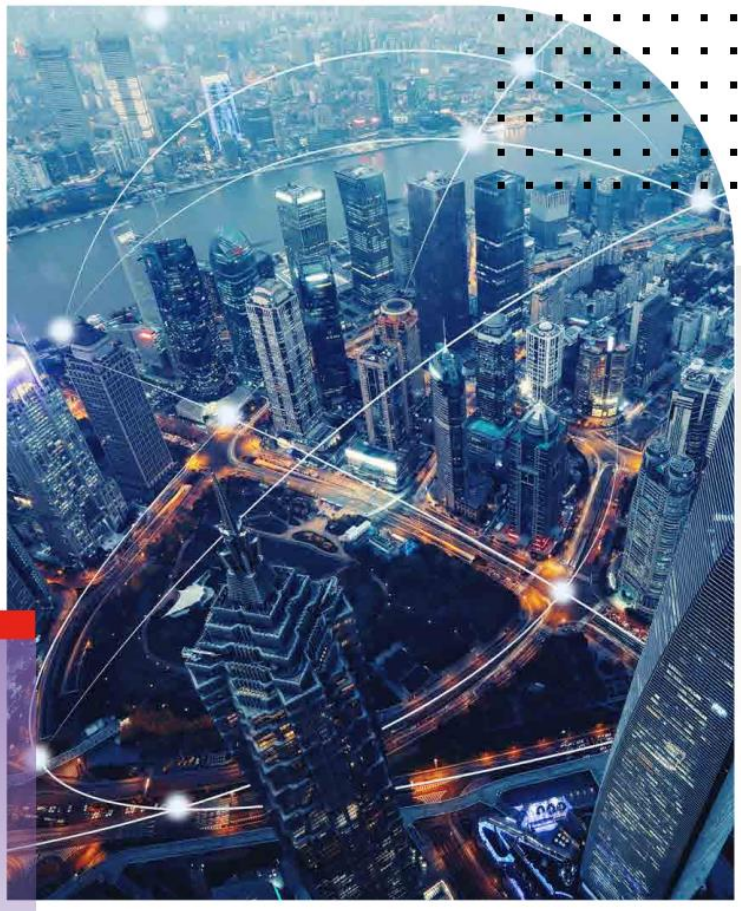
CHANNEL CHEAT SHEET

Fortinet Zero Trust Access

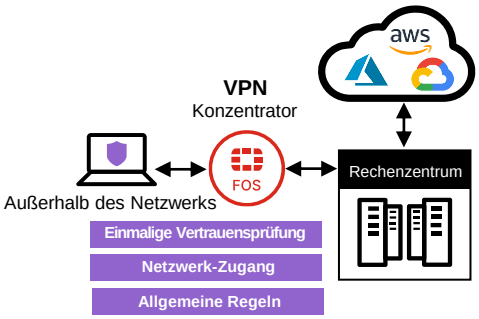


Zero-Trust-Access-Opportunity

Große Opportunity	Wachstumsstarke Opportunity	Einfach zu verkaufen	Neuer Geschäfts-ausbau	Security Fabric neue Chancen
Lösung für VPN und darüber hinaus Markt von 19,6 Mrd. US$	Über 17,4% Wachstum Pandemie beschleunigte Umstellung auf ZTNA	Kostenlos enthalten in FortiGate + FortiClient (EMS)	Authentifizierung (MFA …) FortiAuth. FortiToken	

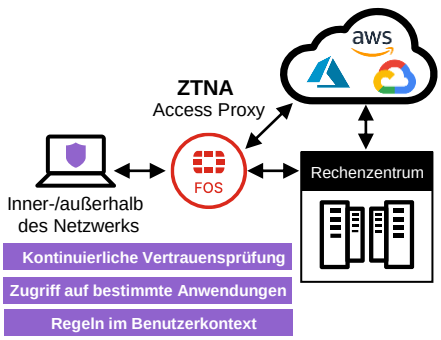
Kundenherausforderungen

- **Schlechte Benutzererfahrung** *wegen Unterschieden und Komplexität inner-/außerhalb des Netzwerks*
- **Höhere Risiken** *durch Angriffe, die Schwachstellen von Heimnetzen und VPNs ausnutzen*
- **Komplexität** *beim Management von Anwendungen, die sich überall befinden (On-Premises, Private Cloud, Public Cloud)*



Vorteile einer Umstellung

- **Bessere Benutzererfahrung**: *transparent, sichere Konnektivität von überall aus*
- **Bessere Security**: *geringere Angriffsfläche und kontinuierliche Überprüfung, Benutzerzugriff nur auf notwendige Anwendungen und Daten, MFA, Authentifizierung pro Sitzung, Kontextregeln, Risikobewertung von Geräten …*
- **Einfacheres Management**: *einfachere Handhabung von Richtlinien für inner- und außerhalb des Netzwerks*



Warum umstellen?

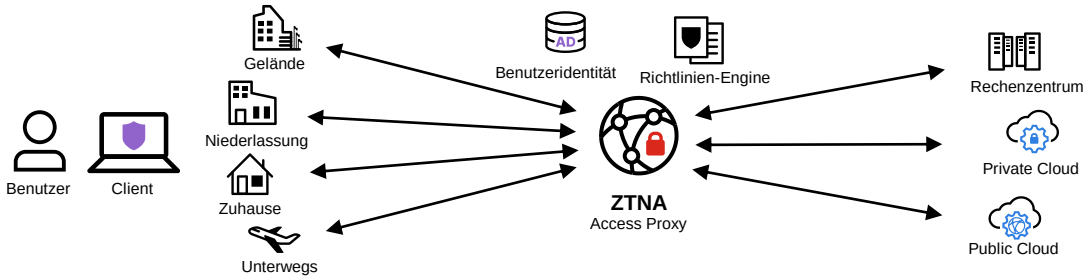
- **Telearbeit**: *massive Einführung von Telearbeit und Homeoffices wegen der Corona-Pandemie*
- **Cloud**-Einführung: *stärkere Dezentralität von Anwendungen (überall verteilt)*
- **Ransomware**-Angriffe: *Anstieg, Einschleusung in lokale Netzwerke über anfällige Remote-Systeme*
- **Finanzielle** Aspekte: *regulatorische u. Compliance-Bußgelder, Rechtskosten bei Sicherheitsvorfällen*

Warum Fortinet?

IT Security Top-Anbieter	Flexibler ZTNA-Ansatz	Geringste TCO auf dem Markt	Weniger Komplexität	Security Fabric-Integration
Gartner: Leader bei Netzwerk-Firewalls	Mehr Flexibilität mit ZTNA für Firewalls *und* SASE	ZTNA + Security mit dem gleichen FortiOS + Client	Integriertes Management ZTNA + Security + MFA + NAC + WAN-Edge …	Ausbaufähig Zukunftssicher Umfassend

ZTNA-Komponenten

Wo die **BENUTZER** sind | **DURCHSETZUNG** von Benutzeridentität u. Geräteprofil | Wo die **ANWENDUNGEN** sind



Geschäftsvorteile mit ZTNA

Bessere Benutzererfahrung

Unterstützung von ortsunabhängigen Arbeiten

- Zugang **im Büro und auswärts**
- Automatisch **sichere** Tunnel zu Anwendungen
- **SSO**-Unterstützung
- **Unabhängig** vom Anwendungsstandort

Geringere Angriffsfläche

Engmaschige Kontrolle über Anwendungen

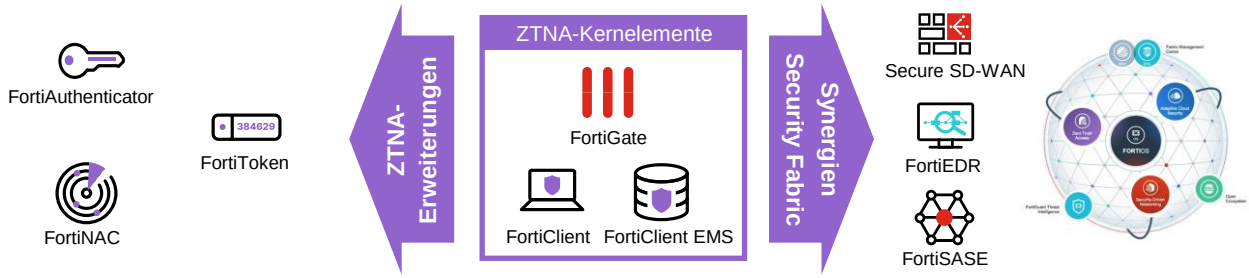
- Authentifizierung der **Benutzer-ID** pro Verbindung
- Starke Authentifizierung (**MFA**, **SSO**)
- Prüfung der **Geräte-Identität** pro Sitzung
- Prüfung des **Geräte-Profils** pro Sitzung
- Zugriff **nur** auf benötigte Anwendungen/Daten
- Anwendungen **im Internet nicht sichtbar**

Einfachere Umstellung auf die Cloud

Zugangskontrolle für Hybrid Clouds

- Bereitstellung von Anwendungen **überall**
- **Zentrales Management** für alles mit On-Premises- und Remote-Durchsetzungspunkten
- **Massenkonfiguration**

Fortinet ZTNA und Security Fabric



ZTNA-Wettbewerbslandschaft

Identitätsmanagement
- Okta, Duo, BeyondCorp …

SASE
- Zscaler, Netskope …
- Palo Alto (Prisma)

Lückenhafte Sicherheit

FORTINET

- ✓ **ZTNA-Komplettlösung**
- ✓ **Integriertes ZTNA-Angebot**
- ✓ **Synergien durch die Security Fabric**

Schlechte Integration

Netzwerk-Security
- CISCO (AnyConnect)
- Palo Alto (Global Protect)
- Checkpoint
- …

Ihre nächsten Schritte

Margen erhöhen:
Spezialisierung

Lernen: Zero Trust Hub im Partner-Portal

Überzeugen:
Battle Cards