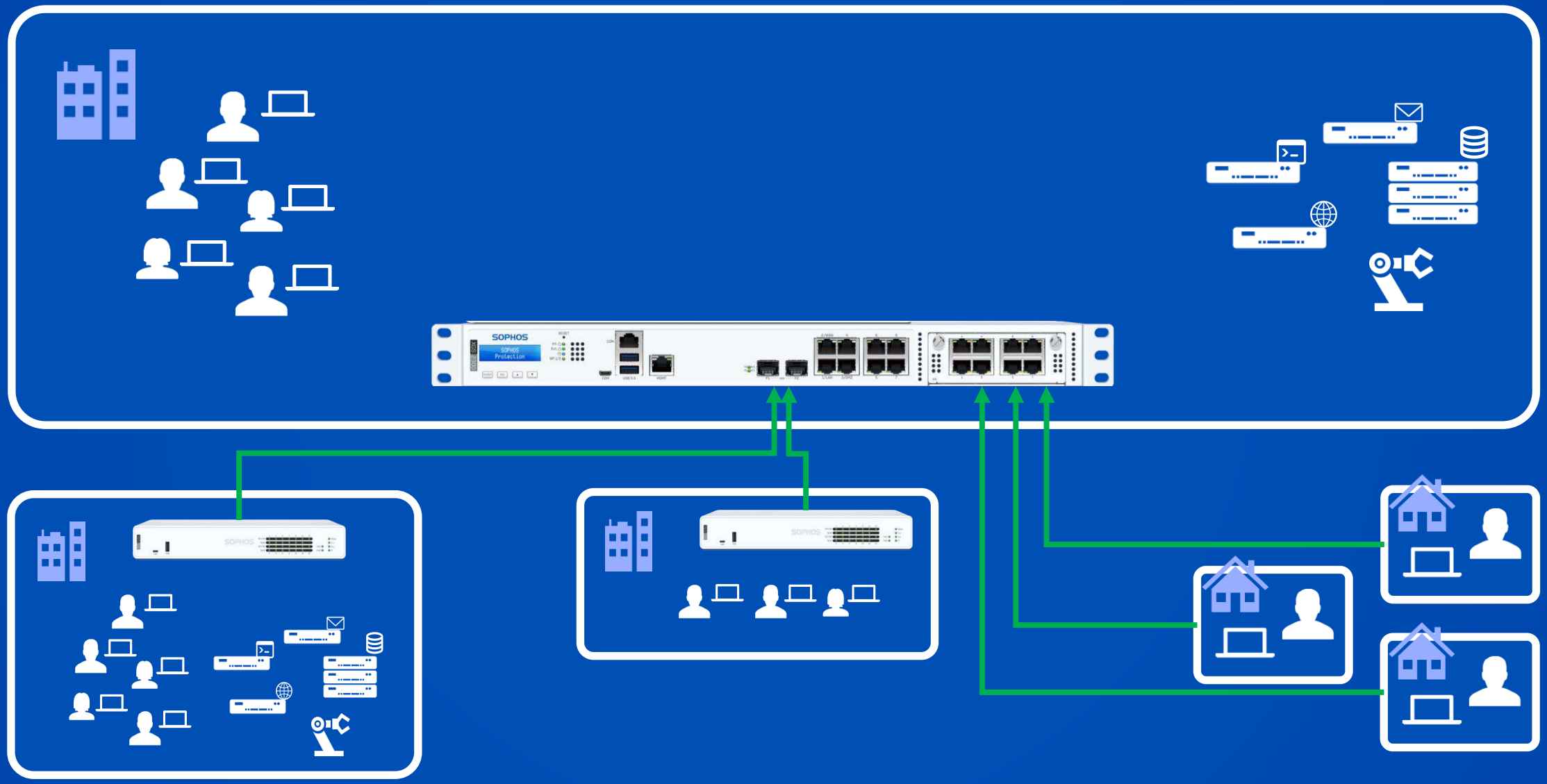
JACOBS
IT Business Next Level

Sicheres Remote Working mit Zero Trust

Stefan Vogt
Sophos Sales Engineer
12.10.2022

SOPHOS

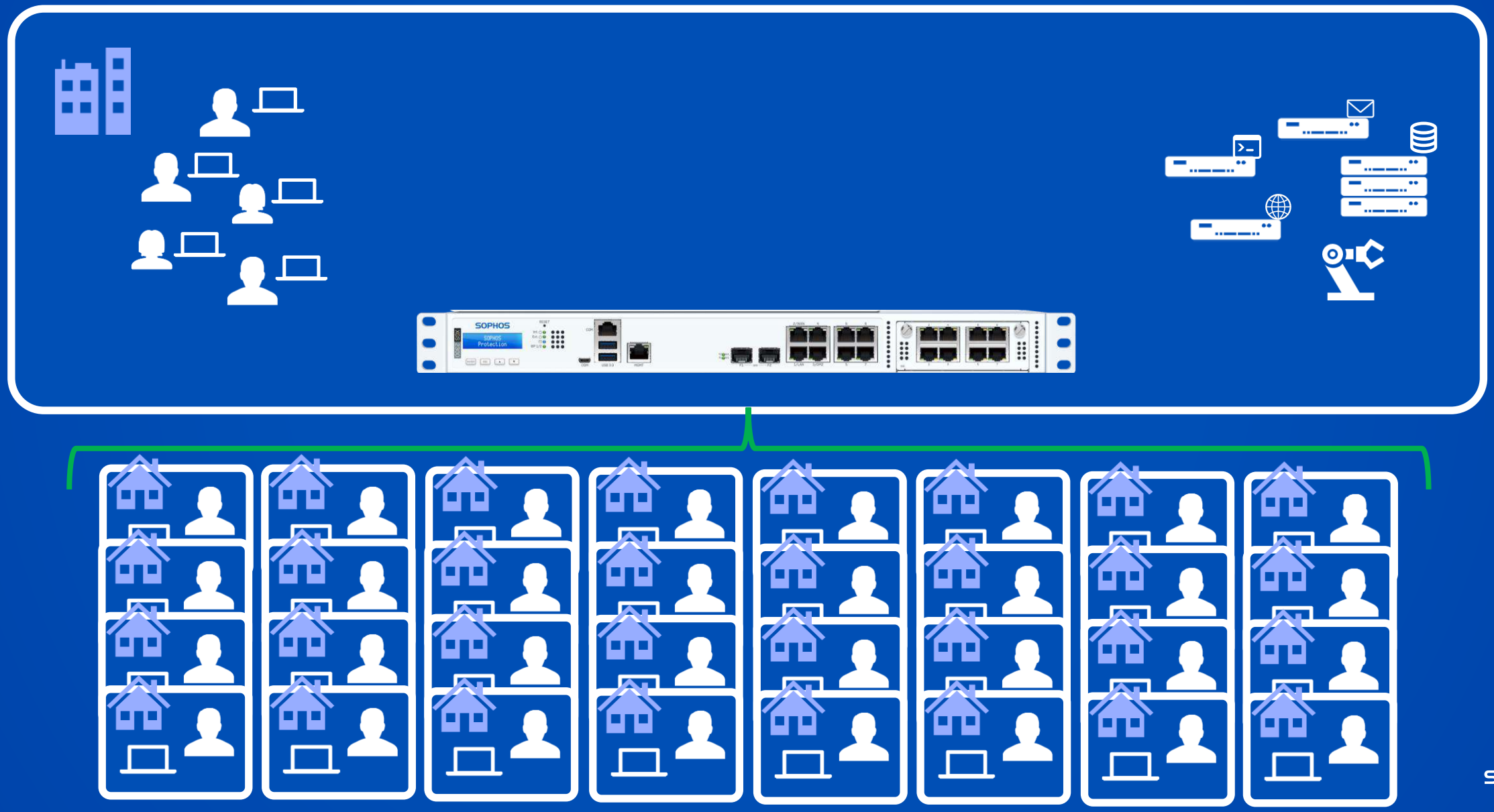
Arbeiten von Zuhause oder Unterwegs via VPN



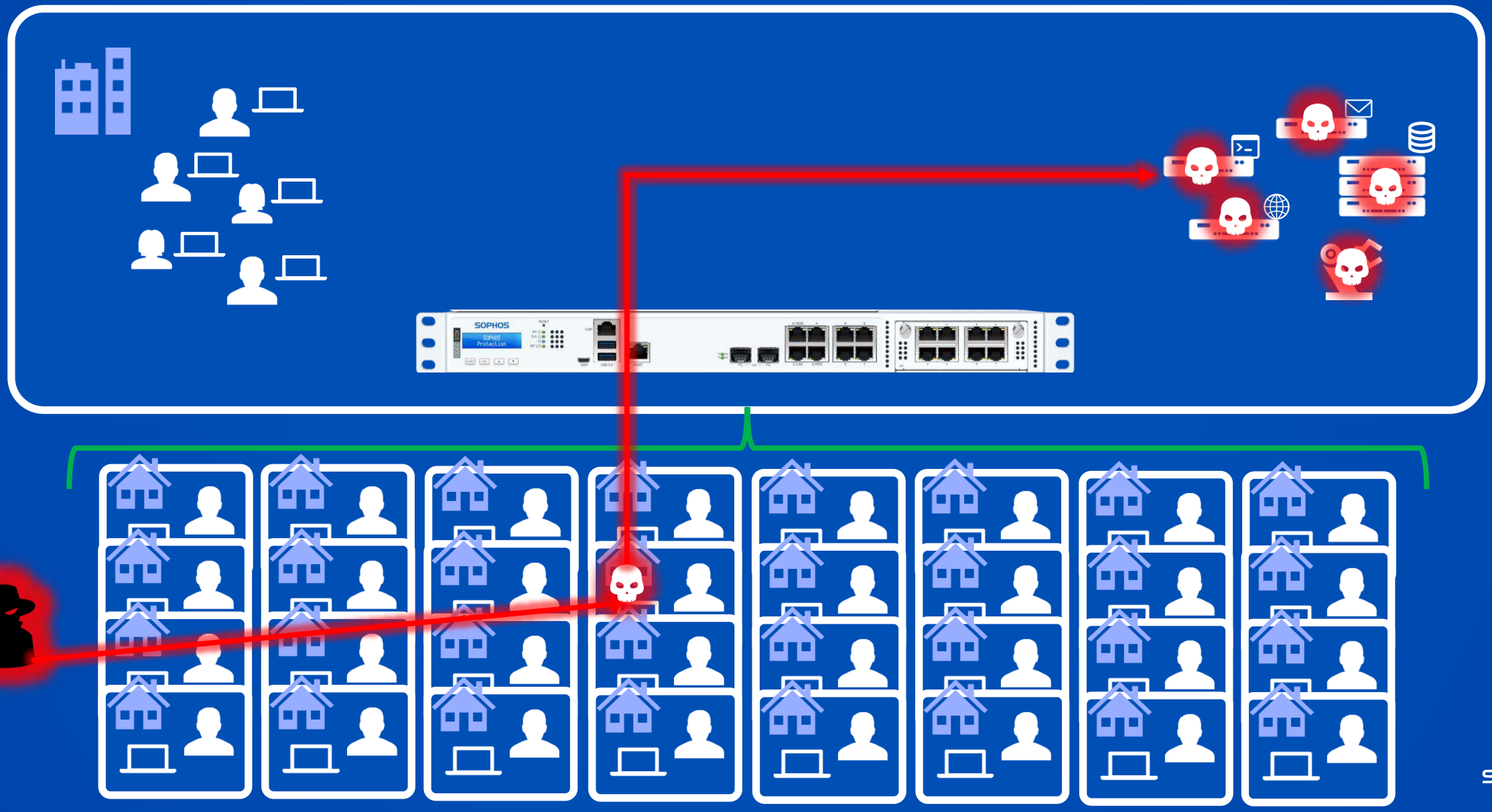
Die Arbeitswelt im Wandel

SOPHOS

Die neue Arbeitsweise



Wie sicher ist VPN eigentlich?



Ransomware Gruppen greifen gezielt VPN an

ZDNet CLOUD STORAGE IOT MOBILE SICHERHEIT NETZWERKE WHITEPAPE

ZDNet / Sicherheit / Cyberkriminalität

Ransomware attackiert VPN und RDP

Ransomware wird immer gefährlicher. Hacker nutzen vor allem das Remote Desktop Protocol (RDP), und Virtual Private Networks (VPN) als Einfallstore. E-Mail-Phishing verliert dagegen an Bedeutung.

von Dr. Jakob Jung am 24. August 2020 .

INFOPOINT SECURITY IT-Security Events Über Uns Kontakt

News > Remote Access VPNs rücken ins Visier von Ransomware-Angriffen

Ransomware

Remote Access VPNs rücken ins Visier von Ransomware-Angriffen

15.01.2020, San Jose | Autor: Herbert Wieler

Sodinokibi-Ransomware nutzt VPN-Verbindung als Schwachstelle für die Attacke auf Travelex

golem.de IT-NEWS FÜR PROFIS HOME TICKER VIDEOS VORGELESEN FORUM

Artikel, News, ... Suchen Golem.de jetzt we

KARRIEREWELT JOBS IT-FACHTRAININGS COACHINGS SPRACHKURSE GEHALTSCHECK | GOLEM-PC PRODUKTVERGLEICH TO

RANSOMWARE

Colonial Pipeline über kompromittiertes Passwort gehackt

Der kürzlich gehackte Pipelinebetreiber Colonial äußert sich zu dem Vorgehen der Ransomware-Gruppe Darkside.

in Pocket speichern merken 7. Juni 2021, 11:24 Uhr, Moritz Tremmel

(Bild: Reuters)

Die Treibstofftanks der betroffenen Colonial Pipeline

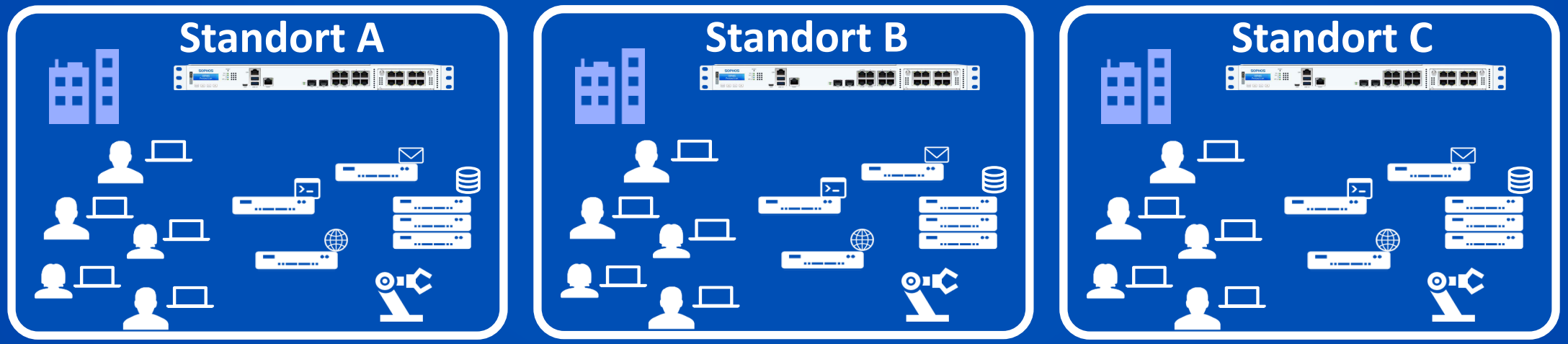
Der Pipeline-Betreiber Colonial wurde über kompromittierte Zugangsdaten gehackt. Laut einem Bericht des Magazins Bloomberg verschaffte sich die Angreifergruppe am 29. April 2021 Zugang zu dem internen Netz von Colonial. Dazu nutzten sie ein VPN-Konto, welches Angestellten den Fernzugriff auf das Netzwerk von Colonial ermöglicht.

ANZEIGE Google Anz Diese Werbung b Warum sehe ich dies

SOPHOS

Herausforderungen von VPN

- Sicherheitsrisiko: „You‘re ON The Network“
- Einschränkung: paralleler Zugriff auf verteilte Ressourcen
- Usability: Manuelle Einwahl statt „Always On“
- Verwaltungsaufwand: Regelwerk, Rollout & Update Clients
- Eingeschränkte Skalierbarkeit

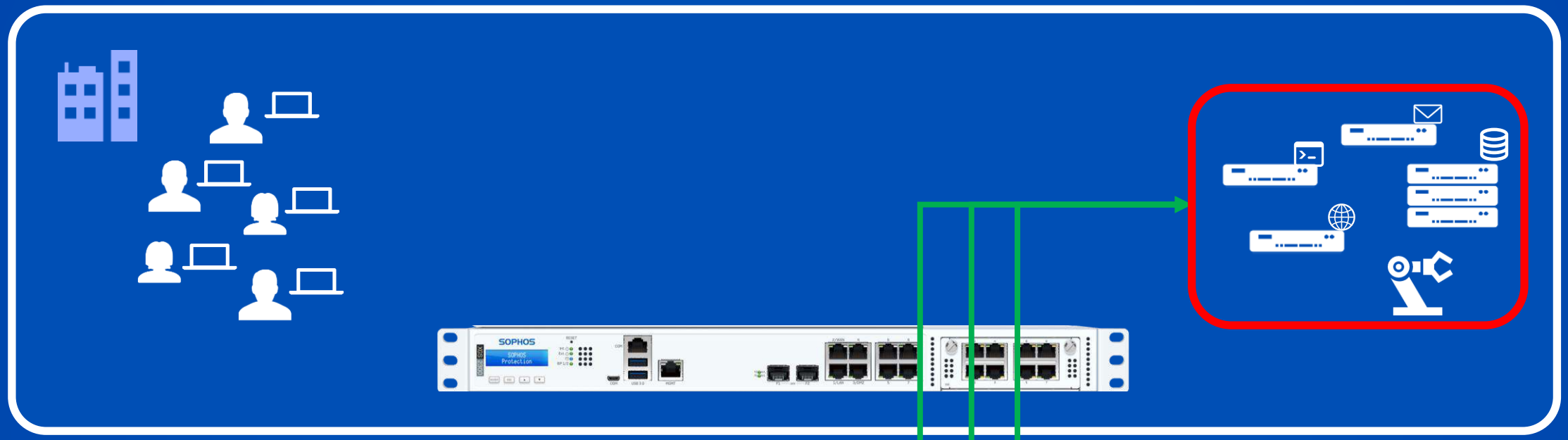


ZTNA

Zero Trust Network Access

SOPHOS

„You‘re ON The Network“

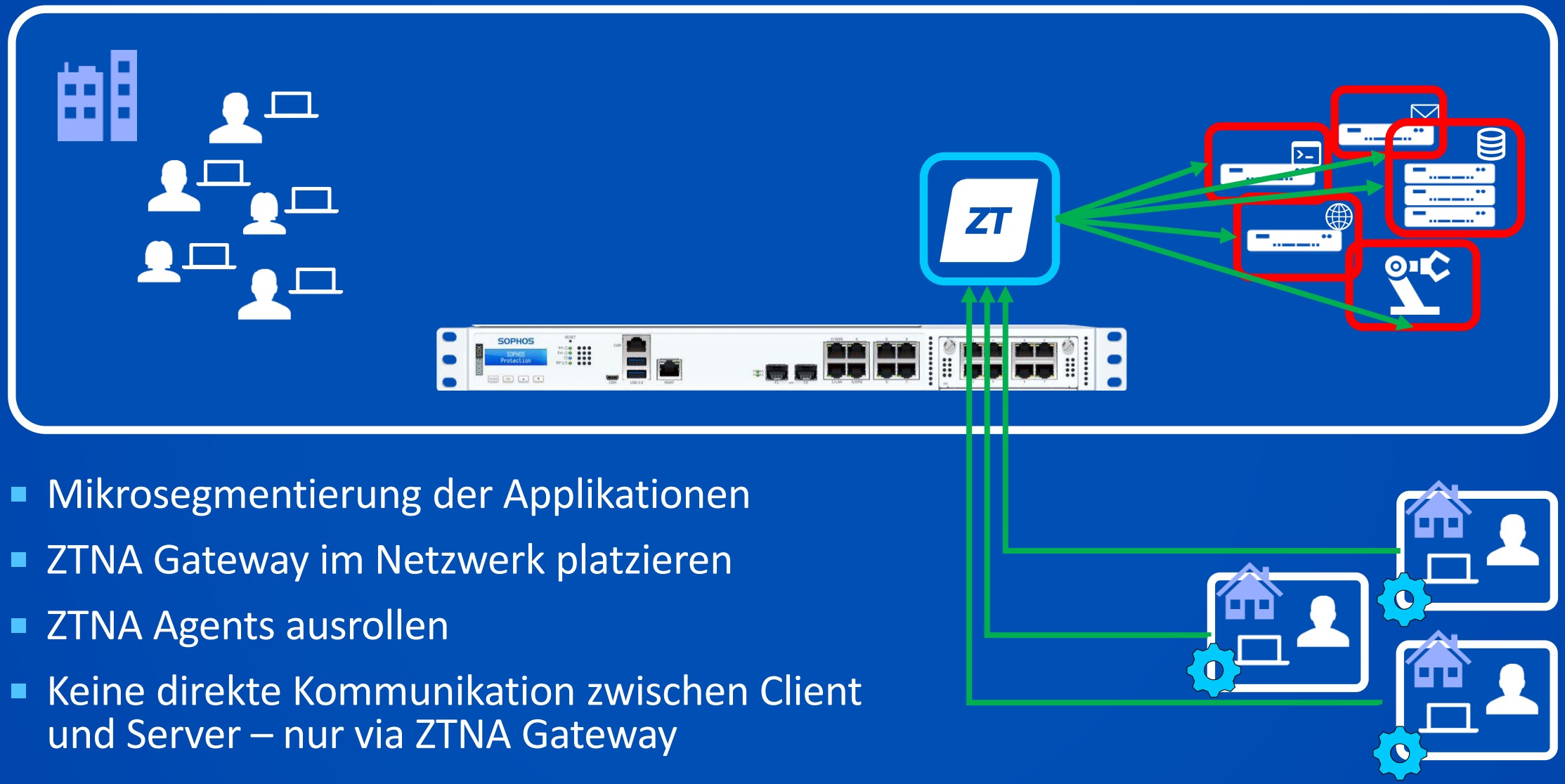


- Großzügiger Zugriff auf (fast) alle Ressourcen
- Direkte Client zu Server Kommunikation
- „VPN ist doch sicher, was soll da passieren?“

„You‘re NOT ON The Network“

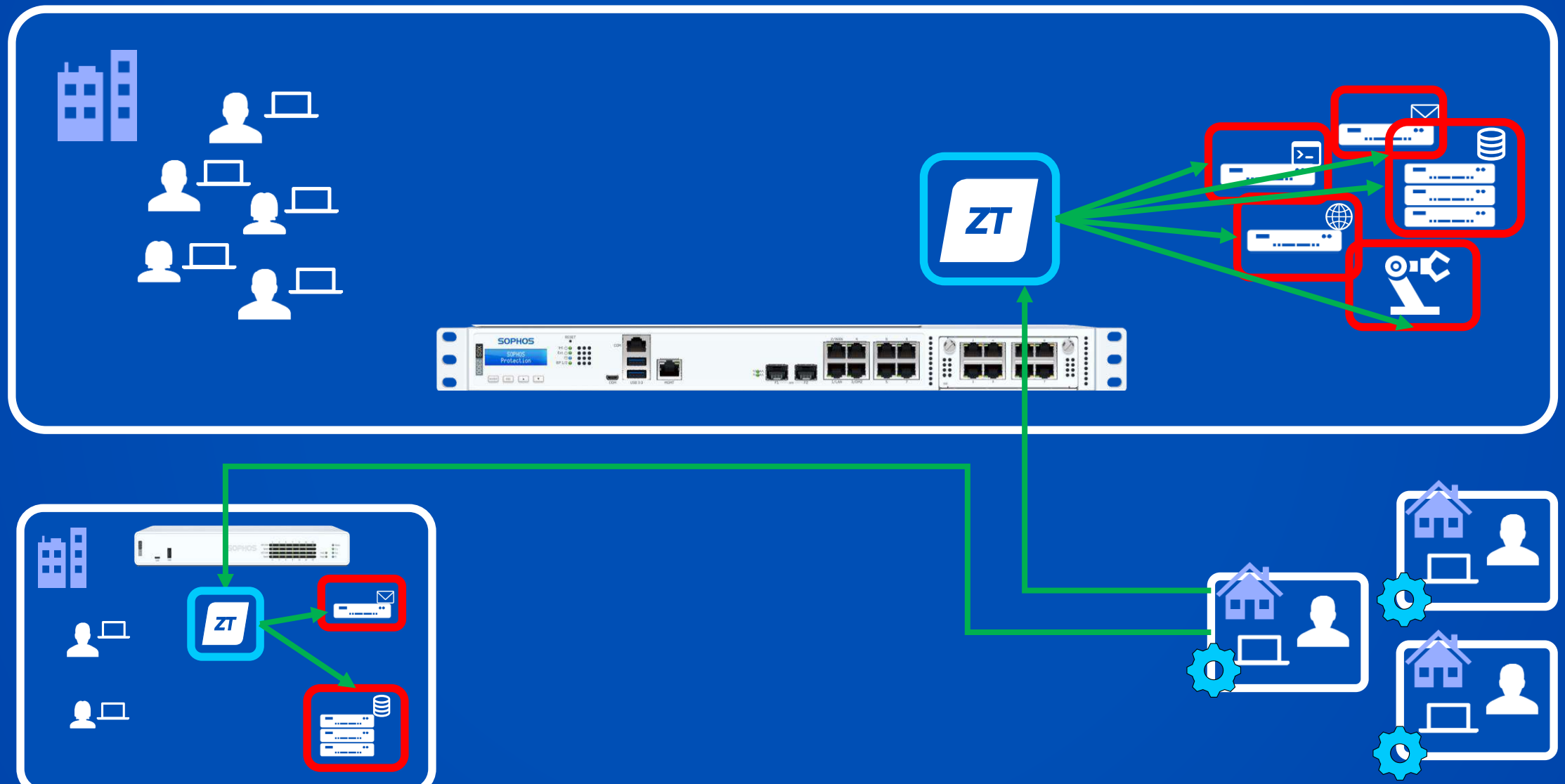
ZTNA Gateway

ZTNA Agent



- Mikrosegmentierung der Applikationen
- ZTNA Gateway im Netzwerk platzieren
- ZTNA Agents ausrollen
- Keine direkte Kommunikation zwischen Client und Server – nur via ZTNA Gateway

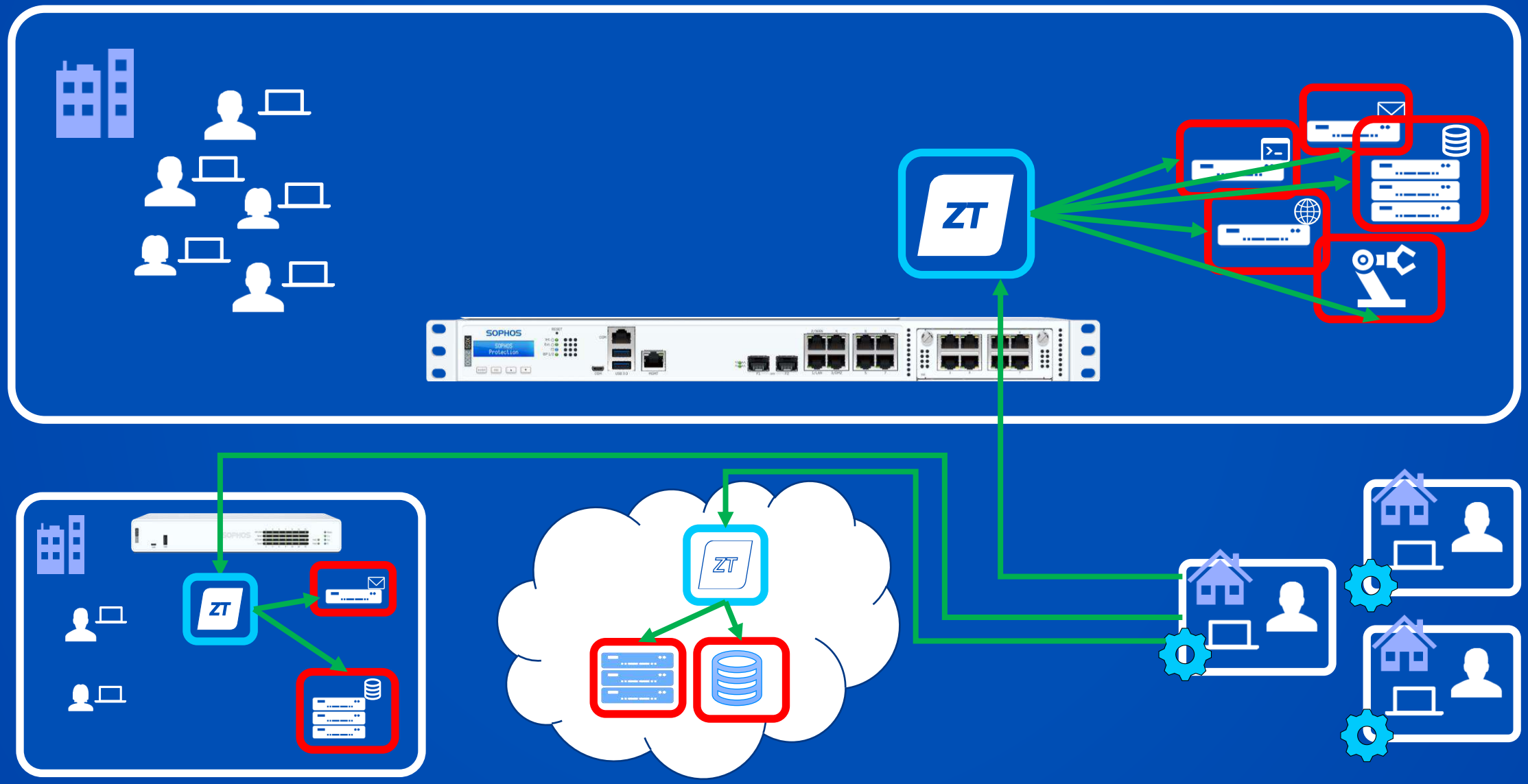
Paralleler Zugriff auf verteilte Ressourcen



Paralleler Zugriff auf verteilte Ressourcen

ZTNA Agent

ZTNA Gateway



SOPHOS

„Drinnen und Draußen“ in der aktuellen Zeit?

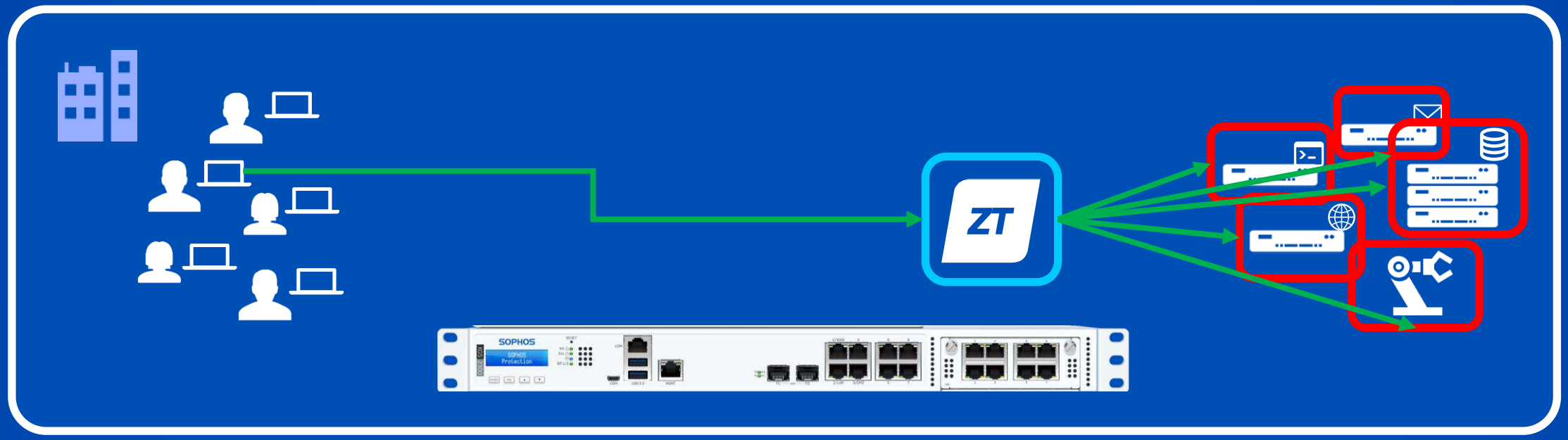
Mobiles Arbeiten - Grenzen verschwimmen

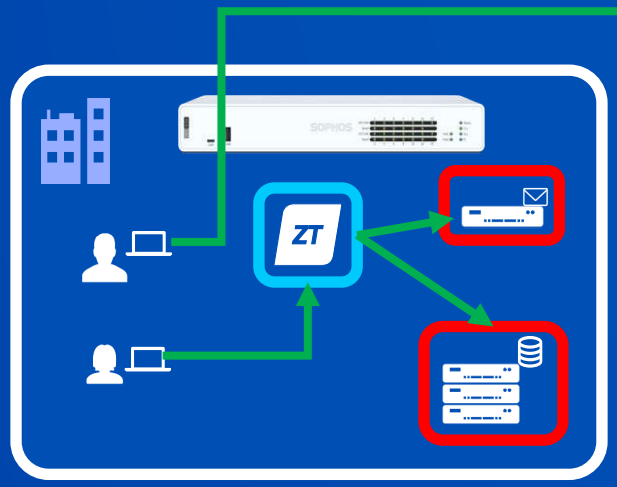
SOPHOS

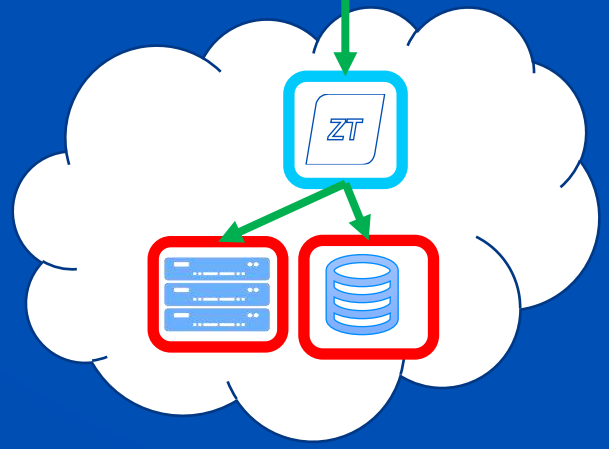
Gleiches Recht für Alle!

ZTNA Agent

ZTNA Gateway







SOPHOS

Wie funktioniert Sophos ZTNA?

ZTNA Agent

ZTNA Gateway

Sophos Central

ZTNA Policy & Management

ZTNA Agent Policy Sync

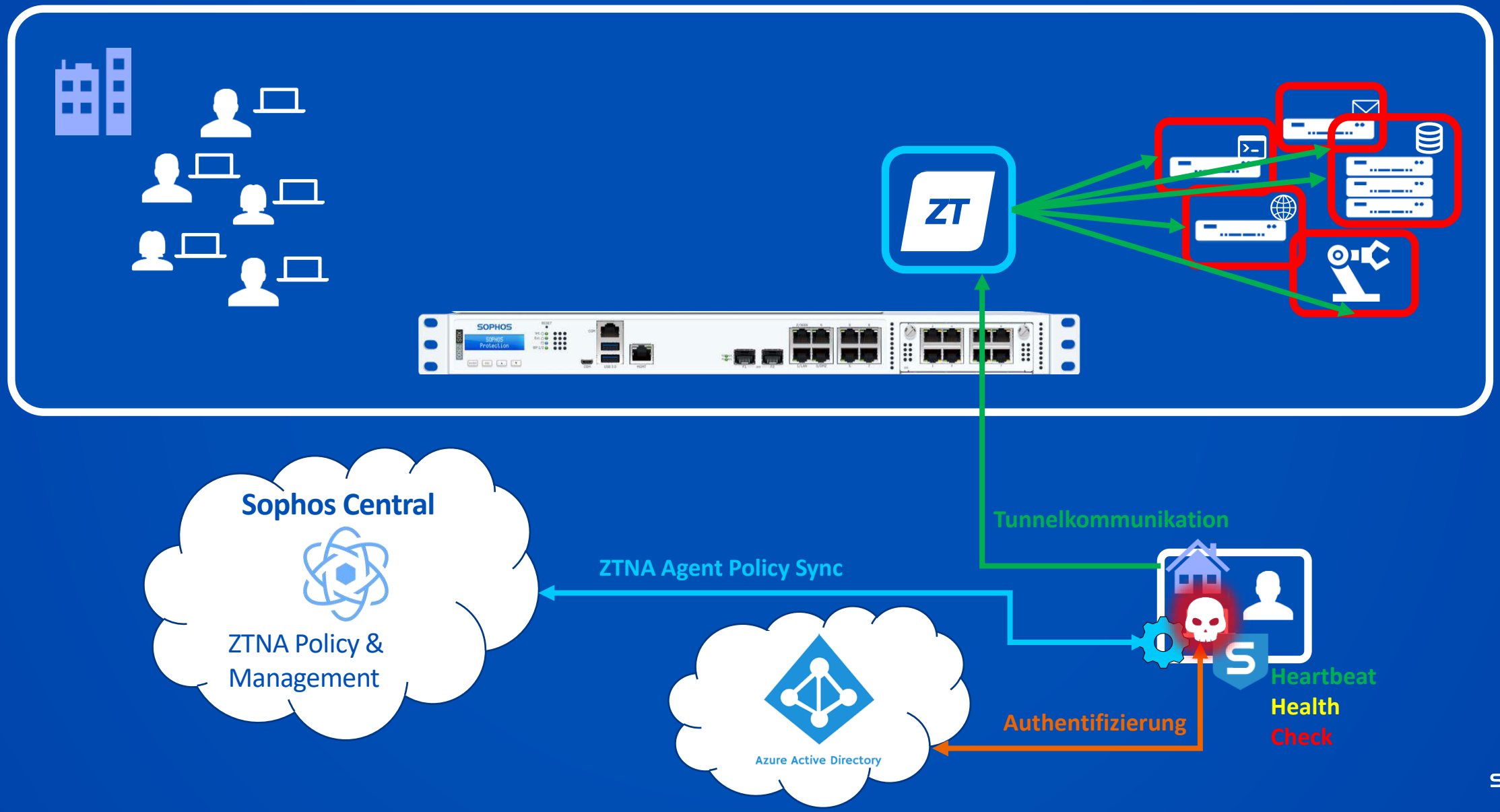
Tunnelkommunikation

Azure Active Directory

Authentifizierung

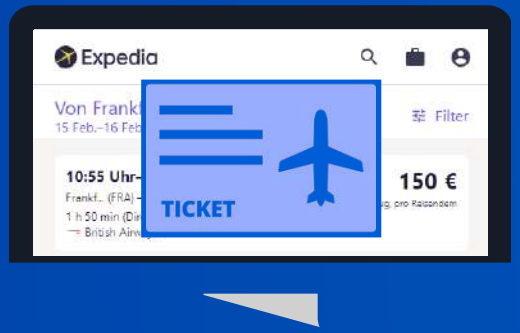
SOPHOS

Sophos ZTNA & Intercept X



Flughafen-Sicherheit damals

Flughafen-Sicherheit heute



Ticketkauf mit Kreditkarte

Überprüfung:

- Ist das Ticket gültig?
- Ist der Pass gültig?
- Stimmt beides überein?

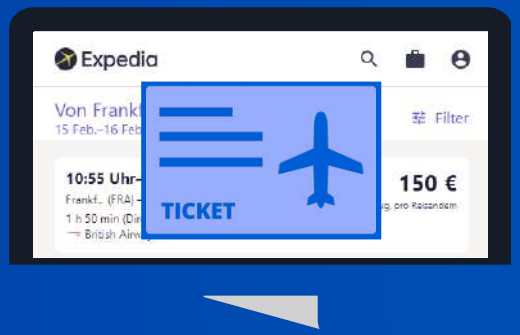
Überprüfung:

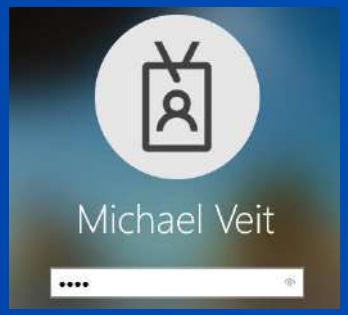
- Waffen, Sprengstoff?
- Darf die Person in ein Flugzeug?

Überprüfung:

- Ist das Ticket gültig?
- Ist der Pass gültig?
- Darf er in dieses Flugzeug?
- Welcher Sitzplatz?

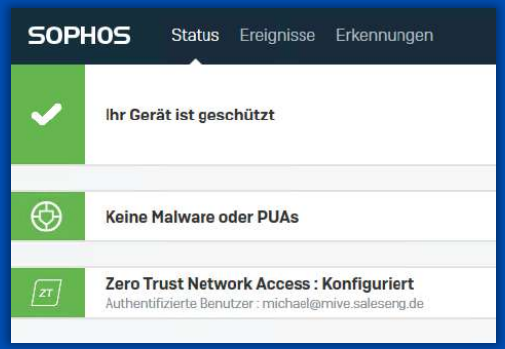
Flughafen-Sicherheit vs. ZTNA Zugriff



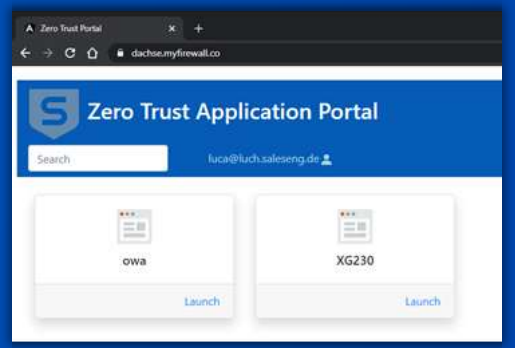


Windows-Anmeldung
mit User/Passwort

MFA Bestätigung
auf Smartphone



Intercept X überprüft,
ob der Computer OK ist



Zugriff nur auf für den User
freigeschaltete Anwendungen

SOPHOS

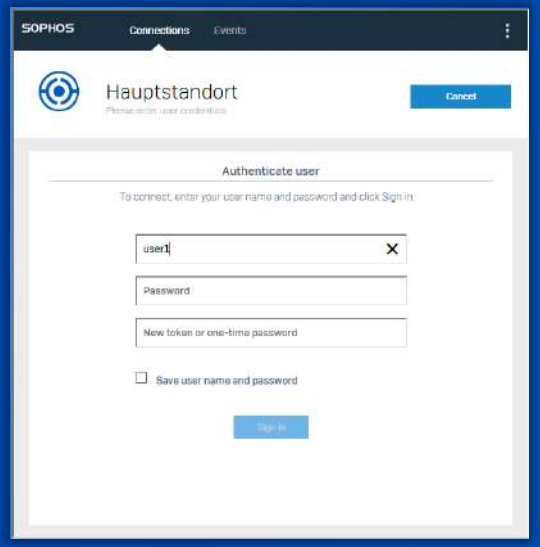
Demo

SOPHOS

Mehrwerte von ZTNA

- Uneingeschränkten Zugriff auf verteilte Ressourcen
- „You are NOT on the network“ - Kein direkter Netzwerkzugriff für ALLE Mitarbeiter
- Permanente Überwachung des Gerätestatus durch Intercept X
- User Experience – Kein Einwahl nötig, permanenter gesicherter Zugriff
- Einfache, zentrale Verwaltung innerhalb von Central
- Schnell und einfach Zugriff für Mitarbeiter und Dienstleister
- Compliance – Sichtbarkeit, wer was darf und wer was gemacht hat

Sicherer Fernzugriff von Sophos für alle Zwecke

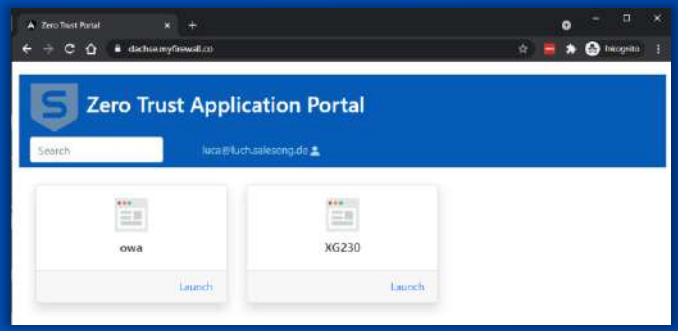


Sophos Connect Software

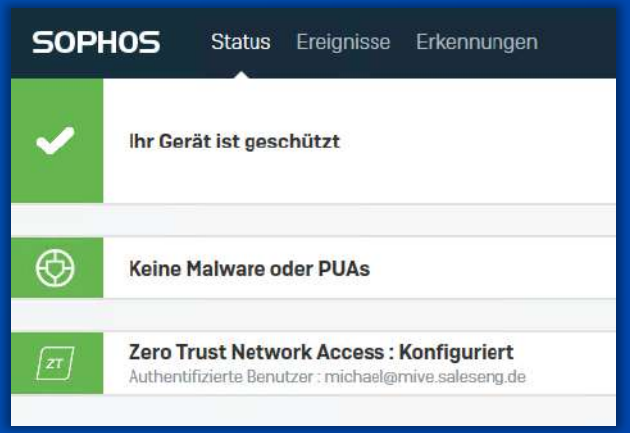
SD-WAN/VPN
für IoT/OT/Server

SD-RED

Kleine Firewalls



Clientless im Browser
oder
ZTNA Agent Software



SOPHOS

Die nächsten Schritte

ZTNA Whitepaper

In diesem Whitepaper gehen wir auf die Einschränkungen und Probleme klassischer Remote-Access-VPN-Lösungen ein und erläutern, welche Vorteile Zero Trust Network Access Unternehmen bietet.

www.sophos.com/de-de/whitepaper/advantages-of-ztna

Webinare

Sophos ZTNA Academy - Teil 1: Einführung in ZTNA

https://events.sophos.com/sophosztnaacademyteil1

Free Trial

Überzeugen Sie sich am besten selbst.

Mit unseren kostenfreien Testversionen, z.B. von Sophos Central, können Sie unsere Lösungen selbst ausprobieren.

www.sophos.com/de-de/products/free-trials

Webinare

Sophos ZTNA Academy - Teil 2: Technik hinter ZTNA

https://events.sophos.com/sophosztnaacademyteil2

SOPHOS