Magenta Security SASE

Managed SASE Service by Deutsche Telekom

ERLEBEN, WAS VERBINDET.

MARKUS MIELICH
Security Sales Expert

TELEKOM SECURITY GMBH
Fasanenweg 5, Leinfelden-Echterdingen 70771
Mobil +49 175 5826000
E-Mail markus.mielich@telekom.de

Die Deutsche Telekom Security auf einen Blick

Telekom Security

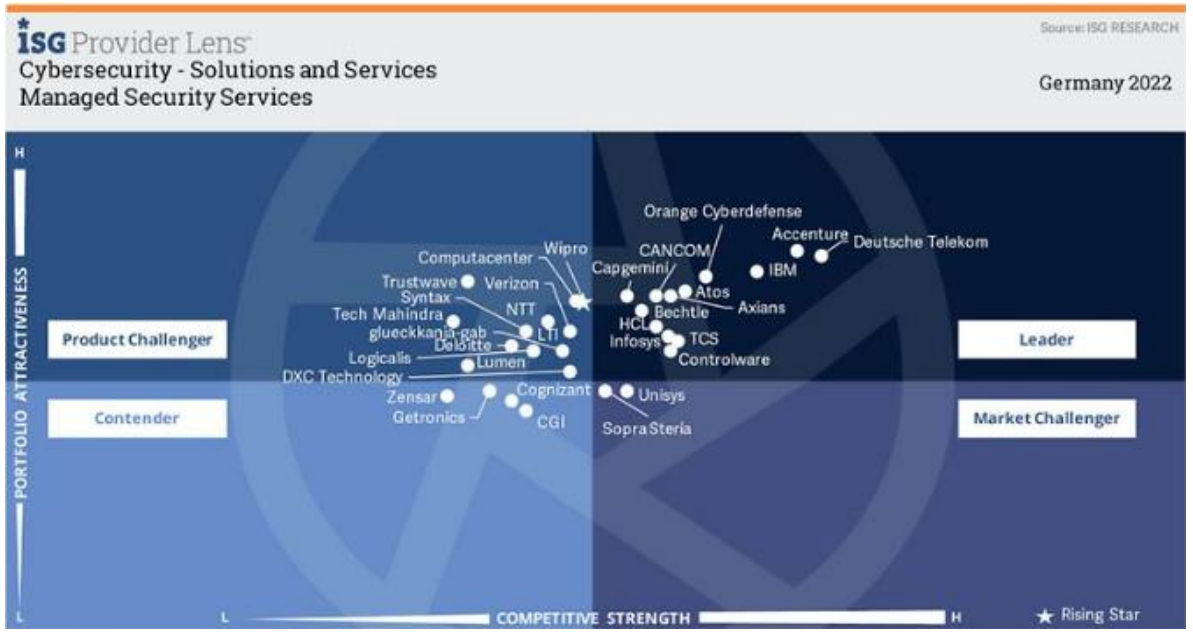
Deutsche Telekom Security GmbH

- Security **“Made in Germany”** (Management, Hosting)
- **“Leading edge”** Security KnowHow
- > 1.600 **Security Experten** weltweit
- Einsatz der gleichen **hochprofessionellen Tools** intern und extern
- Weltgrößte **Threat Intelligence Databank**
- Europas **größtes** integriertes **CDC/SOC**
- **Zero Impact** approach

Telekom Security

Deutsche Telekom Security GmbH

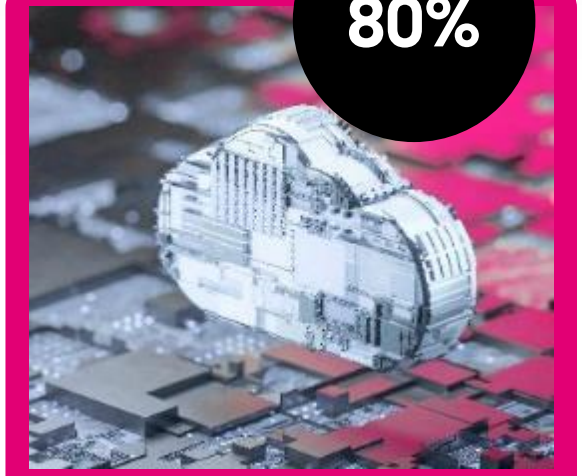
- Security **“Made in Germany”** (Management, Hosting)
- **“Leading edge”** Security KnowHow
- > 1.600 **Security Experten** weltweit
- Einsatz der gleichen **hochprofessionellen Tools** intern und extern
- Weltgrößte **Threat Intelligence Databank**
- Europas **größtes** integriertes **CDC/SOC**
- **Zero Impact** approach



Was ist SASE?

Kundenherausforderungen

80%



Cloud first

die wichtigsten Geschäftsanwendungen werden in die Cloud verlagert

80%

Mobile first

Hybride Arbeitsweise bei Mitarbeitern, (IoT)-Geräte sind verteilt

+10%

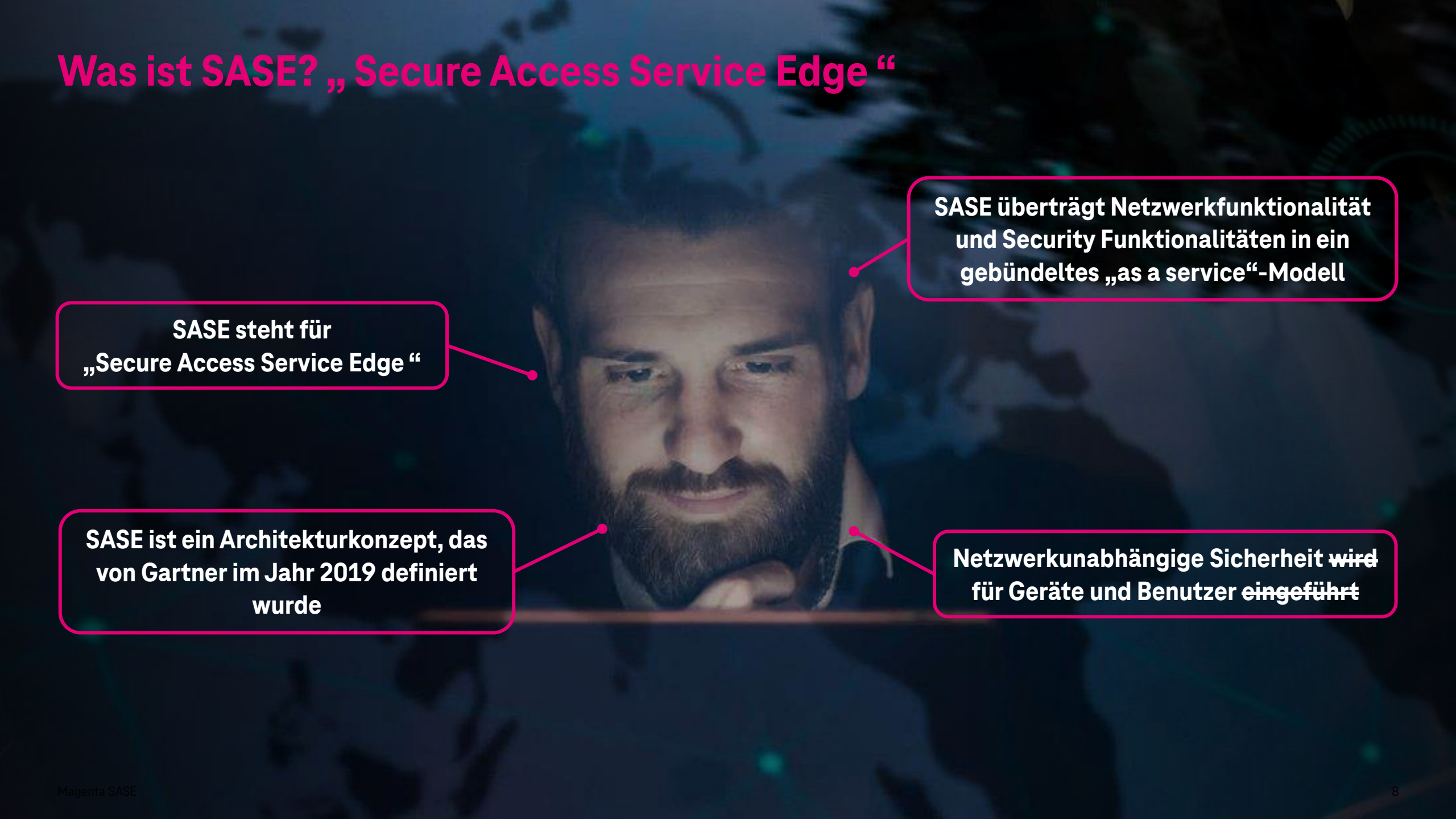
Neue Apps

Steigerung bei der Anzahl der Apps im Unternehmen pro Jahr

+400%

Mehr und mehr Cyberattacken

Was ist SASE? „ Secure Access Service Edge “



SASE steht für „Secure Access Service Edge “

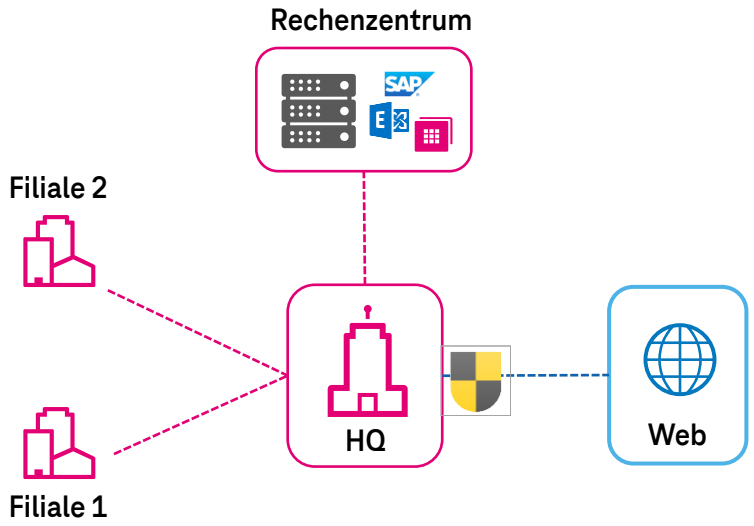
SASE überträgt Netzwerkfunktionalität und Security Funktionalitäten in ein gebündeltes „as a service“-Modell

SASE ist ein Architekturkonzept, das von Gartner im Jahr 2019 definiert wurde

Netzwerkunabhängige Sicherheit ~~wird~~ für Geräte und Benutzer ~~eingeführt~~

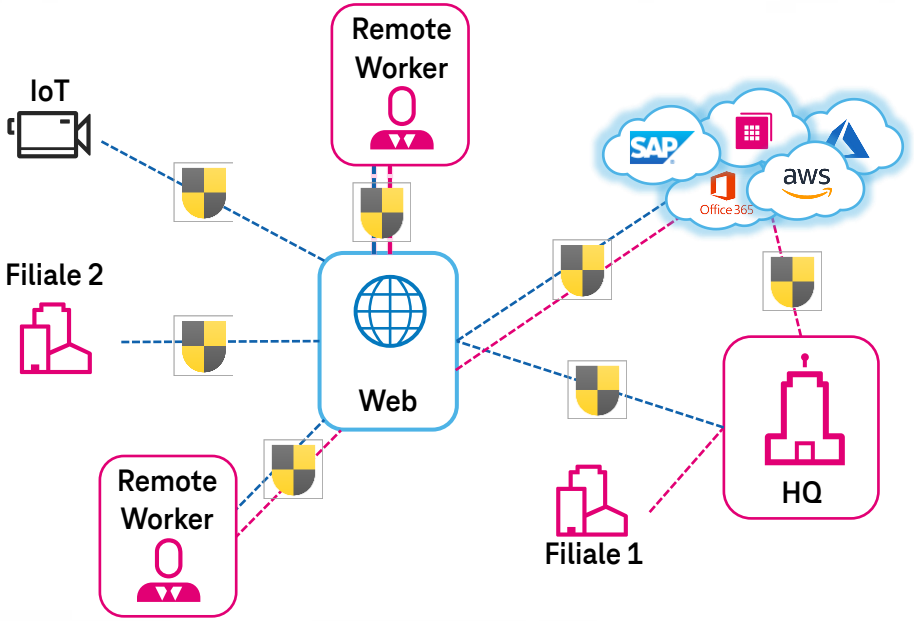
Warum SASE? Denn die Netze haben sich grundlegend verändert!

Von zentralisierten..



- Zentralisierte private Topologie
- Ein einziger Punkt zum Schutz vor Bedrohungen von außen

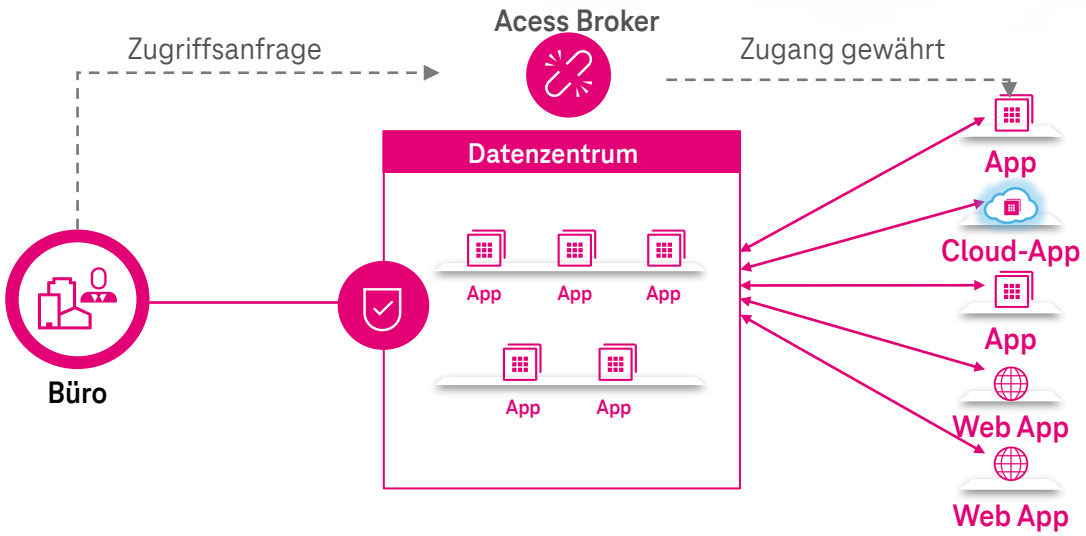
...zur dezentralen Infrastruktur



- Dezentrale Netzwerke mit einem Anteil von bis zu 80 % Internetverkehr
- Fernarbeitskräfte verlangen besten Zugang und erfordern angemessene Sicherheit
- Bürostandorte werden weniger wichtig - Konnektivität von überall

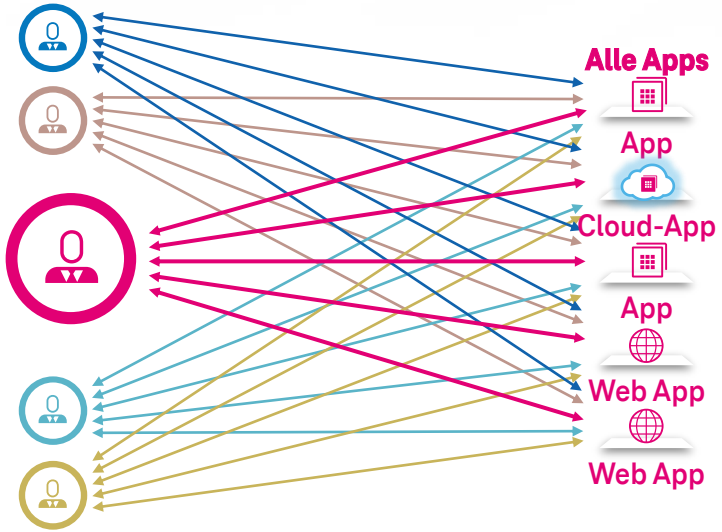
Sicherheit war einfach als die Arbeit noch ein Platz war an den man hinging

Security wird zentral vom Bürostandort aus gesteuert



- App-Verkehr wird nicht geprüft
- Malware oder ‚lateral movement' werden nicht verhindert
- Keine Sicherheitsüberprüfungen und Schutz von Daten
- Nicht alle Anwendungen können gesichert werden
- Sobald der Zugang gewährt wurde, gibt es keine weitere Validierung

Die Angriffsfläche ist gewachsen



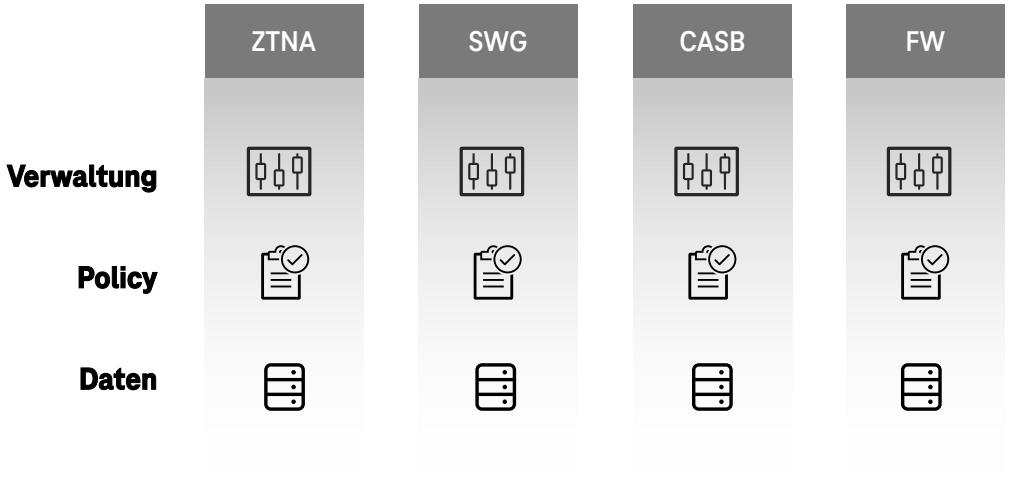
Eine neue Bedrohung, ein neues Security Tool

76

Die durchschnittliche Anzahl von Security Tools in einer Organisation. (+19% in den letzten zwei Jahren, von 64 auf 76)

(PANASEER, 2022)

Fragmentierte Sicherheitslösungen erzielen inkonsistente Ergebnisse

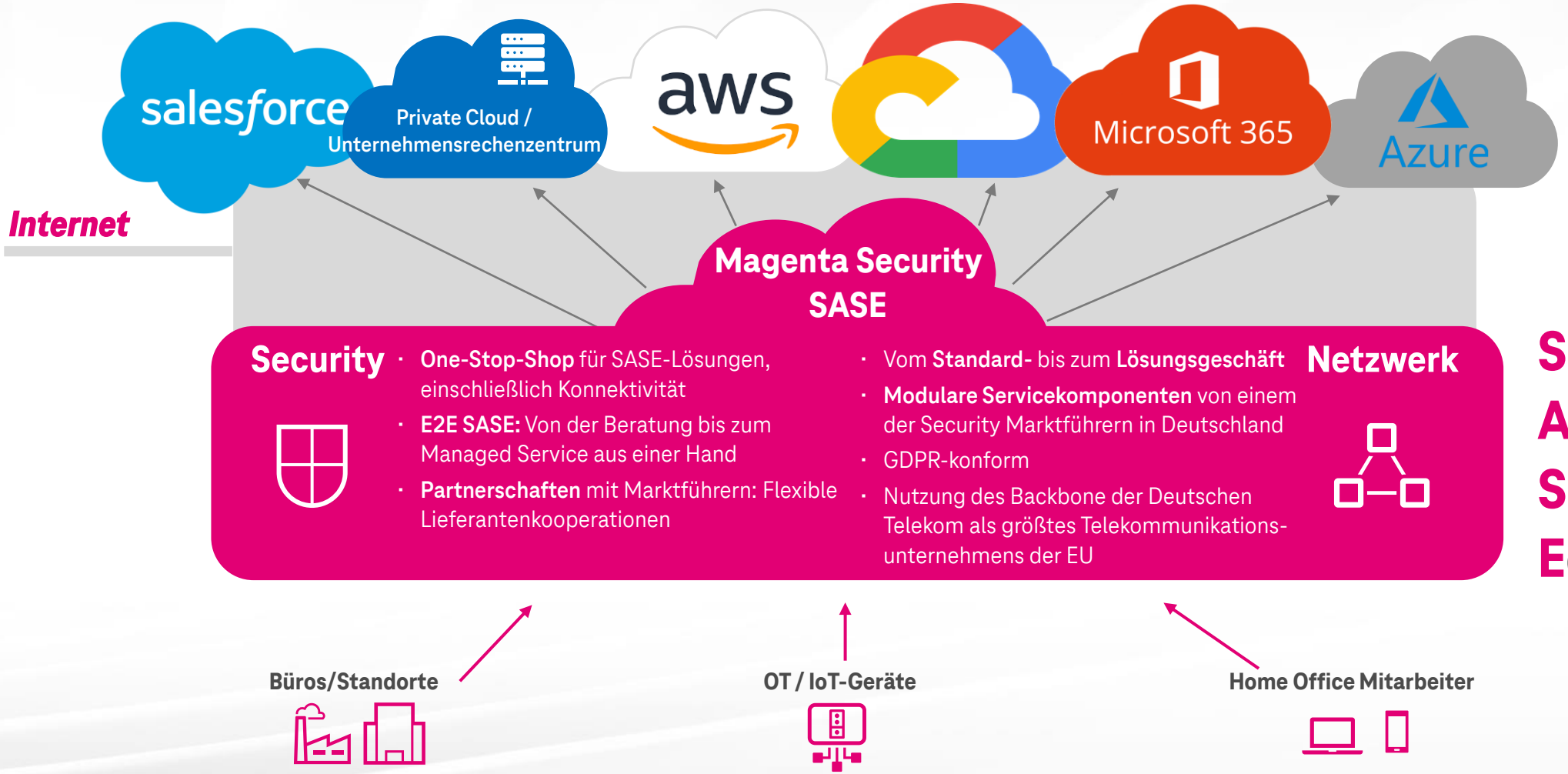


Einzellösungen mit **nicht abgestimmter** Verwaltung, **fragmentierten** Richtlinien und **verstreuten** Daten.

Einheitliche und zentrale Orchestrierung von ZTNA, SWG, CASB, FW, ..

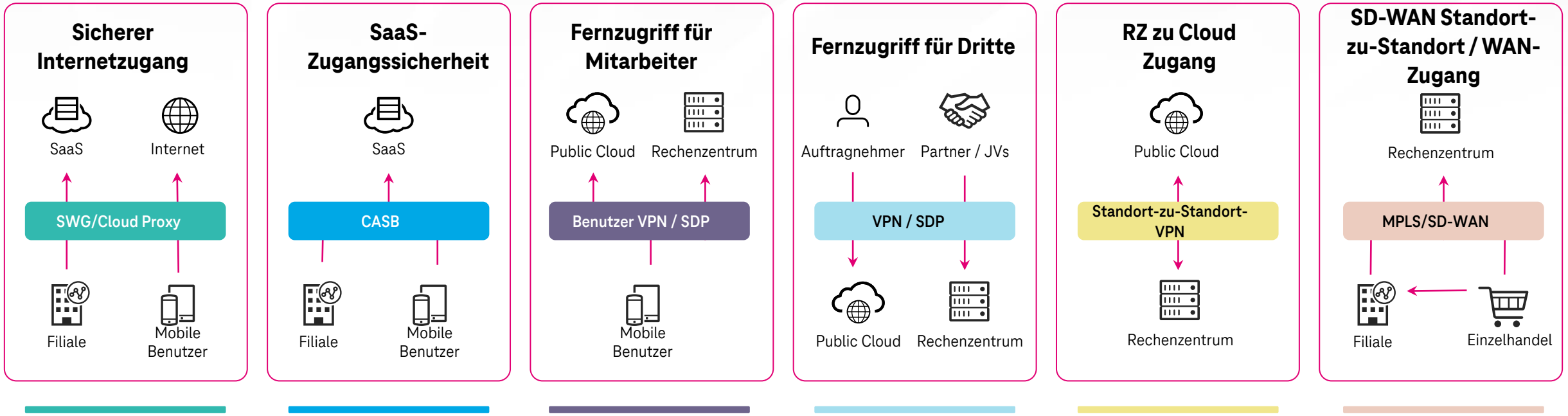
Magenta Security SASE?

Magenta Security ASE: Bündelung von Security und Konnektivität



Secure Access Service Edge

Sechs verschiedene Anwendungsfälle - alle durch eine SASE-Architektur abgedeckt



Mehrere Endpunkt-Clients | Mehrere Policies | Mehrere Verwaltungsschnittstellen | Nicht einheitliche Security Kontrollen

Komplexität, inkonsistente Sicherheit, Kosten für überschneidende Lösungen

▼

Möglichkeiten zur Vereinfachung mit einer einzigen, ~~in der~~ Cloud ~~bereitgestellten~~ Plattform

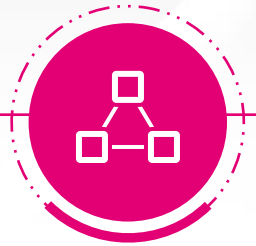
SASE Kernfunktionen

SD-WAN

- Software-defined Wide Area Networks (SD-WAN) ermöglicht ein **zentral orchestriertes Management** der kompletten **WAN Komponenten**
- Kombination von verschiedenen Zugangsarten mit **‚active path selection'** und Optimierung
- Intelligentes Routing
- Sichert das **Overlay durch Verschlüsselung**

NG-Firewall (as a Service)

- FWaaS steuert den **Datenverkehr** auf Netzwerkbasis
- Kombiniert traditionelle portbasierte Policies mit **erweiterten Funktionen**
- Kann vor Ort in einem **kombinierten Service** (One-Box-Design) mit dem SD-WAN-Endpunkt eingesetzt oder in der Cloud bereitgestellt werden



Zero Trust Netzwerkzugang

- Zero-Trust-Netzwerkzugang ändert das **Paradigma der Zugriffspolitik** in Richtung Nutzer, Geräte, Kontext und Dienstleistungsverbrauch
- ZTNA-Policies integrieren **Benutzeridentitäten** mit **dedizierten Informationen** über verwendete Geräte, telemetrische Daten und MFA, um Zugriffe auf SaaS-Applikationen oder andere Datenquellen zu gewähren

Sicheres Web-Gateway (SWG)

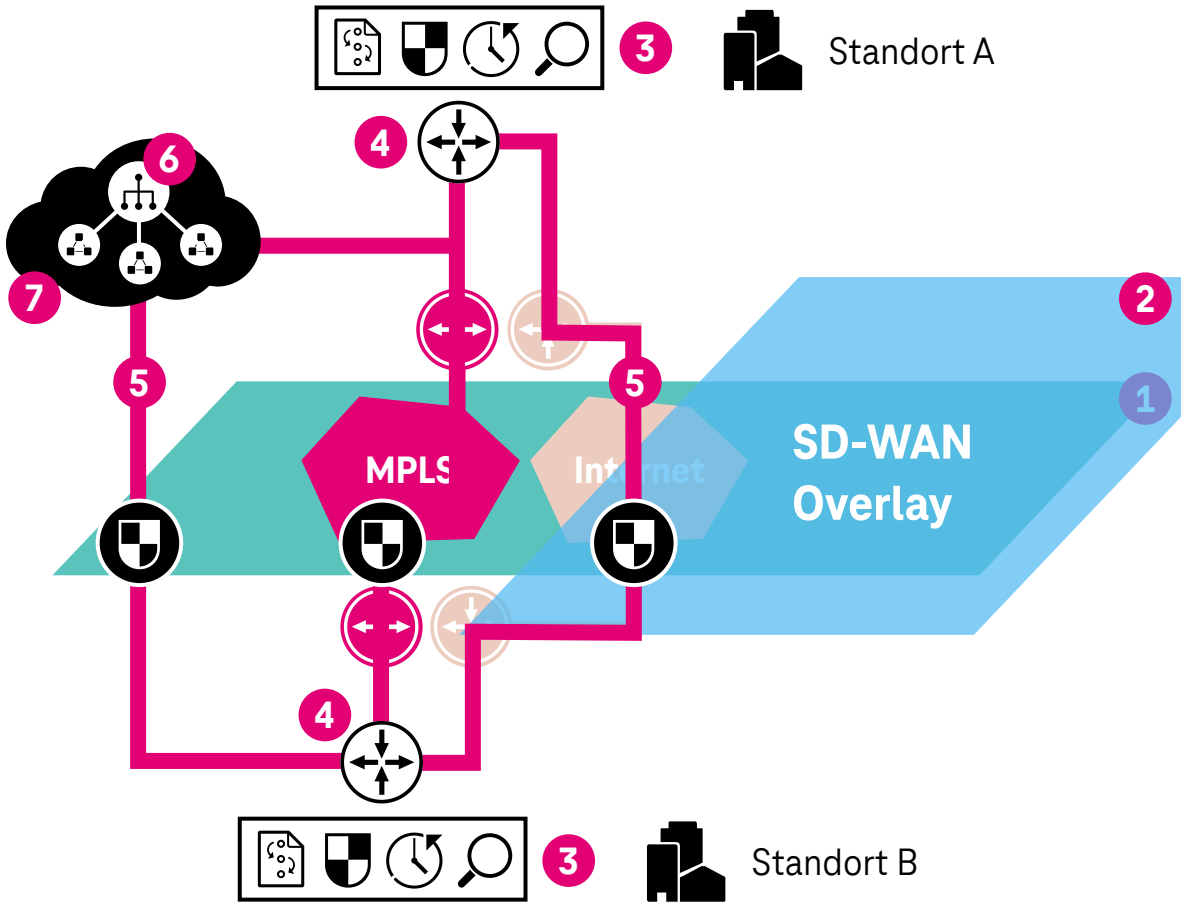
- SWG **schützt die Internetnutzung** durch URL-Filterung, Malware-Schutz und kann den Zugang zu Internetdiensten auf der Grundlage von Unternehmensrichtlinien sperren oder freigeben.
- Gleiche Sicherheitsstufe für **Remote Worker** und **Standorte**

Cloud Access Security Broker

- CASB schützt die **Nutzung von Cloud-Diensten**
- Es besitzt Wissen über **alle verfügbaren Anwendungen** (SaaS, firmeneigene Anwendungen) und **schützt vor Datenverlusten** oder nicht erlaubten Datenflüssen in verbotene oder eingeschränkte SaaS-Anwendungen
- Erkennung von "**Schatten-IT-Umgebungen** "

Einheitliche Verwaltung in der Cloud

So funktioniert SD-WAN

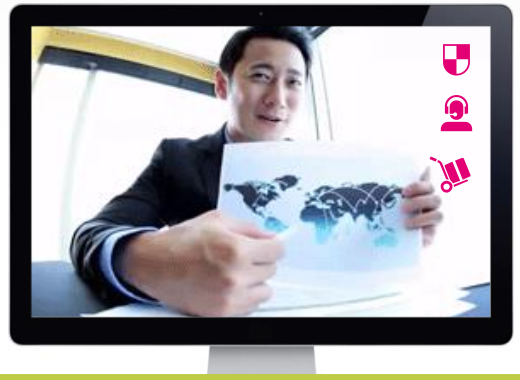


1. SD-WAN nutzt MPLS, Internet, Mobile als Transportnetz (Underlay)
2. Über die Transportnetze wird ein SD-WAN-Netz gelegt
3. Lokale Software (virtualisierte Netzwerk-Services) sorgt für Routing, Security, Monitoring, Acceleration, etc.
4. Die Software läuft auf SD-WAN-Routern, die proprietär oder eine X86- bzw. Cloud-Edge-Architektur haben
5. Die Routing-Funktion zieht verschlüsselte Tunnel zwischen den SD-WAN-Standorten
6. Die zentralen Controller Services steuern Tunnel, updaten Router, überwachen Applikationen u.v.m.
7. Die zentralen Controller Services können in einer Public oder Private Cloud betrieben werden

SD-WAN unterstützt um die Anforderungen der zukünftigen Netzwerke zu erfüllen

- Ermöglichen von Multi-Cloud-Umgebungen
- Sicherstellung der App Performance
- Mehr Mbit pro Euro
- Verbinden und sichern Sie Standorte und Mitarbeiter
- Mehr Agilität durch Verringerung des Aufwands für das IT-Team
- Durchsetzung von Sicherheitsrichtlinien

Schlecht: Unpassender Provider (2% Paketverlust) ✕



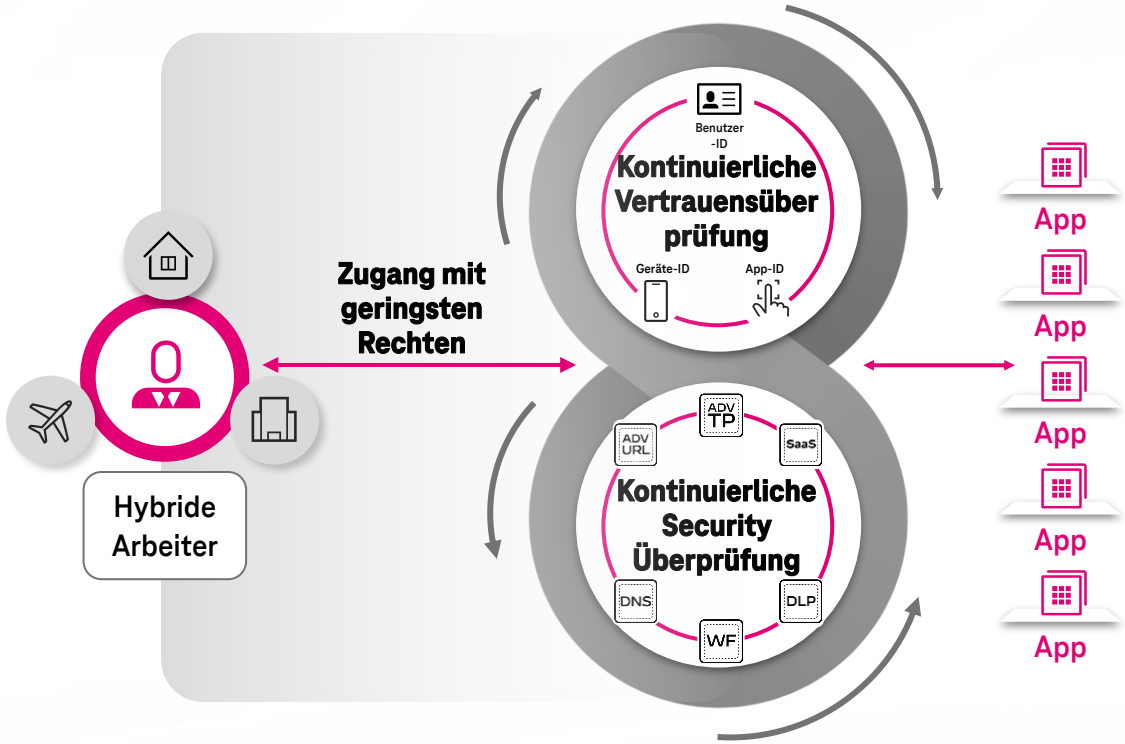
+ Besser: Unpassender Anbieter + SD-WAN

✓ Am Besten: Konnektivität + SD-WAN von der Telekom

Security war einfach, als die Arbeit noch ein Ort war, an den man hinging

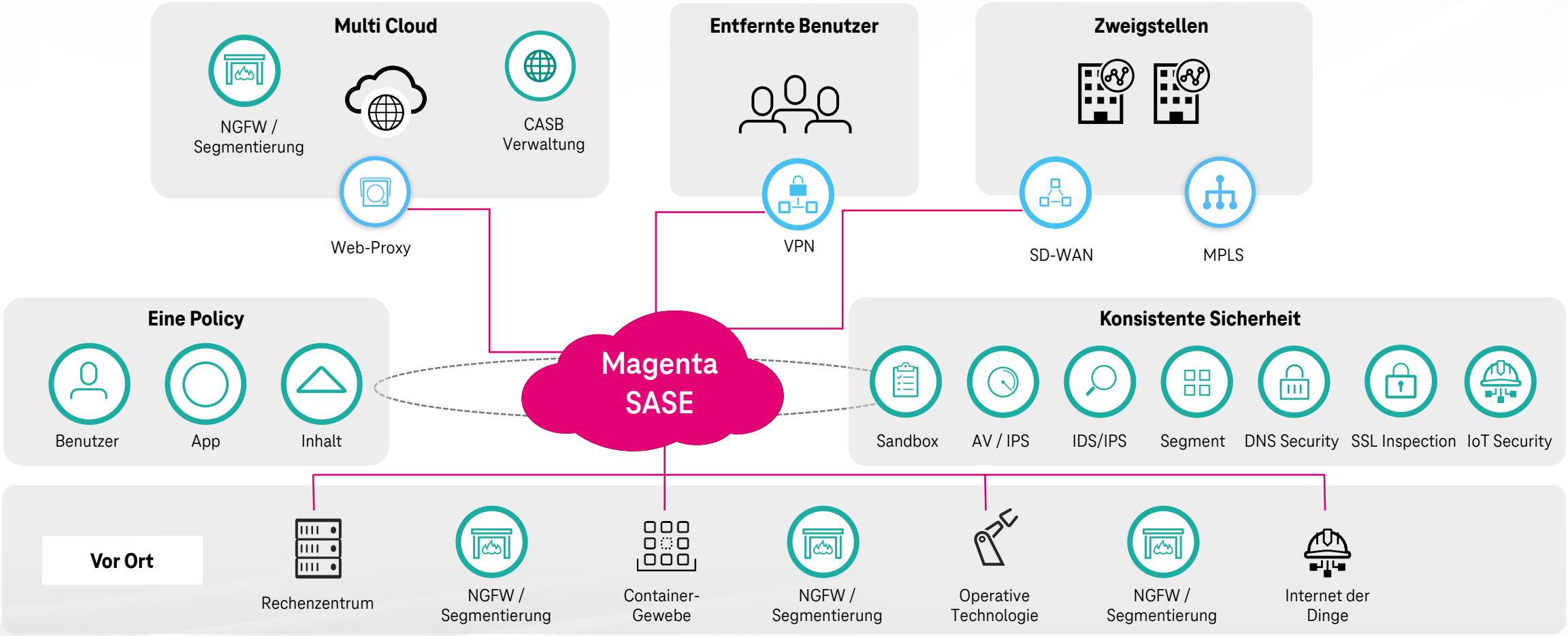
Eine Reise durch ZTNA

- Vollständige Umsetzung des **‚least privilege‘** Prinzips auf Basis von **Layer 7**
- Das Vertrauen wird **kontinuierlich** auf der Grundlage von den Geräten sowie des Benutzer- und des Anwendungsverhaltens **bewertet**
- Detaillierte und kontinuierliche **Überprüfung** des gesamten Datenverkehrs
- Ermöglicht eine tiefe und permanente Überprüfung des gesamten Datenverkehrs, selbst bei erlaubten Verbindungen, um alle Bedrohungen, einschließlich Zero-Day-Threats, zu verhindern.



Blueprint-Architektur

Erzielen Sie Agilität und Kosteneffizienz durch eine einzige Policy-Enforcement



Telekom Security & unser Ansatz

Magenta Security SASE – SSE von Telekom Security

Cloud-zentriert: Weniger Security Komponenten im Unternehmensnetzwerk

01

Weniger Verwaltungsaufwand durch Self-Service, Co-Management und integrierte Funktionen

02

Standortunabhängige, konsistente und **zentralisierte** Durchsetzung der **Sicherheitsregeln**

03

Reduzierung von Kosten und Komplexität durch Konsolidierung von Insellösungen

04

Transparentere **Netzwerkqualität** durch Implementierung von SD-WAN

05

Zero Trust Network Access zum Schutz vor unbekannten Bedrohungen

06

Performante und sichere **Verbindungen** inkl. Monitoring **von überall**

07

Kunden-vorteile

Magenta Security SASE – SSE À la carte
Lizenzen, Professional Services and Managed Services

SSE Transformationsansatz*

Definieren & Entwerfen

- Workshop vor der Einführung
  - Aktuelle Situation
  - Anforderungen definieren
- Use Cases & Testkriterien
- Dokumentation

Design & Blueprint

Start

Konfiguration, Integration und Test

- Unterstützung bei Client-Installation und Rollout
- Verbindungen konfigurieren
- Cloud-Konfiguration
- Application & Policy Design
- Qualitätssicherung
- Benutzer-Authentifizierung

Überprüfung & Vorbereitung

1-2 Monate

Rollout & Migration Ende

- **Phase 1**
  - Begrenzter Nutzerkreis
  - Bewertung der Rückmeldungen
- **Phase 2**
  - Erweiterte Einführung (größere Anzahl von Benutzern und verschiedene Abteilungen)
  - Anpassung des Blueprints
- **Phase 3**
  - Rollout fortsetzen
  - Regelmäßiger Statusupadte und Bewertung
  - Abschließende Bewertung und

Adaptierung & Rollout

3-4 Monate

5-6 Monate

Magenta Security SASE Beratungspakete

1. SSE Starter Paket

Vermittlung des SASE-Framework und Entwicklung einer eigenen SASE-Vision

Im Lieferumfang des Starterpakets enthalten:

SASE-Framework
- Start & Vorbereitung
- SASE-Strategie-Workshop

SASE Vision
- Bewertung der derzeitigen Infrastruktur
- Entwurf der Zielarchitektur

Zusammenfassung und weitere Vorgehensweise
- Empfehlungen zur Transformation
- Individuelle SASE-Vorteile ausarbeiten

Optional:
- Detaillierte SASE Strategie | PoC

- Ihre Vorteile aus dem SASE Framework
- SASE-Strategie für Ihren individuellen Bedarf

2. SSE Transition Paket

Planen Sie Ihre individuelle SASE-Reise

Im Übergangspaket inbegriffen:

SASE-Transitionstrategie
- Überblick über das Übergangsprojekt
- Identifizierung von Anforderungen und Zielen
- Planung der SASE-Übergangsreise

Entwurf des Transitionprojekts
- Auswahl von geeigneten SASE/SSE-Anbietern
- SASE-Fahrplan

Optional
- PoC

- Geringere Komplexität: Wir kümmern uns um Ihre SASE-Roadmap, einschließlich Architekturplanung und Produktauswahl

3. SD WAN Beratung

Vermittlung der SD-WAN-Anforderungen und Gestalten einer individuelle SD-WAN-Strategie

Bei SD-WAN gibt es keine „Einheitsgröße"

Kundenanforderungen
- Funktionalitäten
- Standorte der Kunden
- Zeitplan und Budget
- Sicherheitsstufe
- Applikationen
- Dienstleistungskonzept
- …

Lösungsdesigner
- Verfügbarkeit
- Standorte
- Kostenelemente
- Beschränkungen
- Abhängigkeiten
- Vorlaufzeit
- …

SD-WAN-Auswahl

Underlay Design

Sicherheitsoptionen

Vielen Dank!