Cloud-Access-Infrastruktur mit SASE und SD-WAN

1&1 Versatel

September 2022

Agenda

Cloud-Access-Infrastruktur mit SASE und SD-WAN

1. Cloud-Access-Infrastruktur
2. Secure Cloud Access mit SD-WAN
3. Zero Trust Access
4. Integration von Home-Office und mobilen Nutzern

Die Zahl(en) des Monats

30

Schätzung von IT-Mitarbeitern der durchschnittlich im Unternehmen genutzten Cloud-Dienste[1)]

1) Quelle: McAfee – Cloud Adoption and Risk Report 2019

Die Zahl(en) des Monats

30

Schätzung von IT-Mitarbeitern der durchschnittlich im Unternehmen genutzten Cloud-Dienste[1)]

1.935

Der tatsächliche Durchschnitt

1) Quelle: McAfee – Cloud Adoption and Risk Report 2019

Cloud ist nicht gleich Cloud – eine Unterscheidung ist erforderlich

Überblick Cloud Nutzung

On-Prem	IaaS	PaaS	SaaS
Eigenes DC	Infrastructure as a Service	Platform as a Service	Software as a Service
• Vollständige Kontrolle über alle Bereiche • Firmenkritische Applikationen • Sonderlösungen	• Sehr hohe Flexibilität • Automatisierung • Kostenkontrolle • Skalierbarkeit	• Flexible Anpassung an die Bedürfnisse • Schnelle Entwicklung und Bereitstellung neuer Applikationen	• Funktionsfähiger Service • Einfacher Zugriff • Geringere Kosten • Einfache Skalierbarkeit

Cloud ist nicht gleich Cloud – eine Unterscheidung ist erforderlich

Überblick Cloud Nutzung

On-Prem

Eigenes DC

- Vollständige Kontrolle über alle Bereiche
- Firmenkritische Applikationen
- Sonderlösungen

IaaS

Infrastructure as a Service

PaaS

Platform as a Service

- Flexible Anpassung an die Bedürfnisse
- Schnelle Entwicklung und Bereitstellung neuer Applikationen

SaaS

Software as a Service

- Funktionsfähiger Service
- Einfacher Zugriff
- Geringere Kosten
- Einfache Skalierbarkeit

Cloud ist nicht gleich Cloud – eine Unterscheidung ist erforderlich

Überblick Cloud Nutzung

On-Prem

Eigenes DC

- Vollständige Kontrolle über alle Bereiche
- Firmenkritische Applikationen
- Sonderlösungen

IaaS

Infrastructure as a Service

PaaS

Platform as a Service

SaaS

Software as a Service

- Funktionsfähiger Service
- Einfacher Zugriff
- Geringere Kosten
- Einfache Skalierbarkeit

1&1 versatel

Cloud ist nicht gleich Cloud – eine Unterscheidung ist erforderlich

Überblick Cloud Nutzung

On-Prem

Eigenes DC

- Vollständige Kontrolle über alle Bereiche
- Firmenkritische Applikationen
- Sonderlösungen

IaaS

Infrastructure as a Service

PaaS

Platform as a Service

SaaS

Software as a Service

1&1 versatel

Nutzung vorhandener Netzwerk-Infrastrukturen für Cloud-Access

Cloud-Access über zentralen Internet Breakout

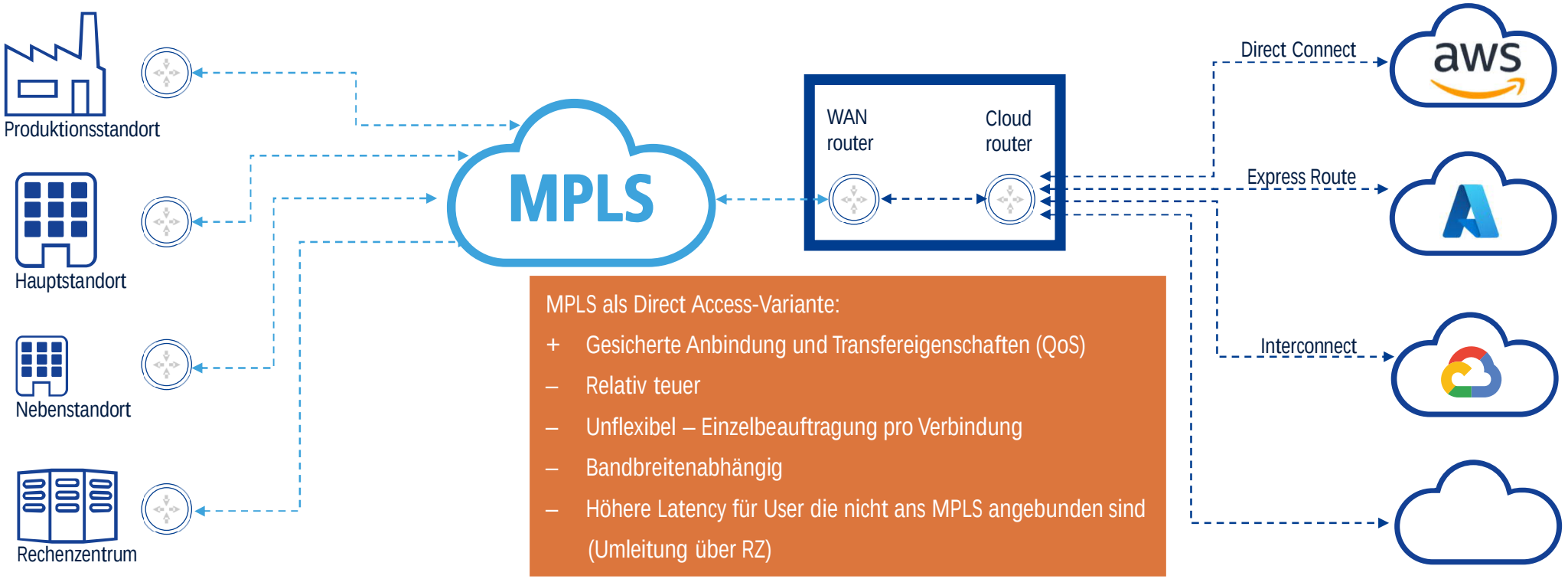
Cloud-Access via Internet:

+ Zentrale Break-Outs über RZ, GWs oder HQ
+ Klassische Perimeter Security an zentralen Standorten
+ Einfache Erreichbarkeit der Cloud Provider
– Möglicher Flaschenhals an den zentralen Standorten
– Security erforderlich

1&1 versatel

Erweiterung des MPLS in die Cloud

Direkte Verbindungen via MPLS



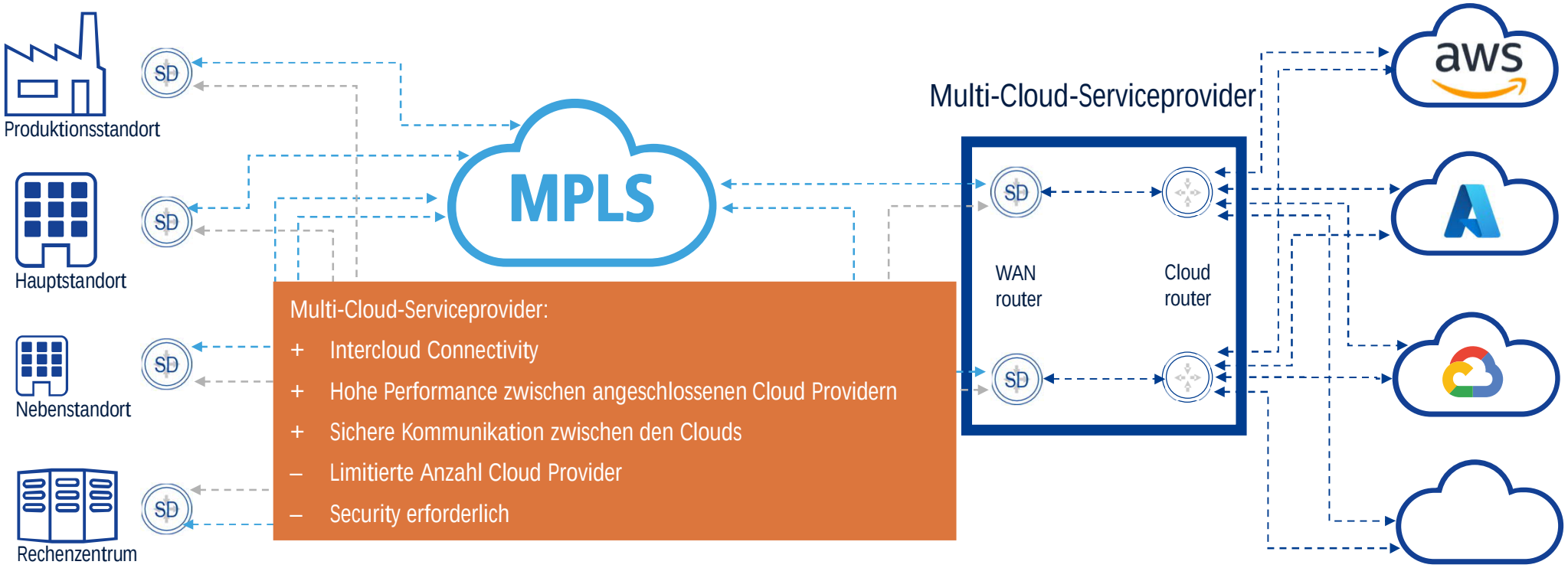
MPLS als Direct Access-Variante:

+ Gesicherte Anbindung und Transfereigenschaften (QoS)
– Relativ teuer
– Unflexibel – Einzelbeauftragung pro Verbindung
– Bandbreitenabhängig
– Höhere Latency für User die nicht ans MPLS angebunden sind (Umleitung über RZ)

1&1 versatel

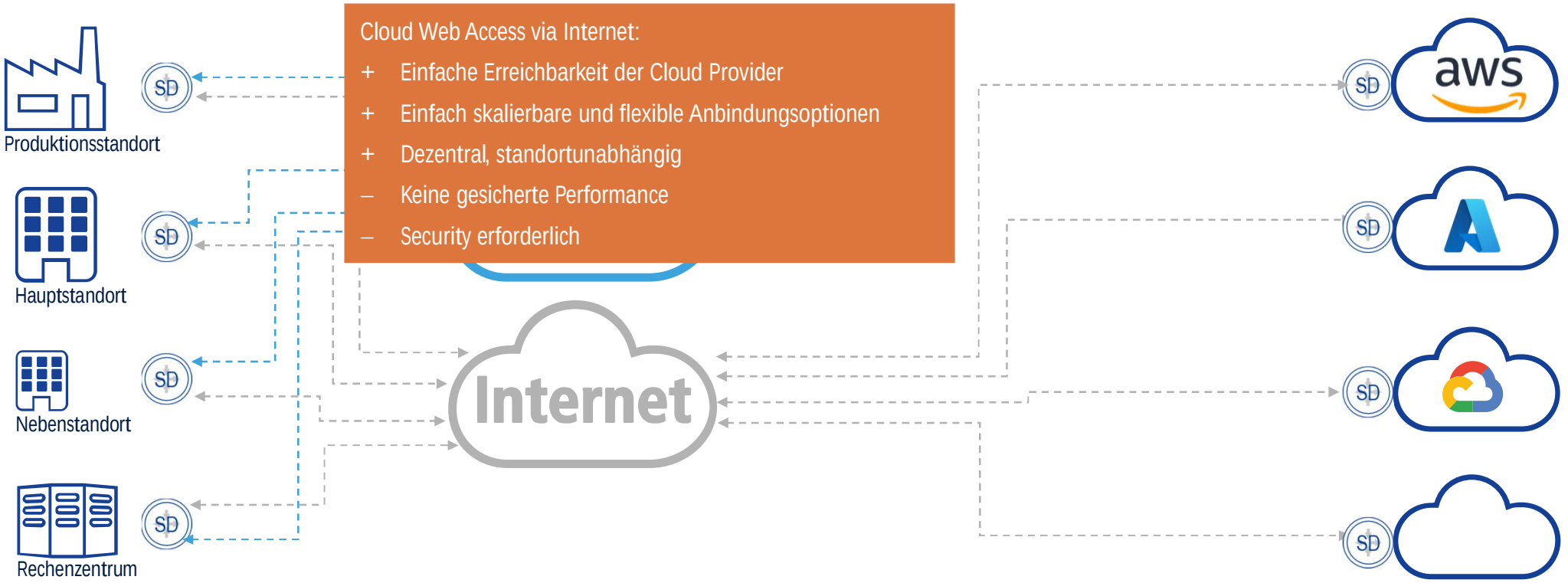
Cloud-Access-Serviceprovider

Multi-Cloud-Service Access



Direkter Internet Access (DIA)

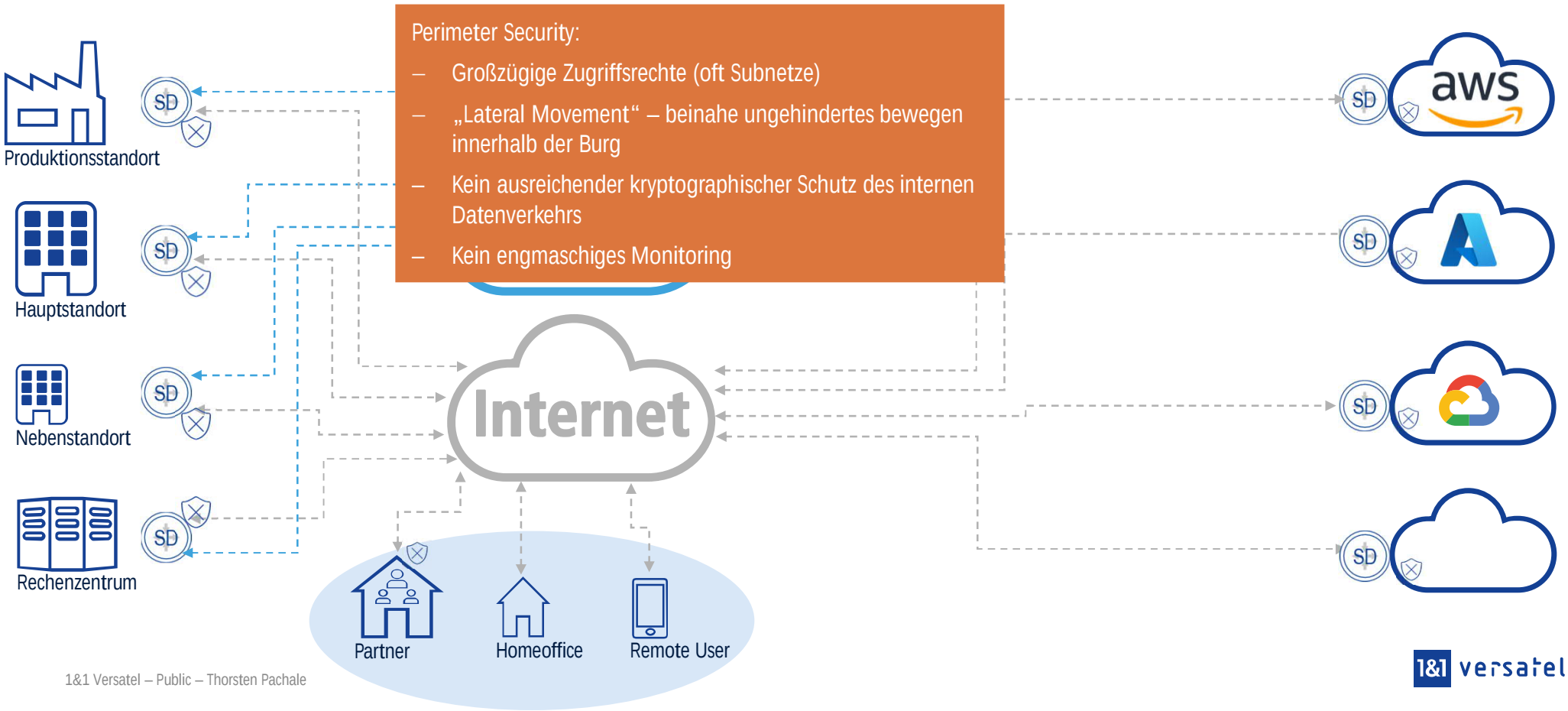
Hybride VPN-Infrastrukturen mit Underlay und Overlay Management



1&1 versatel

Hier fehlt noch etwas

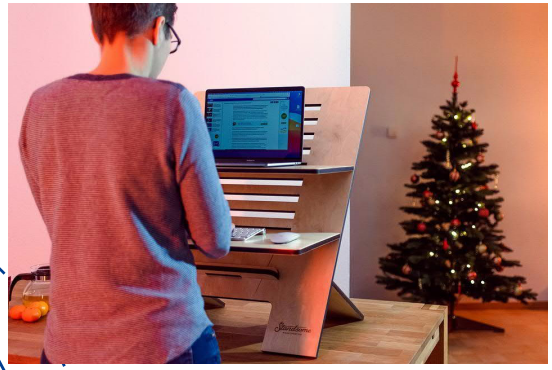
VPN Infrastruktur mit Perimeter Security



Was sind die neuen Realitäten?

Dezentralisierung erhöht Angriffsfläche durch Vervielfachung der Perimeter in unkontrollierten Umgebungen

Cloudification



New Work

IT / OT Convergence

Collaboration

Verlagerung Perimeter

SASE Kompakt

Secure Access Service Edge wie der Markt es sieht

SD-WAN

Software Defined WAN

- Dynamische, durch Software gesteuerte Weitverkehrsnetzwerke
- Basiert oft auf Low-Cost-Access

Security Service Edge (SSE)

Cloud Secure Web Gateway

- Schutz beim Zugriff auf Ressourcen im Netz
- Auch Nutzer außerhalb des Perimeters werden geschützt

Firewall as a Service

- Hybrides Modell aus Firewalls vor Ort und Firewalls in der Cloud

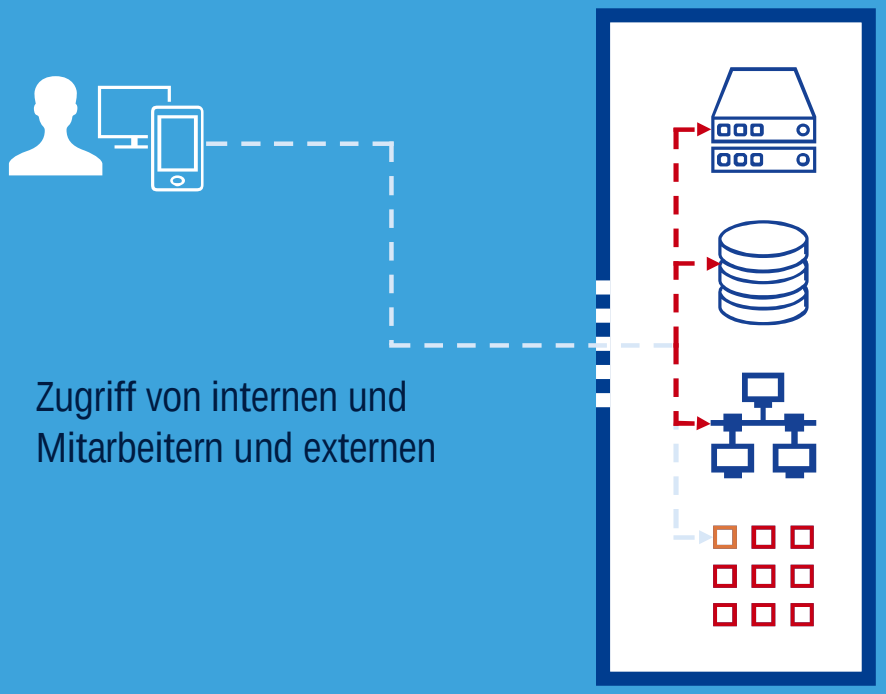
Zero Trust Network Access

- Nachfolger des VPN
- Mapping von Identität zu Applikation

Zero Trust Network Access – ZTNA

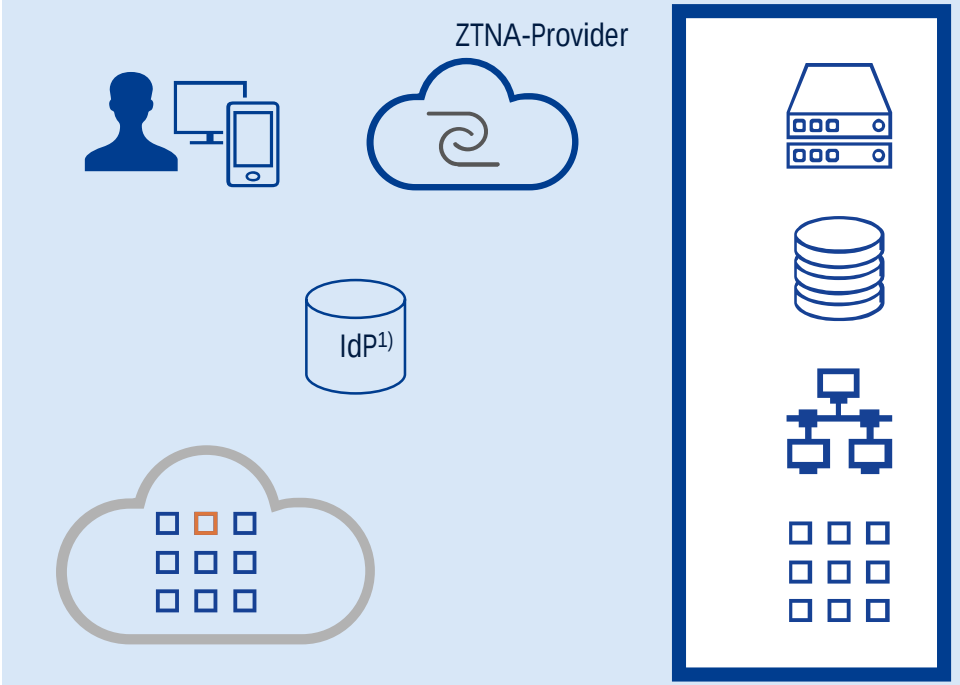
VPN versus ZTNA

Klassisches Anwender-VPN



- Zugriff von internen und Mitarbeitern und externen

Zero Trust Network Access



1) IdP = Identity Provider

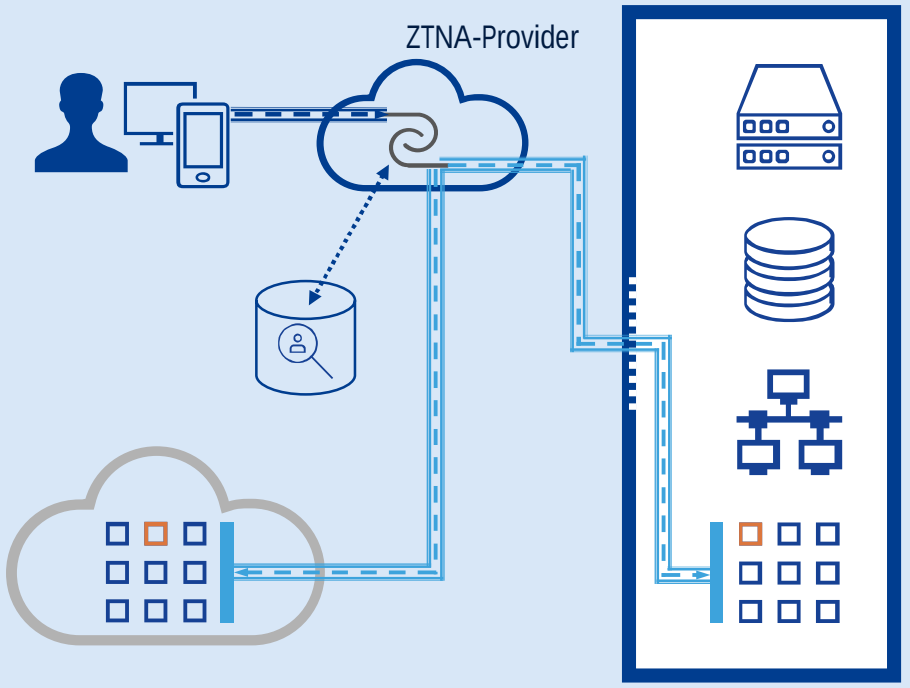
Zero Trust Network Access – ZTNA

Wie es funktioniert

Klassisches Anwender-VPN

1. Ausgehender Tunnel vom Connector zum ZTNA-Provider
2. Ausgehender Tunnel vom Anwender zum ZTNA-Provider
3. Abruf der Berechtigungsinformationen vom Identity Provider
4. Verknüpfung der Tunnel und Aufbau der Verbindung zur Applikation

Zero Trust Network Access



1) IdP = Identity Provider

1&1 versatel

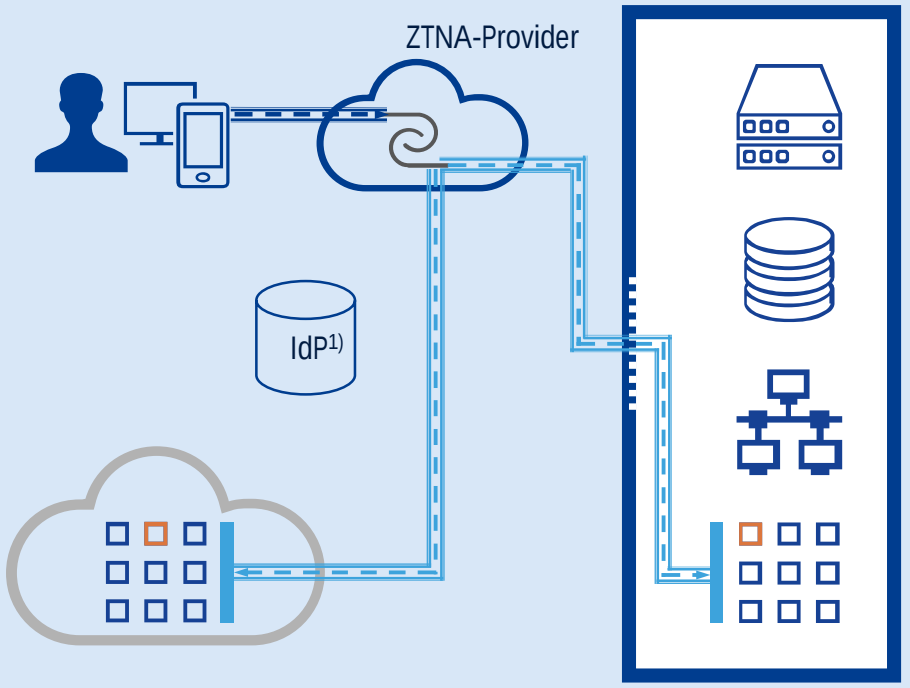
Zero Trust Network Access – ZTNA

Wie es funktioniert

Anwendungsfälle

1. Remote Access / VPN-Ersatz
2. Secure Cloud Access
3. Mergers & Acquisitions
   (Unternehmenszusammenschlüsse und -käufe)
4. Ergänzung eines SD-WAN

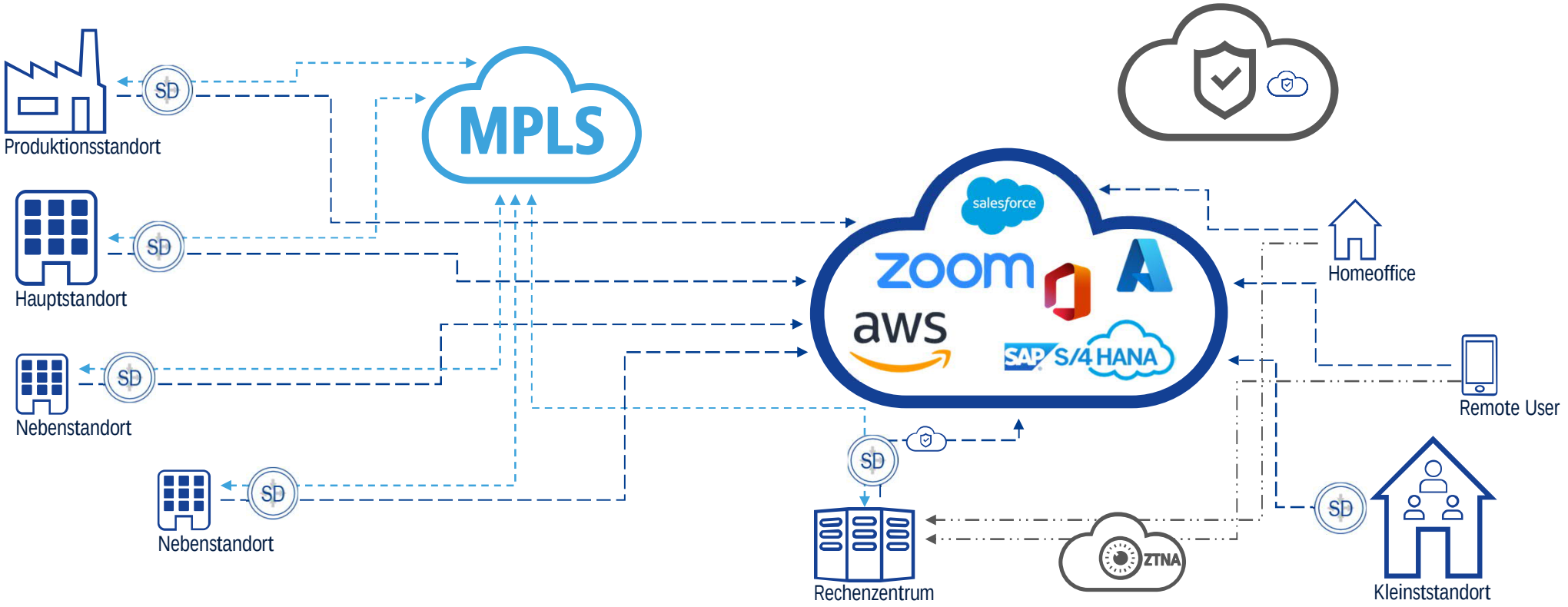
Zero Trust Network Access



1) IdP = Identity Provider

Das Gesamtkonstrukt

SD-WAN und Security Service Edge = SASE



1&1 versatel

Fragen?
Antworten!

1&1 Versatel Deutschland GmbH
Wanheimer Straße 90 | 40468 Düsseldorf | Germany
www.1und1.net