

## Aktuelle treibende Faktoren für die Neubeurteilung von Unternehmensnetzwerken und Cloud-Security im deutschsprachigen Europa

### Digitalisierung und Cloud-Transformation

- Die fortschreitende Digitalisierung und der massive Umstieg auf Cloud-Dienste führen dazu, dass klassische Netzwerkinfrastrukturen (z. B. MPLS) an ihre Grenzen stoßen. Unternehmen benötigen heute flexible, skalierbare und leistungsfähige Netzwerke, um Cloud-Anwendungen, SaaS und hybride Arbeitsmodelle effizient und sicher zu unterstützen <sup>[1][2]</sup>.
- Die Pandemie hat den Trend zu Remote Work und Multi-Cloud-Lösungen beschleunigt, wodurch die Anforderungen an Netzwerkperformance, Verfügbarkeit und Sicherheit massiv gestiegen sind <sup>[3][2]</sup>.

### Wachsende Netzwerkkomplexität und Flexibilitätsbedarf

- Mit der Zunahme von Remote-Arbeit und der Verlagerung von Anwendungen in die Cloud müssen CIOs sicherstellen, dass alle Standorte und Mitarbeitenden sicher und performant angebunden sind, ohne die Komplexität und Kosten der Netzwerke zu erhöhen <sup>[4][2]</sup>.
- SD-WAN-Lösungen bieten hier Vorteile durch zentrale Steuerung, dynamisches Routing und die Möglichkeit, verschiedene Verbindungstypen (MPLS, Breitband, LTE, 5G) flexibel zu kombinieren<sup>[2]</sup>.

### Cybersecurity, Zero Trust und Compliance

- Die Bedrohungslage durch Cyberangriffe nimmt zu, gleichzeitig steigen die regulatorischen Anforderungen (z. B. DSGVO/GDPR, BSI C5-Testat in Deutschland). Unternehmen müssen ihre Sicherheitsarchitekturen kontinuierlich anpassen, um Daten und Systeme zu schützen <sup>[5][4]</sup>.
- Zero Trust-Architekturen und die Integration von Sicherheitsfunktionen direkt ins Netzwerk (z. B. SASE, Verschlüsselung, zentrale Richtlinienverwaltung) werden immer wichtiger, um den Schutz auch in dezentralen und cloudbasierten Umgebungen zu gewährleisten <sup>[4][2]</sup>.
- Compliance und Datenschutz sind zentrale Treiber, insbesondere in regulierten Branchen wie Finance, Healthcare und Industrie <sup>[6][4]</sup>.

### Kosten- und Effizienzdruck

- Klassische WAN-Architekturen sind oft teuer, schwer skalierbar und bieten wenig Flexibilität. SD-WAN und moderne Cloud-Security-Lösungen ermöglichen eine effizientere Nutzung von Ressourcen, zentrale Verwaltung und Kosteneinsparungen durch optimierte Bandbreitennutzung und geringeren Hardwarebedarf<sup>[1][2]</sup>.
- Unternehmen erwarten von neuen Lösungen eine bessere Balance zwischen Investitionssicherheit, Zukunftsfähigkeit und Betriebskosten <sup>[4][7]</sup>.

### Skalierbarkeit und M&A-Fähigkeit

- Unternehmenswachstum, Internationalisierung oder Fusionen und Übernahmen (M&A) erfordern Netzwerklösungen, die sich schnell und kosteneffizient an neue Standorte und Organisationsstrukturen anpassen lassen. SD-WAN und cloudbasierte Security-Architekturen bieten hier entscheidende Vorteile <sup>[4][2]</sup>.

**Technologische Innovationen (5G, IoT, SASE)**

- Die Einführung von 5G und die zunehmende Verbreitung von IoT-Geräten erhöhen die Anforderungen an Bandbreite, Latenz und Sicherheit. SD-WAN kann die Vorteile von 5G optimal nutzen und so neue Anwendungsfälle ermöglichen <sup>[6]</sup>.
- SASE (Secure Access Service Edge) vereint Netzwerk- und Sicherheitsfunktionen in einer cloudbasierten Plattform und adressiert damit die Herausforderungen moderner, dezentraler IT-Landschaften <sup>[4]</sup>.

**Zusammenfassung der wichtigsten Treiber**

Faktor	Beschreibung
Digitalisierung & Cloud	Bedarf an flexiblen, performanten Netzwerken für Cloud- und SaaS-Anwendungen
Remote Work & Mobilität	Sichere, ortsunabhängige Anbindung aller Mitarbeitenden
Cybersecurity & Compliance	Schutz vor Cyberangriffen, Einhaltung regulatorischer Vorgaben (DSGVO, BSI C5 etc.)
Kosten- & Effizienzdruck	Reduktion von Betriebskosten, zentrale Verwaltung, bessere Ressourcennutzung
Skalierbarkeit & M&A	Schnelle Integration neuer Standorte/Unternehmen, flexible Anpassung an Wachstum
Technologische Innovationen	Nutzung von 5G, IoT, SASE für mehr Performance, Sicherheit und neue Geschäftsmodelle

Diese Faktoren führen dazu, dass IT-Verantwortliche und CIOs im deutschsprachigen Europa und besonders in der Schweiz ihre WAN-, SD-WAN- und Cloud-Security-Strategien neu evaluieren, um die Wettbewerbsfähigkeit, Sicherheit und Zukunftsfähigkeit ihrer Unternehmen zu gewährleisten<sup>[6][4][2]</sup>.

**Quellen:**

1. <https://www.swissict.ch/sd-wan-warum-das-digitale-business-neue-anforderungen-an-die-weitverkehrsnetze-stellt/>
2. <https://itsecurityschweiz.ch/sd-wan/>
3. <https://www.netzwoche.ch/news/wo-schweizer-it-entscheider-prioritaeten-setzen>
4. <https://aveniq.ch/sase/>
5. <https://www.paloaltonetworks.de/company/press/palo-alto-networks-cloud-security-services-receive-c5-attestation-meeting-high-german-standards>
6. <https://www.marketdataforecast.com/market-reports/europe-sd-wan-software-defined-wide-area-network-market>
7. <https://www.inseya.ch/de/was-beschaefigt-einen-cio-in-der-heutigen-it-welt-einen-einblick-in-5-strategische-projekte>

**Kontakt:**

Marcel Koenig  
Principal Consultant  
[marcel.koenig@ancoma.org](mailto:marcel.koenig@ancoma.org)  
[linkedin.com/in/koenigmarcel](https://www.linkedin.com/in/koenigmarcel)  
[www.ancoma-global.com](https://www.ancoma-global.com)

31.07.2025