CISCO
SECURE

CISCO The bridge to possible

Zero trust –
traue niemandem!

Dirk Eberwein
Cybersecurity Sales Specialist

Herausforderungen

Angriffsvektoren

User/Homeoffice

Devices

Netzwerk

Anwendungen

Wahrnehmung

It’s segmentation

It’s ZTNA

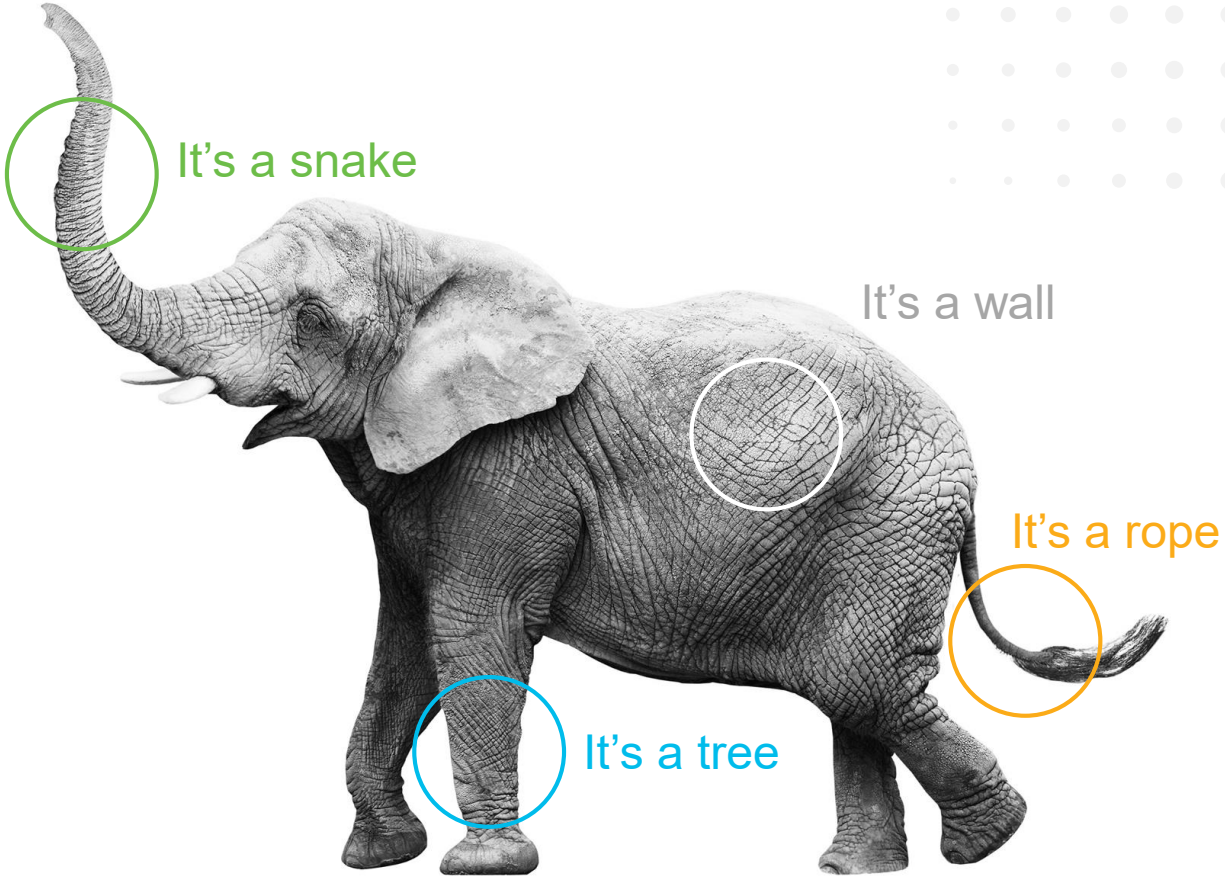
It’s endpoint security

It’s firewall

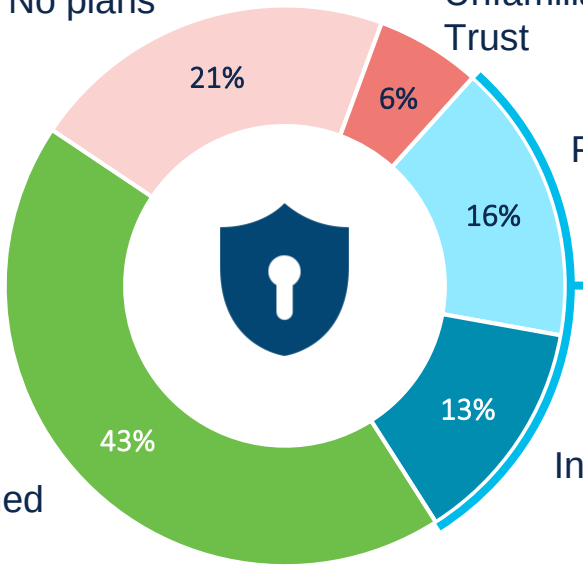
It’s identity

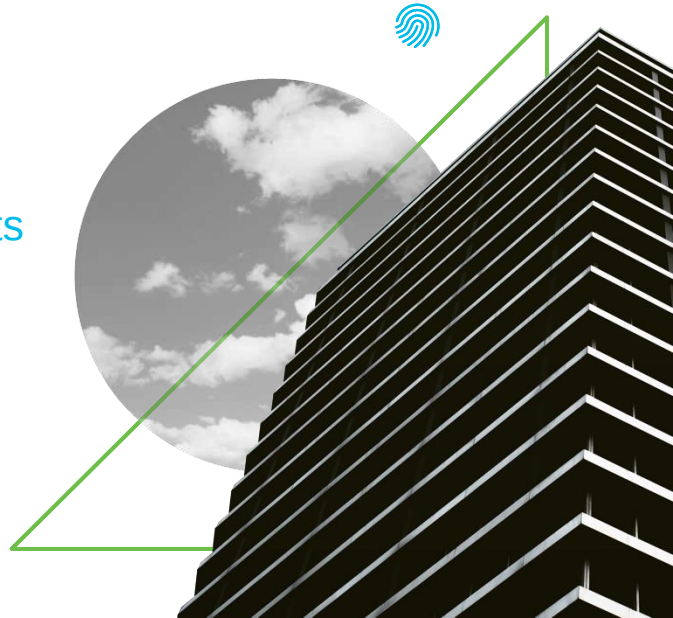
Menschen –
Devices –
Netzwerk –
Anwendungen

With Zero Trust ... everyone has a different perspective



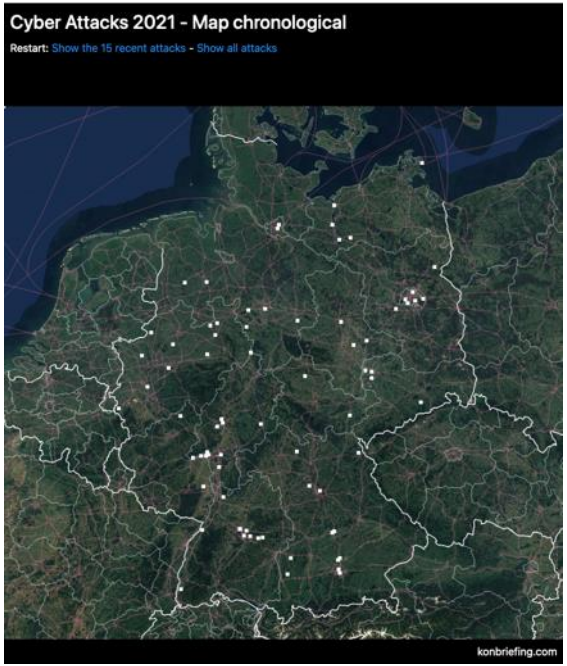
73% of Organizations Plan to Implement Zero Trust





Öffentl. bekannte Cyber Attacken in Deutschland auf einen Blick

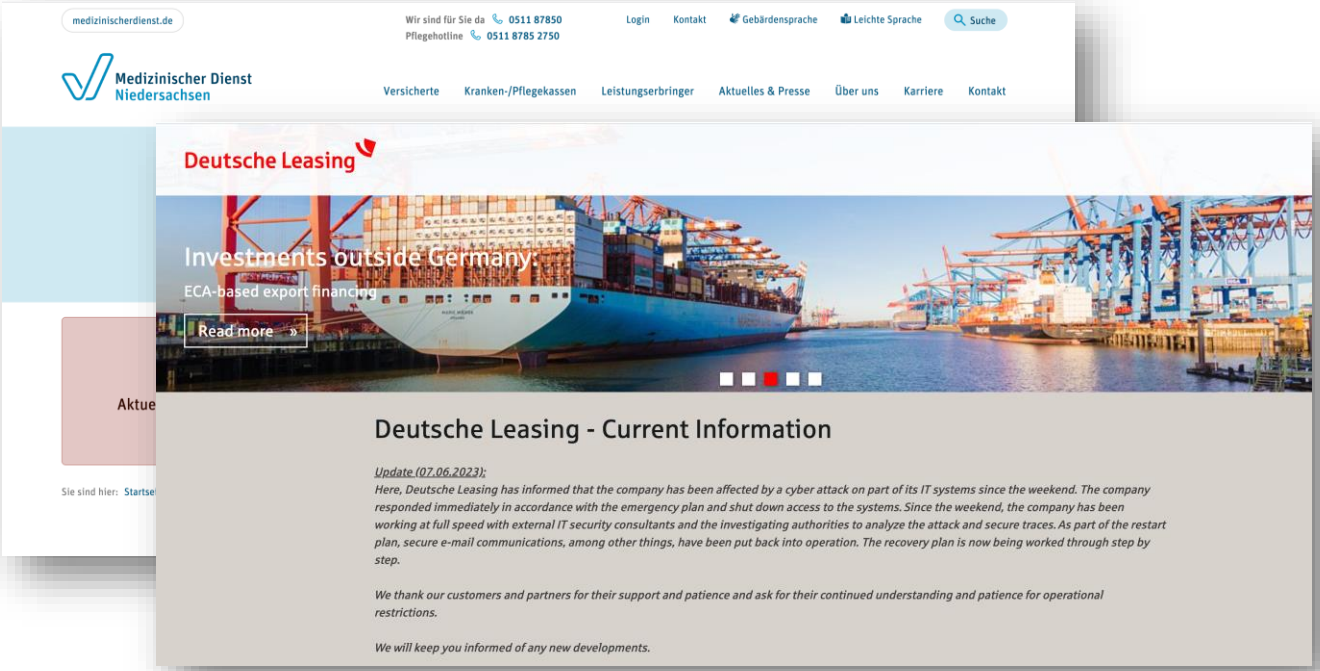
Von September 2021 bis 01. Dezember 2022 aus Verwaltung, Bildung und Gesundheit in Deutschland



- Bundeswahlleiter
- Stadt Leipzig
- Bundestag
- Sozialdienst Olching
- Kreis Wesel
- Stadtwerke Wismar
- Stadt Dessau
- Universität Leipzig
- Kommunalservice Mecklenburg
- Stadt Schwerin
- Stadt Neustadt-Glewe
- Landkreis Ludwigslust-Parchim
- Stadt Witten
- SIS Schwerin
- Verwaltung LAiV Land Mecklenburg-Vorpommern
- Evangelisches Familien-Bildungsstätte Giessen
- Nürnberg Institute of Technology
- Mittelschule Enger
- Mediatixx GmbH (Medical)
- Stadt Sassnitz
- Realschule Enger (NRW)
- Privates Gymnasium Königswinter
- Verbandsgemeindeverw. Seehausen
- Bayrische Krankenhaus Gesellschaft
- Stadtwerke Pirna
- Klinikum Braunschweig
- Leipziger Stadtreinigung
- Zahnarztpraxis Düsseldorf
- Stadt Schmalkalden
- CompuGroup Medical SE
- Unfallkasse Thüringen
- Ev. Schule St. Marien Neubrandenburg
- Medizin Campus Bodensee
- Pfarrei Heilig Kreuz Winnweiler
- FH Münster
- Kunstmuseum Stuttgart
- Museum Ulm
- Hochschule Anhalt
- BBS Goslar
- Stadtverwaltung Bochum
- Stadt Suhl in Thüringen
- BBS Cloppenburg
- Stadt Dingolfing
- TH Aschaffenburg
- Fraunhofer Institut Halle
- Donau-Stadtwerke Dillingen
- Stadt Schriesheim
- Uni-Bibliothek Leipzig
- Hochschule für Technik und Wirtschaft in Berlin
- Bundespolizei und Bundestag
- Stadt Murnau
- Stadt Bissingen
- Stadtreinigung Kassel
- Päd. Hochschule Freiburg
- FH Münster
- Komm DL. Hessen
- Stadt Burladingen
- Uni Wuppertal
- AMEOS Klinikum Neuburg
- Gymnasium Gunzenhausen
- IHK Verbände
- Stadt Stockach
- Stadt Egelsbach
- Gemeinde Dorn-Dürkheim
- Caritasverband
- Kath. Sozialdienstleister SKM Düsseldorf
- Leibniz Institut Frankfurt
- Landtag NRW
- Verwaltung Rhein-Pfalz Kreis
- Hochschule Ansbach
- Schulverwaltung München
- Enercity Stadtwerke Hannover
- Reha Klinik Bad Säckingen
- Hochschule Heilbronn
- Richard Wolf Medizingeräte GmbH
- Klinikum Lippe
- Die Zieglerschen
- TH Ulm
- Goetheschule Hannover
- Universität Duisburg – Essen
- Stadtverwaltung Drensteinfurt NRW

https://konbriefing.com/en-topics/hacker-attacks-germany.html#/

Aktueller Sicherheitsvorfall

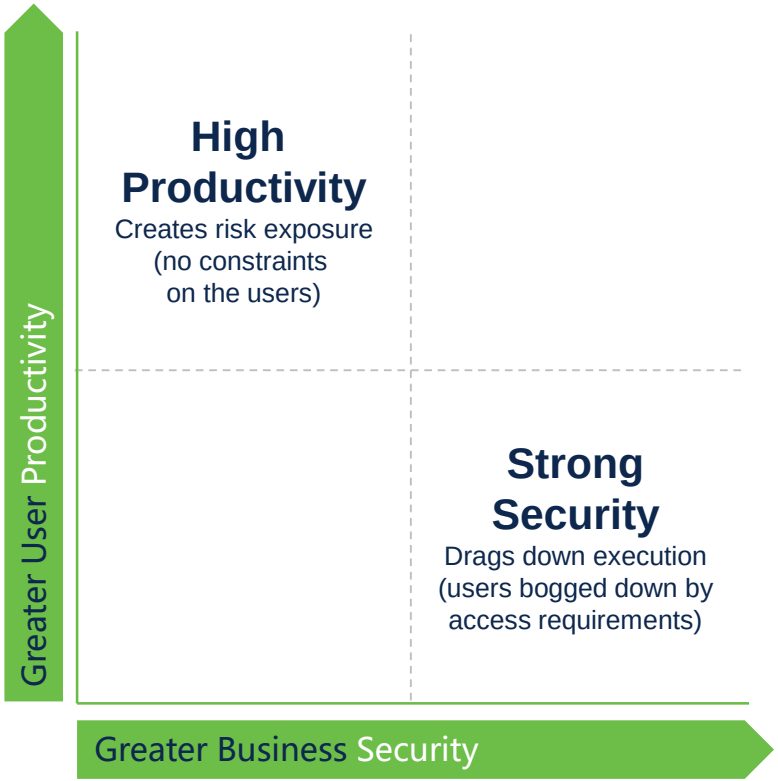


Das “alte” Sicherheitsmodell funktioniert nicht mehr

- Unternehmen im starken Wettbewerb
- Jeder ist ein “Insider”
- Hybrid work is here to stay

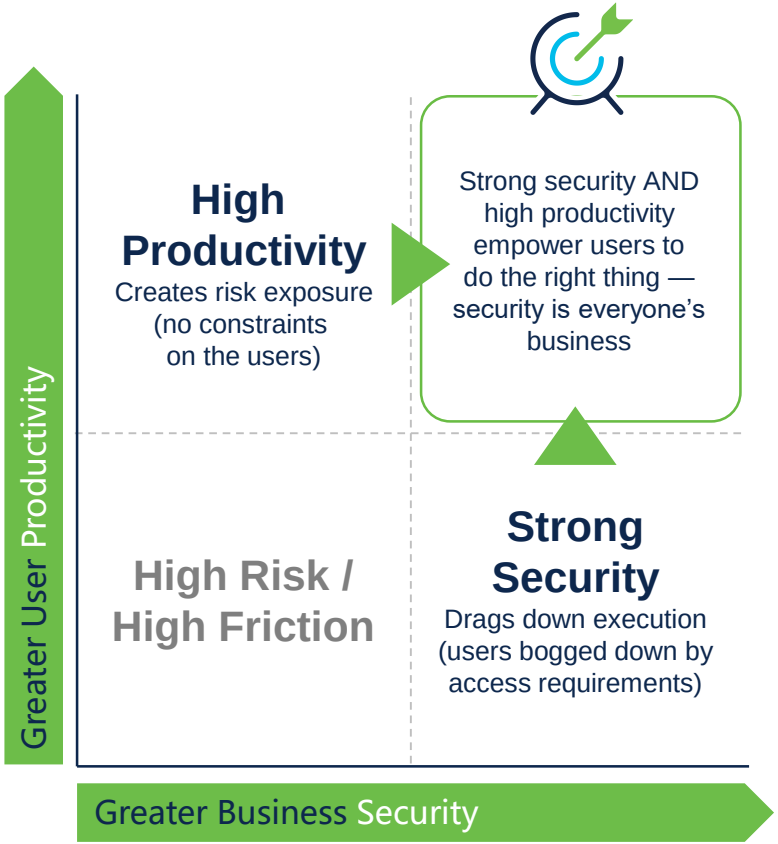
Der heutige Kompromiss ist der Verzicht

Security vs. productivity



Kompromiss beseitigen

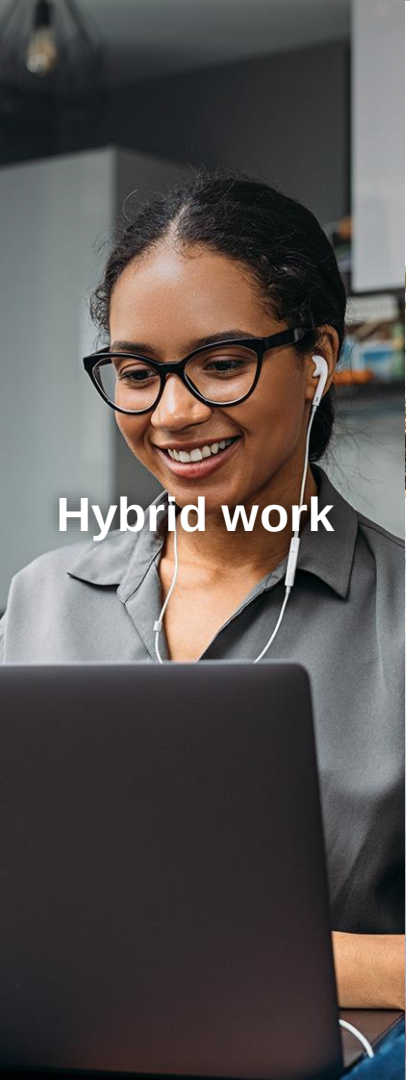
Frustrieren sie Attacker, nicht ihre Anwender



Wie kommen wir ans Ziel?

Zero Trust führt zu mehreren Ergebnissen

1. Security mit einem abgesetztem Perimeter
2. Reaktion auf sich entwickelnde Bedrohungen
3. Zugang zu Ressourcen mit den geringsten Rechten ermöglichen
4. Angriffsfläche verkleinern
5. Einhaltung von Vorschriften

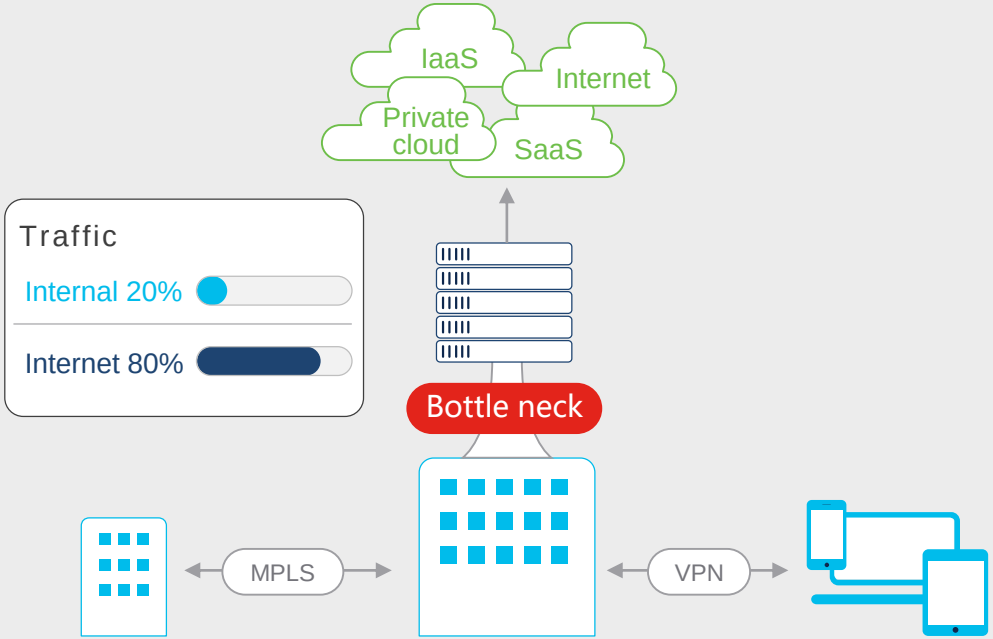


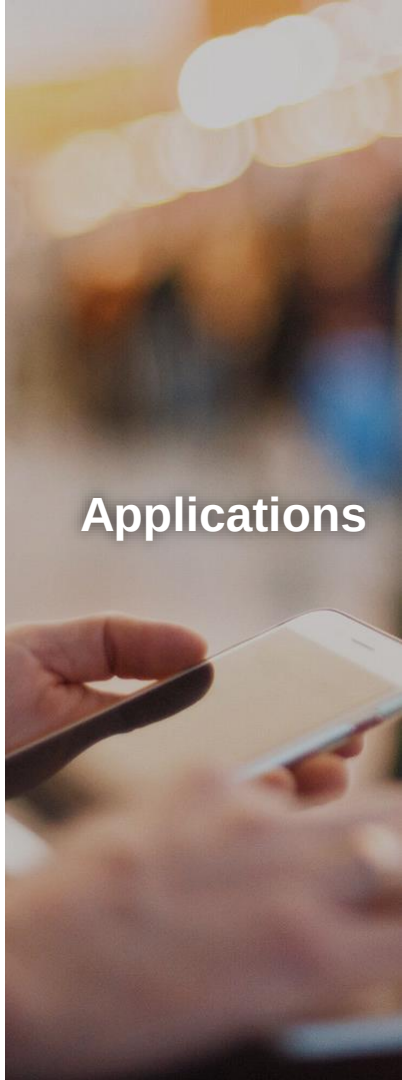
1. Security mit einem abgesetztem Perimeter

Changes in traffic patterns are creating bottlenecks and performance challenges

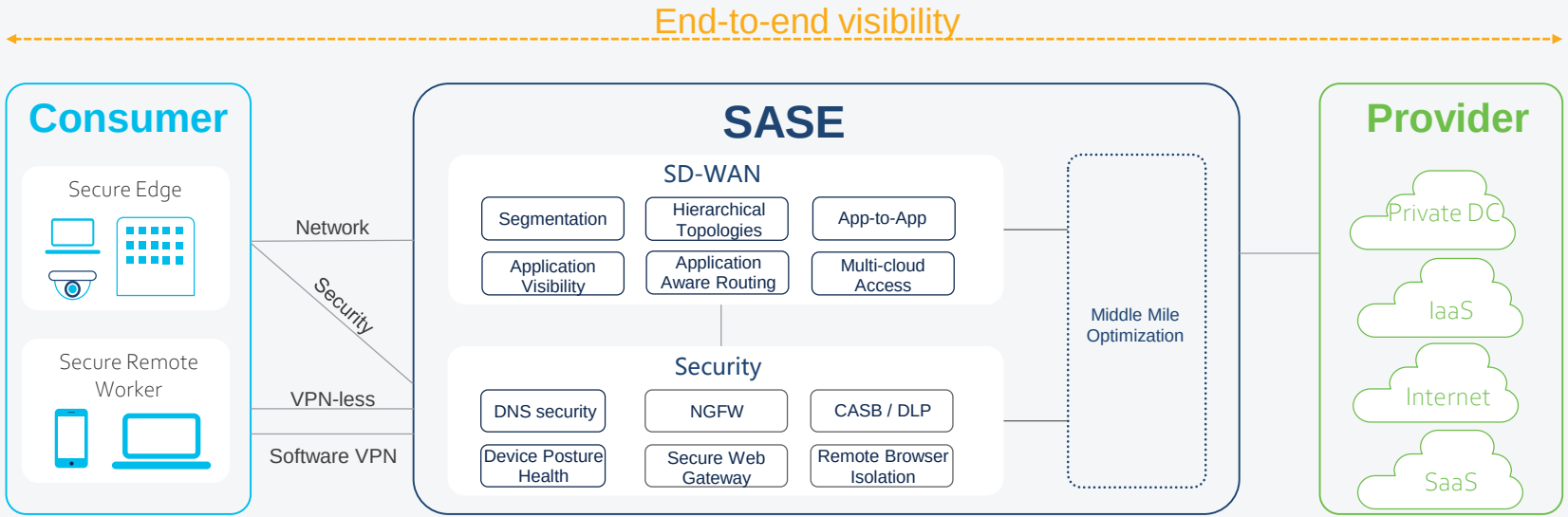
Problems

- App performance
- User experience
- Security efficacy
- # of tools / vendors
- Integrations





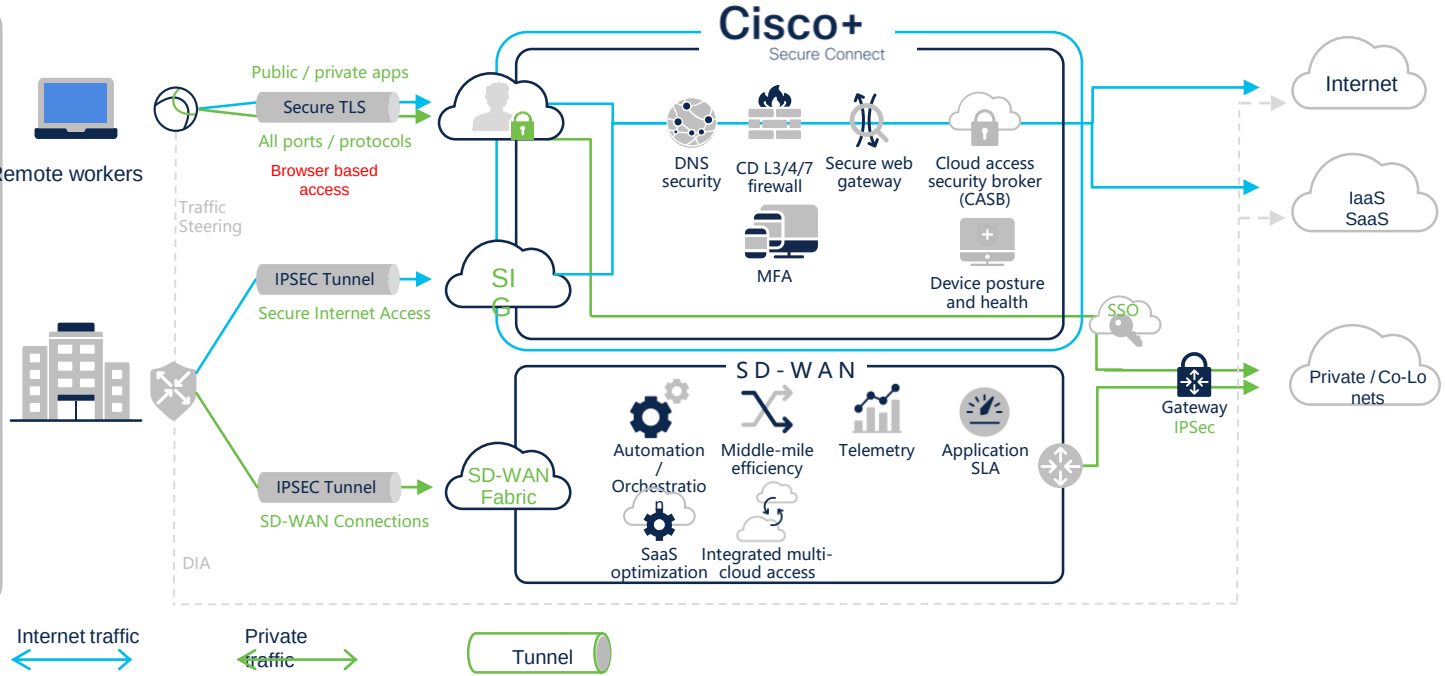
1. Security mit einem abgesetztem Perimeter



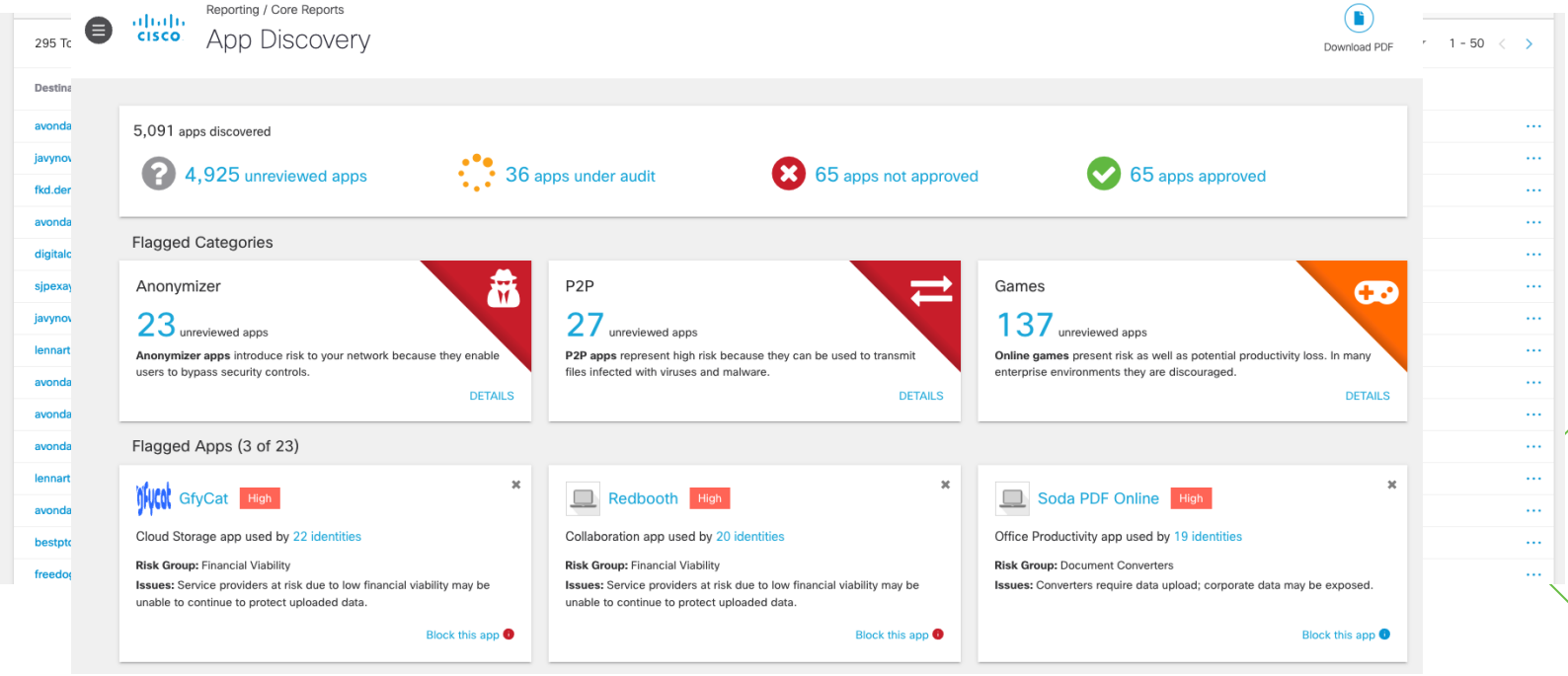
1. Security mit einem abgesetztem Perimeter

CORE ELEMENTS

- Cloud security
  - DNS
  - CDFW
  - SWG
  - CASB
- Secure RaaS
  - Device Posture
- Secure Branch
  - SIG for Internet
- Existing SD—WAN Fabric



2. Reaktion auf sich entwickelnde Bedrohungen



2. Reaktion auf sich entwickelnde Bedrohungen

Cisco Umbrella

DNS-layer security

Firewall as a Service (FWaaS)

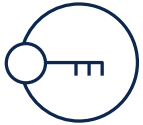
Cloud Access Security Broker (CASB)

- App Discovery and Control
- Cloud Malware Detection
- Data Loss Prevention (DLP)

Cisco Talos Threat Intelligence

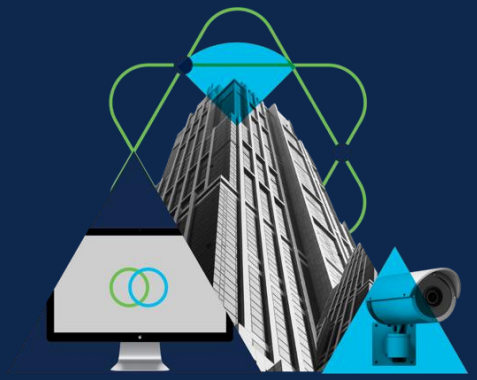
Secure Web Gateway (SWG)

Remote Browser Isolation (RBI)



Zero Trust Network Access (ZTNA)

3. Zugang zu Ressourcen mit den geringsten Rechten ermöglichen



Grant the right level of network access to users and devices

Classify and segment users, devices and apps on your network

Contain infected endpoints and revoke network access

By

Network authentication and authorization

Network segmentation

Continuously monitoring and responding to threats

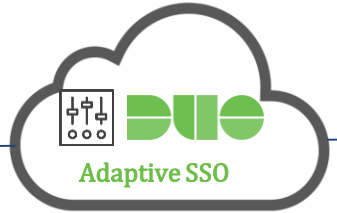
3. Zugang zu Ressourcen mit den geringsten Rechten ermöglichen

Device Health Checks

- OS version + patch level
- Browser version
- Disk encryption
- Password / biometrics
- Host firewall (Workstations)
- Rooted / Jailbroken (Mobile)

Third-Party Posture Signals

- Management status (MDM)
- Endpoint agent presence (AV/EDR)
- Malware infection status



Contextual Factors:

- User Groups
- Application
- Device Trust
- Location
- Network

Allow access for **secure and compliant** unmanaged devices

Allow only **managed and trusted devices** to access sensitive data.

Block access for **non-compliant** devices and enable self-remediation.

4. Angriffsfläche verkleinern

Herausforderung

Establish Trust

Enforce Trust-Based Access

Continuously Verify Trust

Challenge:

- Unbefugter Zugriff über gestohlene oder kompromittierte Anmeldedaten
- BYOD-Sicherheit und Transparenz

Challenge:

- Schützen Sie jede Anwendung mit kontextbasierten Richtlinien
- Erlauben Sie Benutzern nur den Zugriff auf Anwendungen und Daten, die sie benötigen

Challenge:

- Verhindern, dass Geräte mit Malware auf Anwendungen und Daten zugreifen können
- Überprüfen Sie Benutzer bei jedem Anmeldeversuch

4. Angriffsfläche verkleinern

Lösung

Establish Trust

Enforce Trust-Based Access

Continuously Verify Trust

Solution:
Überprüfen Sie das Vertrauen von Benutzern und Geräten mit Multi-Faktor-Authentifizierung (MFA)

Solution:
Durchsetzung von Zugriffsrichtlinien für jede Anwendung mit adaptiven und rollenbasierten Zugriffskontrollen

Solution:
Kontinuierliche Überwachung risikobehafteter Geräte mit Endpoint Health & Management Status

WHY Cisco??

Integration statt Einzelbetrachtung

CISCO SECURE

Security Reference Architecture

Threat Intelligence | Malware Analytics | Actionable Intelligence | Unmatched Visibility | Collective Responses

Security Operations

XDR

- Managed Detection and Response Services
- Security, Orchestration, Automation and Response
- Incident Response and Remediation Services
- Threat Visibility & Hunting
- Asset Inventory
- Vulnerability Mgmt
- Cloud Posture Mgmt
- 3rd Party Integrations

User/Device Security

ZERO TRUST

Adaptive MFA | Passwordless | Trust

Secure Access | Secure E-mail

SASE/REMOTE WORKER

Unified Client | EDR | Cloud Managed

Secure Client

- VPN
- Posture
- Telemetry
- Threat
- Query
- Visibility

Network Security

Cloud Edge

SECURE ACCESS SERVICE EDGE (SASE)

Threat Protection | Secure Access Control | Managed Remote Access

Cloud Security

- ZTNA
- DNS-layer security
- Secure web gateway
- L7 firewall + IPS
- Cloud access security broker/ shadow IT
- RAaaS
- SSL decryption
- Remote browser Isolation
- Data loss prevention
- Cloud malware detection

PRIVATE CLOUD EDGE (MSP or CUSTOMER)

Reliable | Scalable | Flexible | Visibility

SDWAN

SDWAN | Firewall | Visibility | Cloud DDoS

On-Premises

SASE/SDWAN

Scalable | Flexible | Visibility | Comprehensive Security

Network Edge

SDWAN | Firewall | Visibility

IoT/OT SECURITY

Secure Critical Infrastructure | Unified IT and OT

Industrial Router | Industrial Firewall | Industrial Switch/AP | Identity

ZERO TRUST

Segmentation | Identity and Context | Profiling | Containment | Encrypted Visibility

Firewall

Logging | DDoS protection | Flow Analytics | Identity | Segmentation

Web Security

Application Security

ZERO TRUST

Policy | API Security
Application Segmentation
Run-time Application Security

Application Security Stack

- Cloud Native Security
- App Segmentation
- Workload Security
- Secure Application

App Visibility | Detection | Response

Hybrid Private | Public Cloud*

- Cloud Analytics
- Firewall
- Visibility
- DDoS/WAF

CISCO SECURE