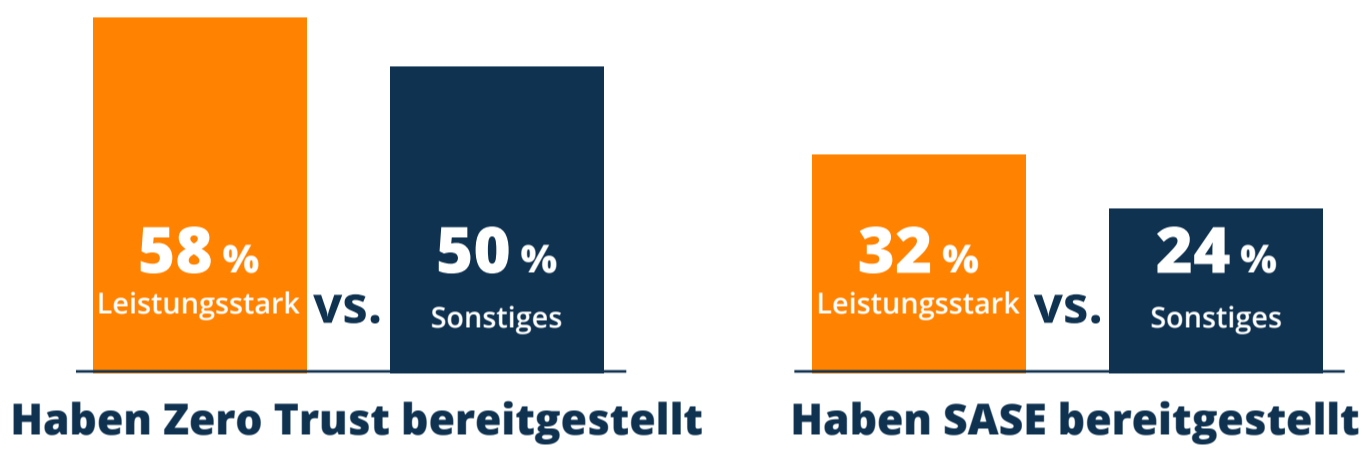
Was für Veränderungen gibt es bei Sicherheitsarchitekturen?

Die Einführung von Zero Trust und SASE-Sicherheit hat sich in den vergangenen zwei Jahren beschleunigt. Haben Sie die Nase vorn?



Was machen leistungsstarke Unternehmen anders?

Leistungsstarke Unternehmen richten eher Zero Trust- und SASE-Architekturen ein.



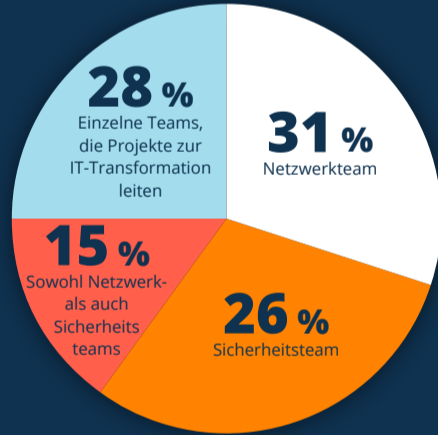
Wer trifft Entscheidungen hinsichtlich der Sicherheitsarchitektur?

Bei vielen Unternehmen leiten Netzwerkteams die Sicherheitsentscheidungen, doch es entstehen auch neue Entscheidungsgremien: einzelne Projekt teams, die Projekte zur IT Transformation leiten.

Leistungsstark

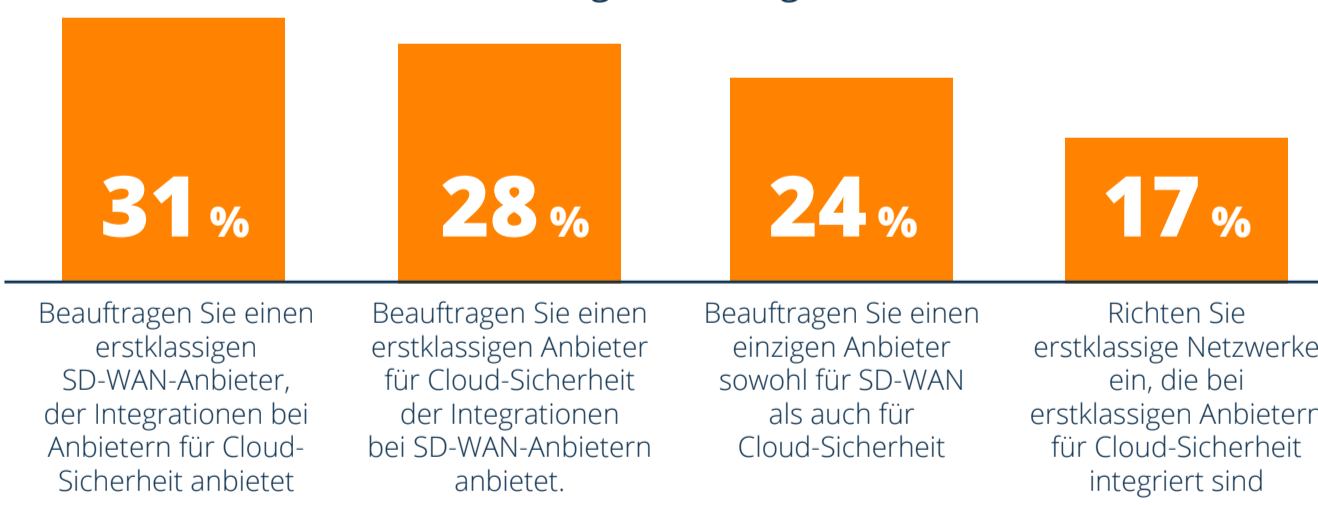


Gesamt



Planen Sie die Implementierung einer neuen Sicherheitsarchitektur?

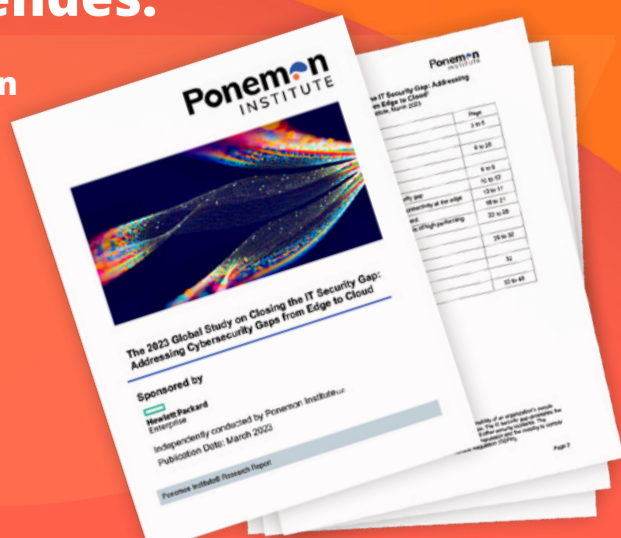
Wenn es um die Bereitstellung ihrer SASE-Architekturen geht, sind die Präferenzen der Teilnehmenden bei der Auswahl von erstklassigem SD-WAN, erstklassiger Cloud-Sicherheit sowie SD-WAN und Cloud-Sicherheit aus einer Hand fast gleichmäßig verteilt.



Die Kombination von fortschrittlichem, sicherem, SD-WAN mit den bestmöglichen Kapazitäten von SSE (Security Service Edge) ist eine effektive Möglichkeit, Cloud-basierte Sicherheitsservices in bestehende Netzwerk- und Sicherheitsinfrastruktur zu integrieren. Ein Ansatz mit nur einem einzigen Anbieter bietet evtl. mehr Einfachheit.

In diesem ausführlichen Bericht erfahren Sie mehr über Folgendes:

- Nutzungsraten und Bereitstellungspräferenzen von Zero Trust- und SASE-Lösungen
- Die Rolle von Zero Trust und SASE bei der Schließung der IT-Sicherheitslücke
- Die Bedeutung der Transparenz bei der Schließung von IT-Sicherheitslücken
- Wie Ihre Umstellung auf Zero Trust- und SASE-Frameworks im Vergleich Unternehmen mit besonders effektiver Netzwerksicherheit und Implementierung abschneidet



[Bericht lesen →](#)