

DIE ZUKUNFT DES SICHEREN NETZWERKS

Der Wechsel von zugesetzter zu integrierter Sicherheit

Jetzt starten >

Die Welt hat sich verändert und mit ihr die Sicherung eines Netzwerks. Heutzutage greifen immer mehr Benutzer von überall auf das Netzwerk zu. IoT-Geräte (die möglicherweise nicht über strenge Sicherheitsvorkehrungen verfügen) erfreuen sich zunehmender Beliebtheit und immer mehr Anwendungen werden in die Cloud verlagert, außerhalb der Reichweite und des Schutzes des Unternehmensnetzwerks.

Da diese Faktoren die Angriffsfläche vergrößern, sind herkömmliche Lösungen, die den Netzwerkumfang mit zusätzlichen Produkten wie Firewalls und virtuellen privaten Netzwerken (VPNs) sichern, nicht mehr in der Lage, die Sicherheit des Netzwerks zu gewährleisten.

Faktoren, die zu einer Zunahme von Cyberangriffen führen

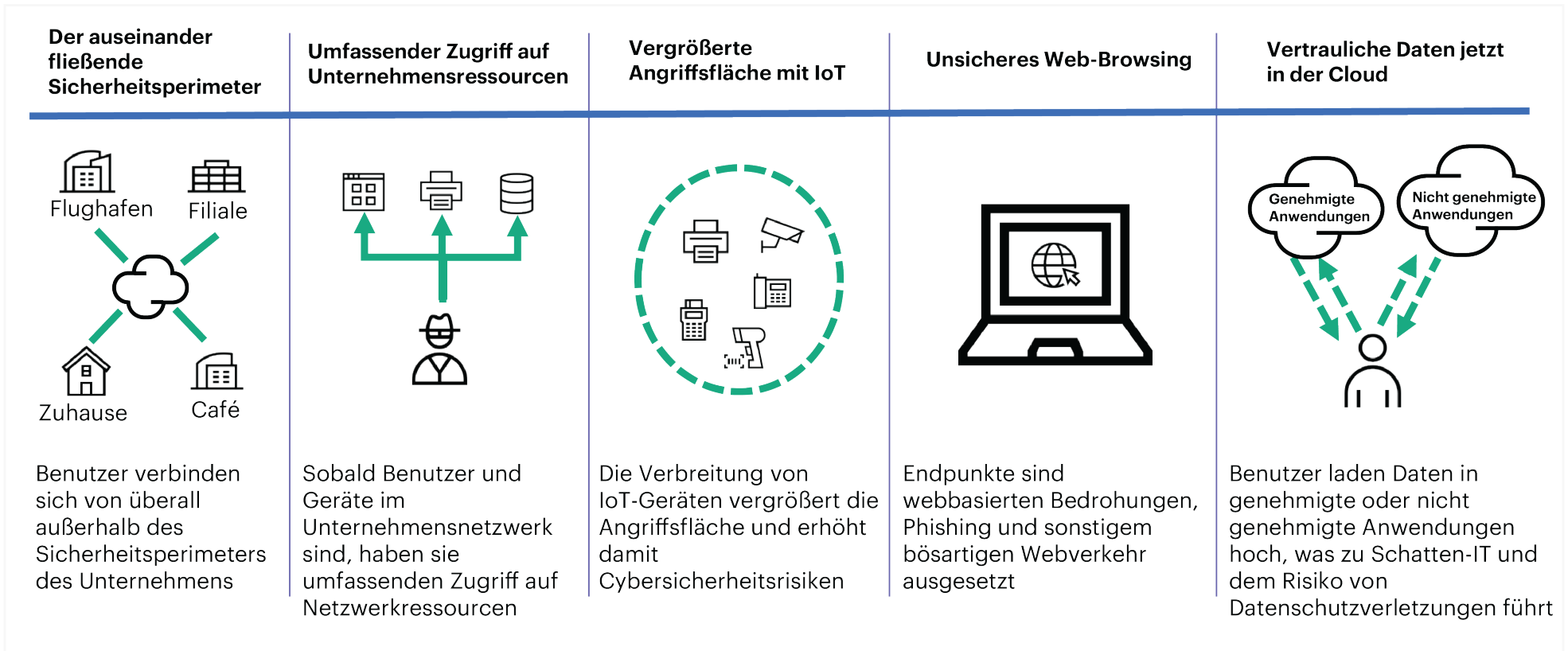


Abbildung 1. Zu den neuen Netzwerkschwachstellen zählen die Auflösung von Sicherheitsperimetern, ein breiterer Zugriff auf Unternehmensressourcen, mehr IoT-Geräte und Cloud-Anwendungen sowie unsicheres Web-Browsing und unsichere Cloud-Anwendungen

Sicherheitsansätze neu überdenken

Es ist Zeit, über den Tellerrand hinaus zu blicken

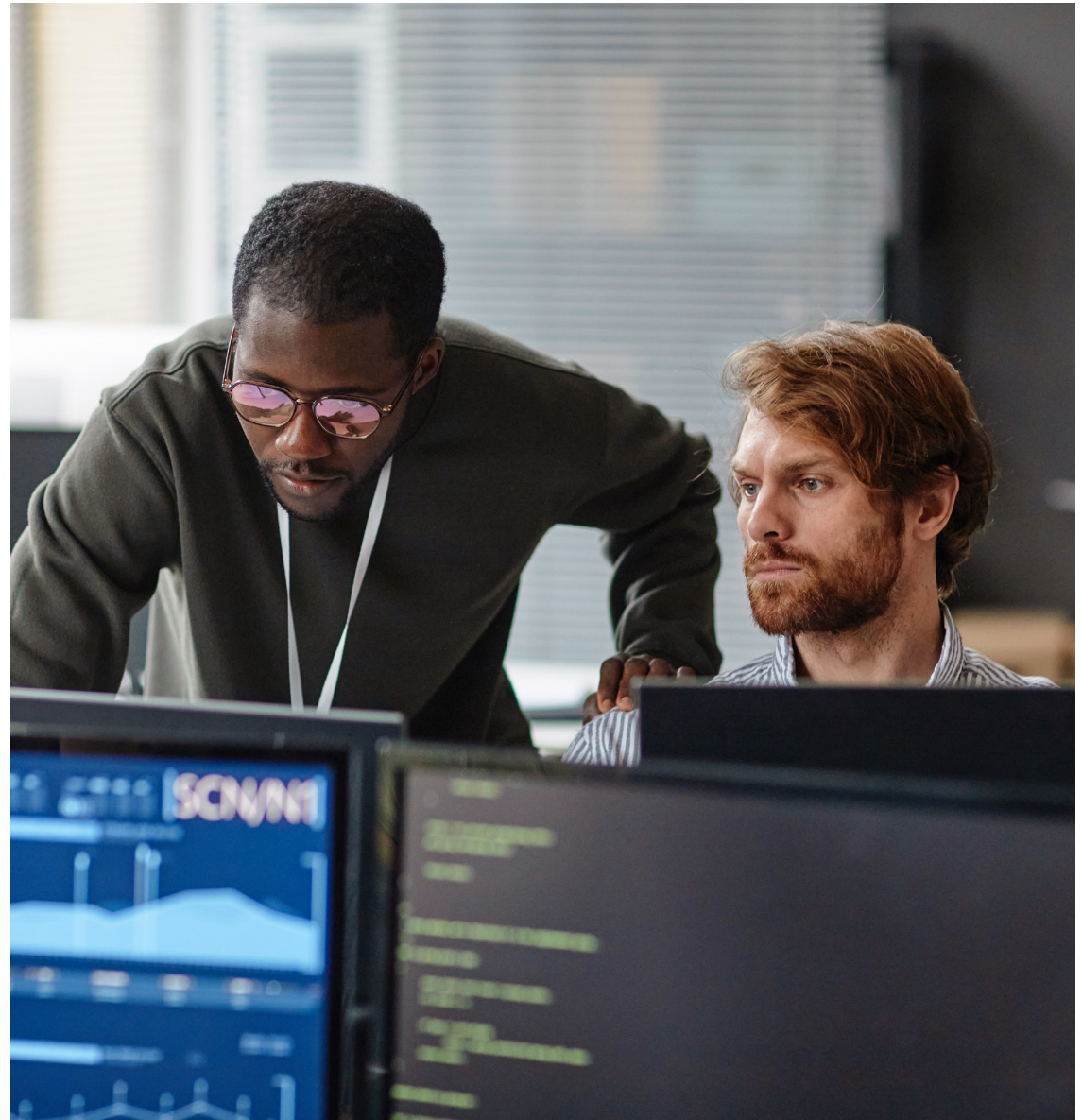
Perimeterbasierte Lösungen bergen Risiken, da sie Benutzer, Geräte und Anwendungen nicht kontinuierlich überprüfen können, sobald sie im Netzwerk sind. Doch über diese Einschränkung hinaus können sie auch selbst Sicherheitsrisiken schaffen. VPNs erfordern jedes Mal, wenn sich ein Benutzer mit dem Netzwerk verbindet, eine Öffnung in der Firewall – und vergrößern damit die Angriffsfläche für Cyberangriffe. Und je mehr Firewalls zum Sicherheits-Stack hinzugefügt werden, desto mehr Silos und Sicherheitslücken entstehen. Dadurch steigt nicht nur das Angriffsrisiko, sondern auch die Komplexität, was die Konnektivität und die Netzwerkleistung beeinträchtigen kann.

Es wird Zeit, Sicherheit und Netzwerkbetrieb zu verknüpfen

Die Sicherheitslandschaft wird noch dadurch komplizierter, dass Sicherheits- und Netzwerkteams manchmal unterschiedlicher Meinung sind. Netzbetreiber stehen unter dem ständigen Innovationsdruck, der eine höhere Zuverlässigkeit und Abdeckung des Netzwerks erfordert.

Die Implementierung von Lösungen zur Erfüllung geschäftlicher Anforderungen kann zu unnötigen Risiken für das Unternehmen führen.

Wie können Unternehmen in dieser neuen Welt gewährleisten, dass die Verbindungen zwischen Personen, Geräten und Anwendungen – wo auch immer sie sich befinden – sicher bleiben und dabei gleichzeitig dem Bedürfnis nach Sicherheit und Verbindung gerecht werden? Es ist ein neuer Ansatz erforderlich: Ein Ansatz, der Sicherheitsservices vom Edge bis zur Cloud bereitstellen kann.



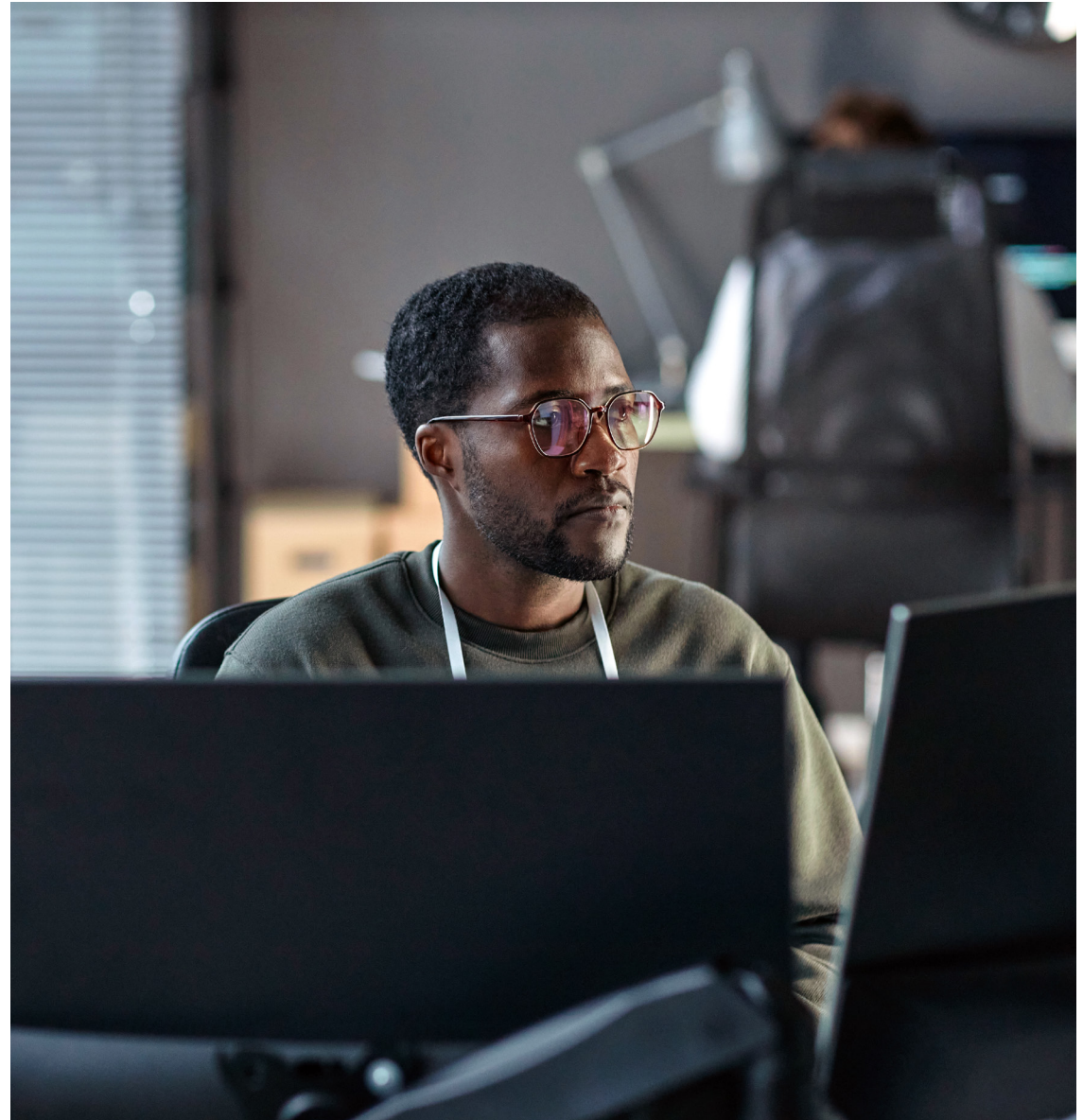
Ein neues Paradigma: Das Netzwerk als Sicherheitslösung

Die Antwort auf diese Herausforderungen besteht darin, das Netzwerk selbst in eine Sicherheitslösung zu verwandeln. Aber was bedeutet das? Es bedeutet, dass man ein Netzwerk hat, in dem die Sicherheit von Anfang an integriert ist, einschließlich:

- Unterstützung für **SASE** und **Zero Trust** mit Cloud-basierter Zugriffssteuerung
- Firewalls der nächsten Generation, Angriffserkennung, Angriffsverhinderung und adaptive DDoS-Abwehr

Auf dieser Grundlage können Netzwerke eine aktive Rolle beim Schutz von Benutzern, Geräten und Anwendungen spielen: Sie brechen durch Firewalls bedingte Silos auf, beseitigen durch VPN verursachte Risiken und blockieren böswillige Akteure vor dem Eindringen über unbediente IoT-Geräte. Dabei können die Ziele der Netzwerk- und auch der Sicherheitsteams mit einem Netzwerk erreicht werden, das hohe Leistung und unterbrechungsfreien Zugriff bei geringstmöglichem Risiko bietet.

Indem das Netzwerk als Sicherheitslösung etabliert wird, können sich Sicherheitsteams auf das Netzwerk als integralen Bestandteil ihres Sicherheitsökosystems verlassen.



Was ist Zero Trust? Die Grundprinzipien.

**Niemals
vertrauen,
immer
prüfen**

Der Zugriff wird basierend auf Identität, Kontext und kontinuierlicher Überprüfung gewährt

**Geringstmögliche
Zugriffsrechte**

Benutzer und Geräte erhalten nur Zugriff auf das, was sie benötigen, wodurch die Angriffsfläche reduziert wird

Mikrosegmentierung

Verhindert seitliche Bewegungen und begrenzt so mögliche Verstöße

Universell

Setzen Sie Zero Trust überall und auf jedem Gerät (verwaltet, nicht verwaltet, IoT) konsequent durch

Abbildung 2. Zero Trust-Prinzipien: Niemals vertrauen, immer überprüfen; Mikrosegmentierung; Zugriff mit geringsten Rechten; universelle Durchsetzung

Weiter



Was ist SASE?

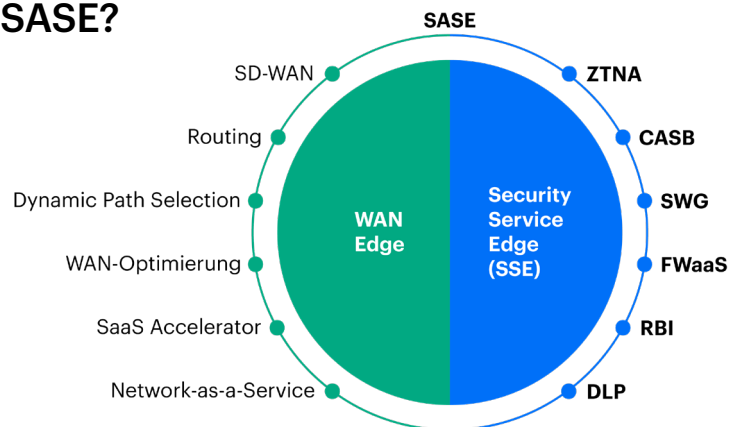


Abbildung 3. Die Komponenten von SASE

SASE ist eine Kombination aus sicherem SD-WAN und Security Service Edge (SSE). Durch die Zusammenführung dieser beiden Elemente bietet SASE sicheren und optimierten Zugriff auf Anwendungen und Daten von jedem Benutzer oder Gerät aus, unabhängig vom Standort. SASE setzt Zero Trust-Prinzipien durch und verbessert so die Sicherheit, Leistung und Agilität für hybrides Arbeiten und die Cloud-Einführung.

SASE bietet außerdem ein gemeinsames Netzwerk- und Sicherheitsframework und eine gemeinsame Toolbox, wodurch die Implementierung von Richtlinien vereinfacht und sichergestellt wird, dass Richtlinien im gesamten Netzwerk vom Edge bis zur Cloud durchgesetzt werden. Das Ergebnis? Verbesserte Netzwerkleistung, Effizienz und Zuverlässigkeit, reduzierte Komplexität, optimierte Fähigkeit zur Einhaltung der gesetzlichen Compliance und bessere Zusammenarbeit zwischen den Netzwerk- und Sicherheitsteams.

SASE = Sicheres SD-WAN + SSE

Sicheres SD-WAN

Verbindet Zweigstellenbenutzer sicher mit Anwendungen, die in der Cloud oder in Hybrid Cloud-Umgebungen gehostet werden. Dabei wird eine virtuelle WAN-Architektur verwendet, um jede Kombination aus Breitband-, LTE- und MPLS-Verbindungen zu nutzen. Es lenkt den Datenverkehr intelligent in die Cloud, vermeidet so leistungsmindernde Backhaul-Verbindungen zum Rechenzentrum und reduziert gleichzeitig die MPLS-Abhängigkeit und die Infrastrukturkosten.

Zu den sicheren SD-WAN-Lösungen gehören integrierte Firewalls, die zugesetzte Firewalls und Router ersetzen, um die Hardwarestellfläche in Zweigstellen zu optimieren.

SSE

Ermöglicht von überall aus durchgängig sicheren Zugriff auf das Web, SaaS-Anwendungen und private Anwendungen. Es umfasst erweiterte Sicherheitsfunktionen wie Zero Trust Network Access (ZTNA), Secure Web Gateway (SWG), Cloud Access Security Broker (CASB) und Firewall as-a-Service (FWaaS).

Eine einheitliche SSE-Plattform vereinfacht die Sicherheit. Das IT-Team muss die Zugriffsrichtlinien nicht mehr mehrfach in verschiedenen Sicherheitsprodukten einrichten, was mühsame Arbeit überflüssig macht. Jetzt gibt es für alles eine einzige Schnittstelle. Und noch besser: Diese Richtlinien werden von der Cloud aus überall einheitlich durchgesetzt. Wenn sich die Richtlinien ändern, werden diese Aktualisierungen auch sofort und universell vorgenommen.

Weiter



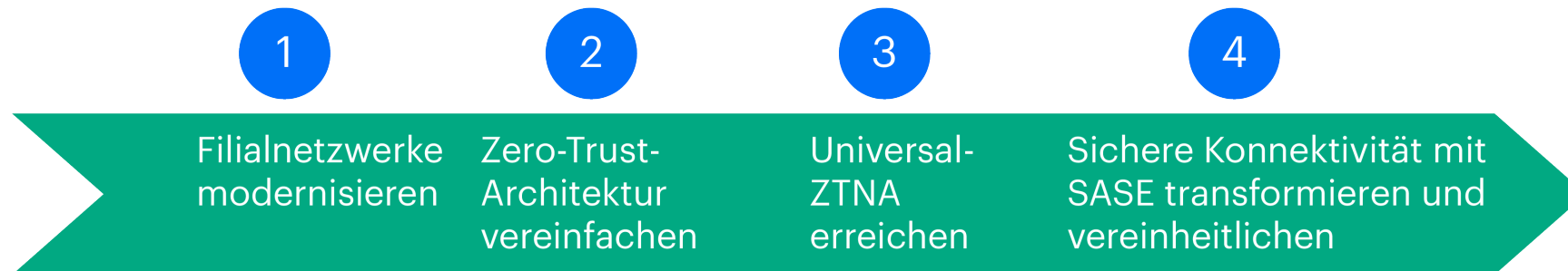
Der einfache Weg zu SASE und Zero Trust vom Edge bis zur Cloud

SASE und Zero Trust sind der Weg in die Zukunft. Wir sind uns jedoch bewusst, dass Implementierungen komplex und überwältigend sein können.

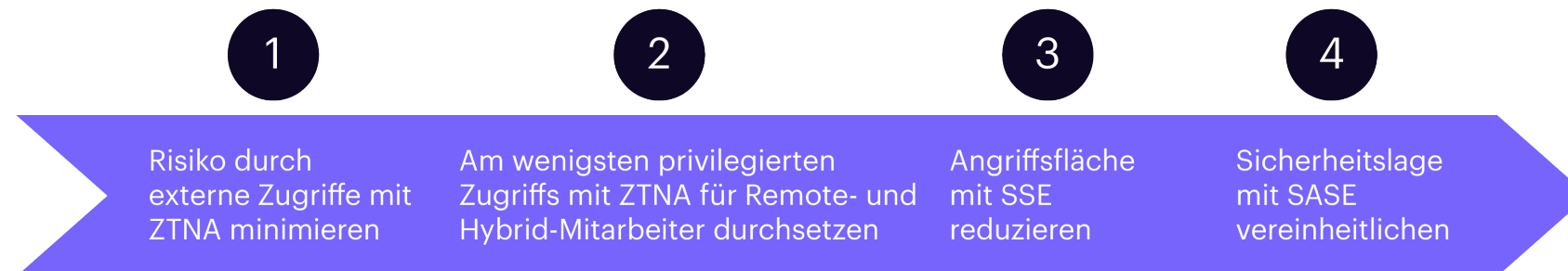
Für den Umstieg auf SASE und Zero Trust gibt es zwei Möglichkeiten: einen netzwerkorientierten oder einen sicherheitsorientierten Ansatz.

Bei einem netzwerkorientierten Ansatz steht die Modernisierung und Vereinfachung der Netzwerkinfrastruktur im Vordergrund, während bei einem sicherheitsorientierten Ansatz der Schwerpunkt zunächst auf der Verringerung von Risiken und der Durchsetzung strenger Sicherheitsmaßnahmen liegt. Keiner von beiden ist besser als der andere – es hängt ganz von Ihren geschäftlichen Prioritäten ab.

Netzwerkorientierter Ansatz



Sicherheitsorientierter Ansatz



Der Unterschied mit HPE Networking

- Integriertes Zero Trust
- Integrierte Firewalls der nächsten Generation
- Einheitliche Definition und Ausführung von Richtlinien
- Interoperabilität mit Produkten von Drittanbietern
- Offenes SASE-Ökosystem

Netzwerke in Sicherheitslösungen verwandeln

Bisher verwendete Sicherheitslösungen können mit der heutigen hybriden Welt der IoT-Geräte, in der alles in der Cloud stattfindet, nicht Schritt halten. Vertrauen Sie Ihr Netzwerk nicht veralteter Technologie an. Machen Sie daraus eine Sicherheitslösung mit integrierter Sicherheit, die die Prinzipien des Zero Trust vom Edge bis zur Cloud umsetzt und so für verbesserten Schutz und Compliance sorgt. Holen Sie alles aus Ihrem Netzwerk heraus, was Sie brauchen: hohe Leistung bei geringstmöglichem Risiko.

Weitere Informationen finden Sie unter

[HPE.com/Networking](https://www.hpe.com/Networking)

HPE.com besuchen

[Jetzt chatten](#)

© Copyright 2025 Hewlett Packard Enterprise Development LP. Die hier enthaltenen Informationen können jederzeit ohne vorherige Ankündigung geändert werden. Neben der gesetzlichen Gewährleistung gilt für Produkte und Services von Hewlett Packard Enterprise (HPE) ausschließlich die Herstellergarantie, die in den Garantieerklärungen für die jeweiligen Produkte und Services explizit genannt wird. Aus dem vorliegenden Dokument sind keine weiterreichenden Garantieansprüche abzuleiten. Hewlett Packard Enterprise haftet nicht für hierin enthaltene technische oder redaktionelle Fehler oder Auslassungen.

a00147879DEE, Rev. 1

HEWLETT PACKARD ENTERPRISE

[hpe.com](https://www.hpe.com)

