

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



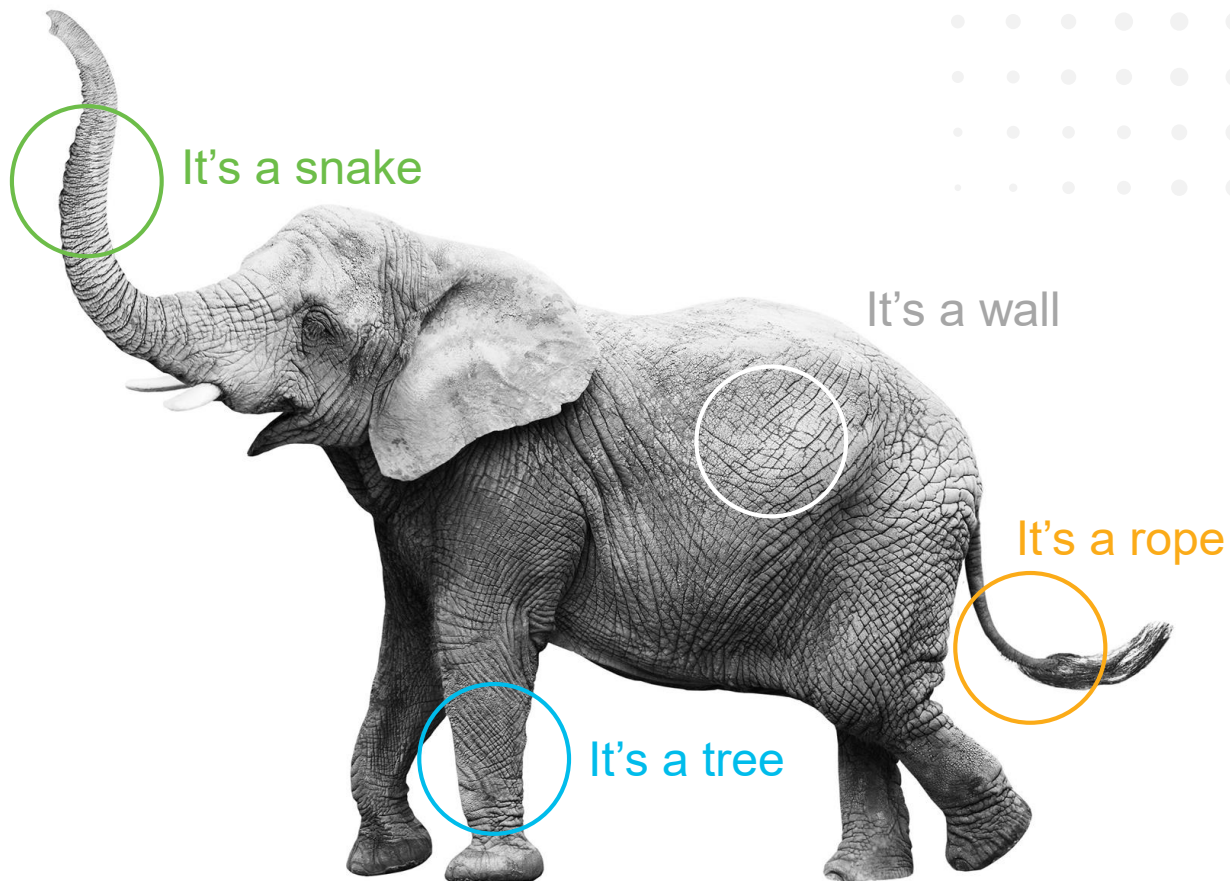
It's firewall



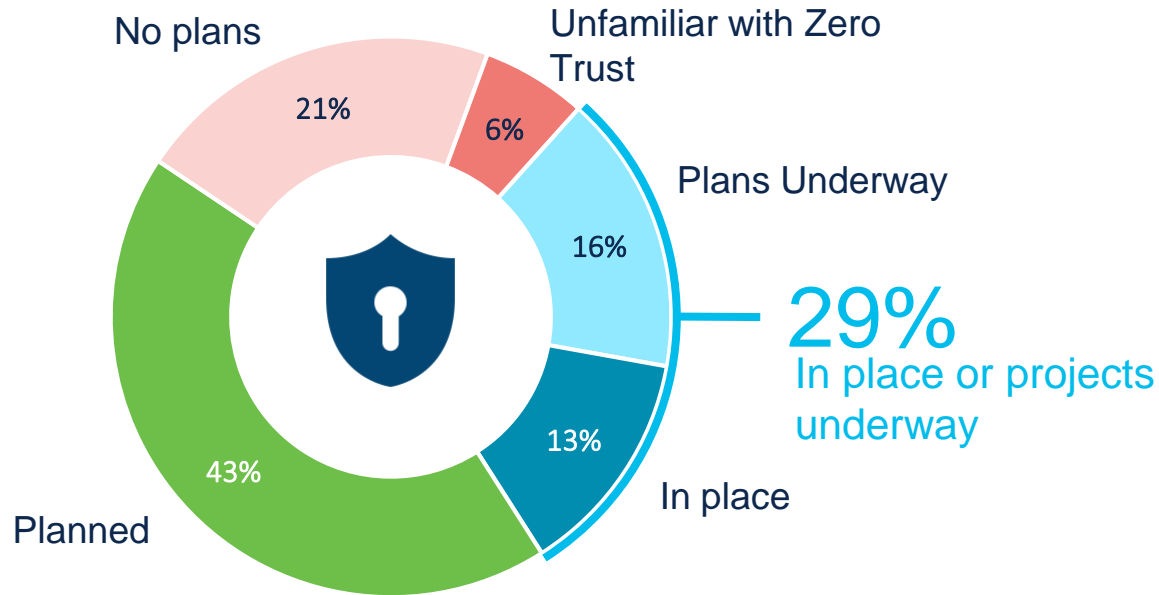
It's identity

Menschen –
Devices –
Netzwerk –
Anwendungen

With Zero Trust
... everyone has
a different
perspective

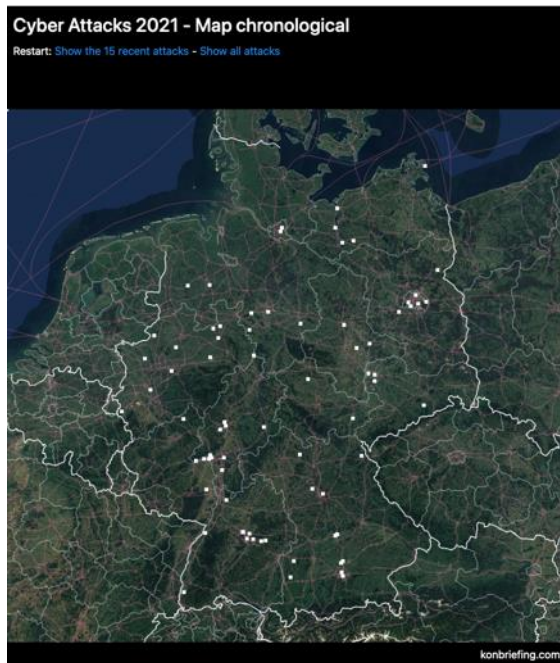


73% of Organizations Plan to Implement Zero Trust



Öffentl. bekannte Cyber Attacken in Deutschland auf einen Blick

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

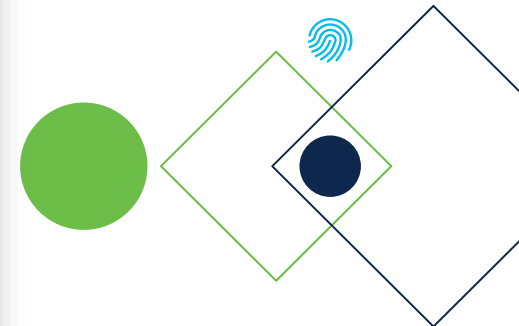


- Bundeswahlleiter
- Stadt Leipzig
- Bundestag
- Sozialdienst Olching
- Kreis Wesel
- Stadtwerke Wismar
- Stadt Dessau
- Universität Leipzig
- Kommunalservice Mecklenburg
- Stadt Schwerin
- Stadt Neustadt-Glewe
- Landkreis Ludwigslust-Parchim
- Stadt Witten
- SIS Schwerin
- Verwaltung LAiV Land Mecklenburg-Vorpommern
- Evangelisches Familien-Bildungsstätte Giessen
- Nürnberg Institute of Technology
- Mittelschule Enger
- Mediatrix 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

The screenshot shows the website for Medizinischer Dienst Niedersachsen. The header includes the company name, phone numbers (0511 87850 and 0511 8785 2750), and navigation links for Login, Kontakt, Gebärdensprache, and Leichte Sprache. A search bar is also present. The main content area features a large image of a container ship at a port with the Deutsche Leasing logo. Below the image, the text reads: "Investments outside Germany. ECA-based export financing." and "Read more". The main heading is "Deutsche Leasing - Current Information". The update date is "Update (07.06.2023)". The text states: "Here, Deutsche Leasing has informed that the company has been affected by a cyber attack on part of its IT systems since the weekend. The company responded immediately in accordance with the emergency plan and shut down access to the systems. Since the weekend, the company has been working at full speed with external IT security consultants and the investigating authorities to analyze the attack and secure traces. As part of the restart plan, secure e-mail communications, among other things, have been put back into operation. The recovery plan is now being worked through step by step." Below this, it says: "We thank our customers and partners for their support and patience and ask for their continued understanding and patience for operational restrictions." and "We will keep you informed of any new developments."

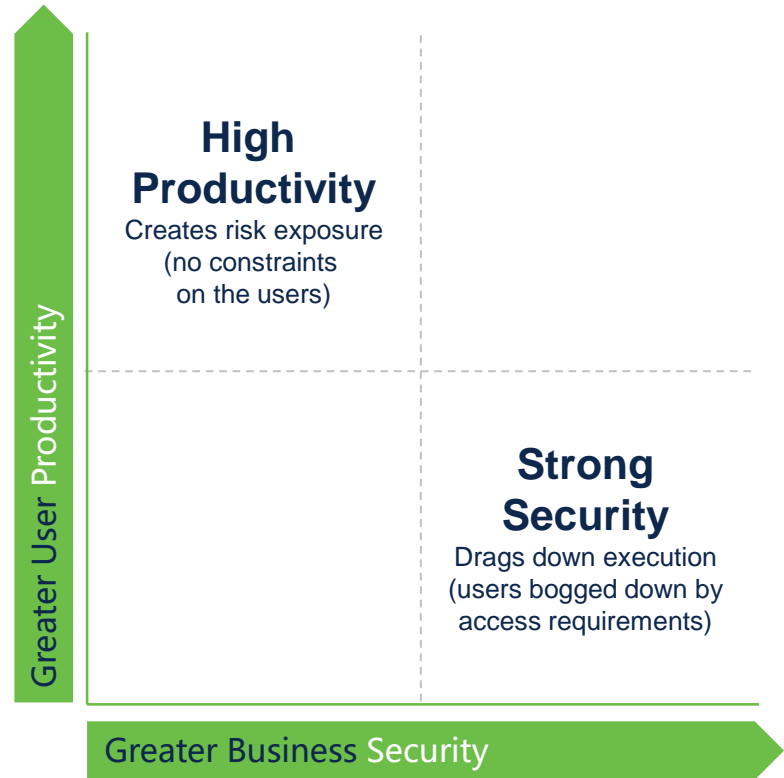


Das “alte” Sicherheitsmodell funktioniert nicht mehr

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

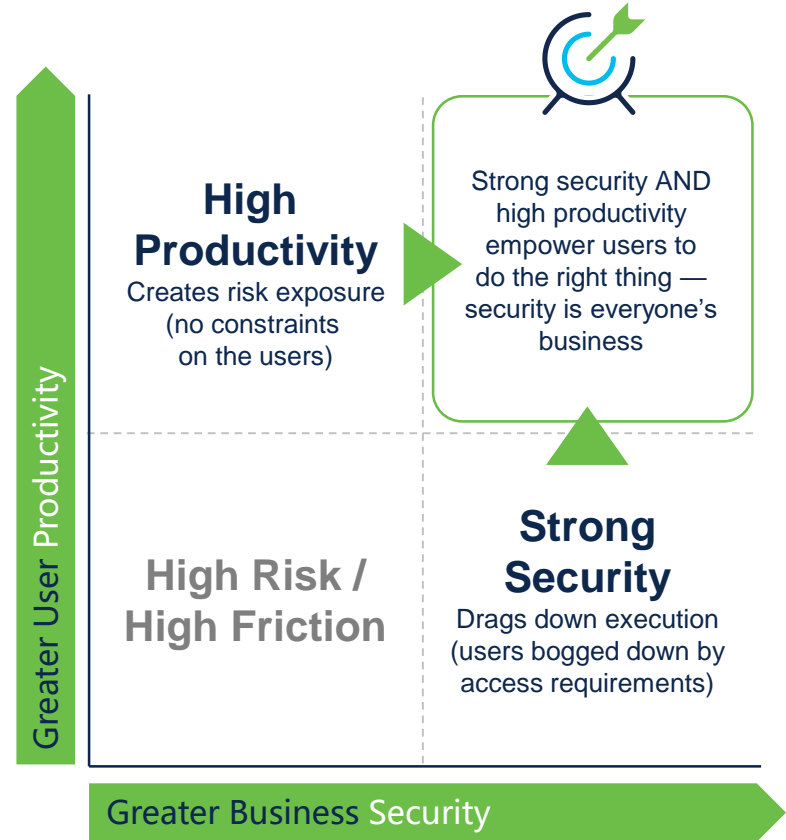
Der heutige Kompromiss ist der Verzicht

Security vs.
productivity



Kompromiss beseitigen

Frustrieren sie Attacker, nicht
ihre Anwender



A scenic landscape featuring a winding asphalt road that curves through a hilly area. On the left, a grassy hillside rises, with a few small figures of people visible on its crest. The sky is a vibrant mix of deep blue and golden yellow, indicating a sunset or sunrise. Numerous birds are scattered across the sky, some in flight. The overall atmosphere is serene and contemplative.

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



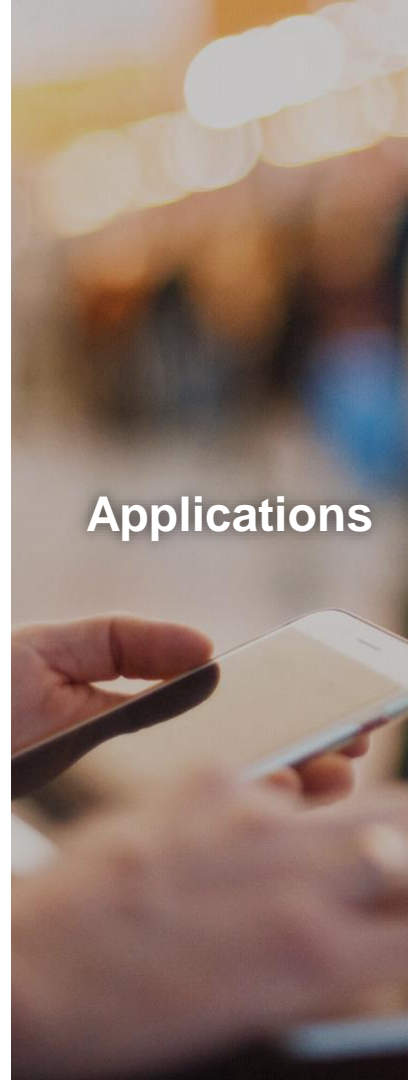
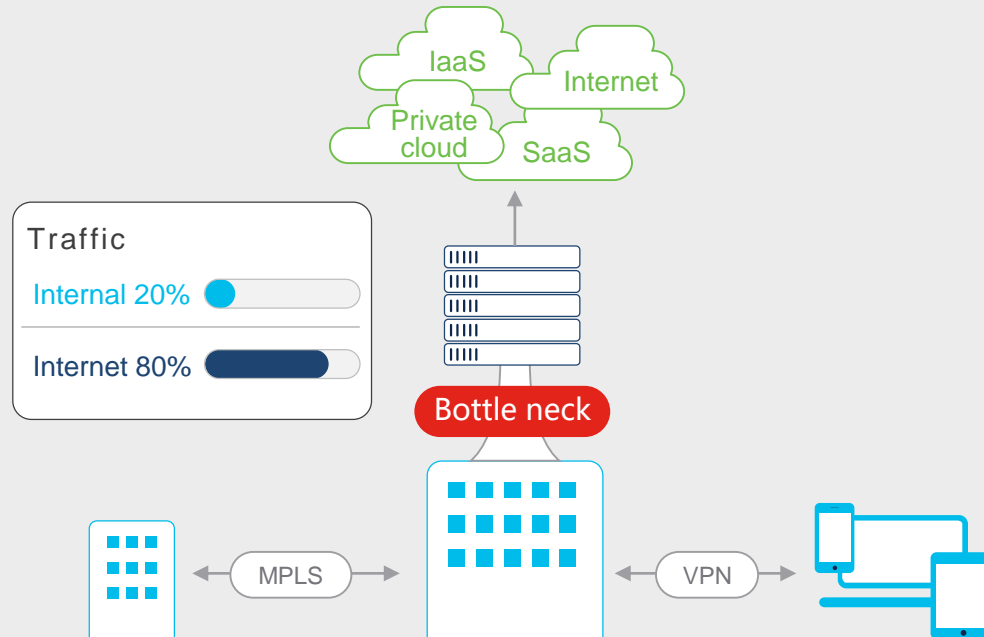
Hybrid work

1. Security mit einem abgesetztem Perimeter

Changes in traffic patterns are creating bottlenecks and performance challenges

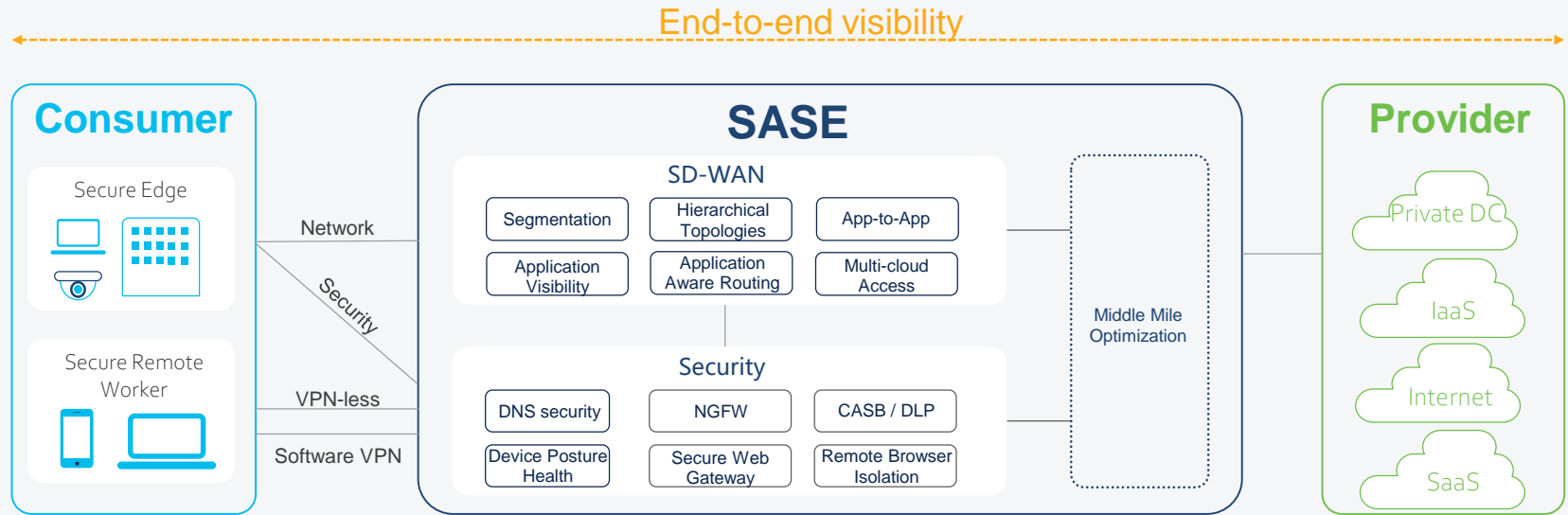
Problems

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

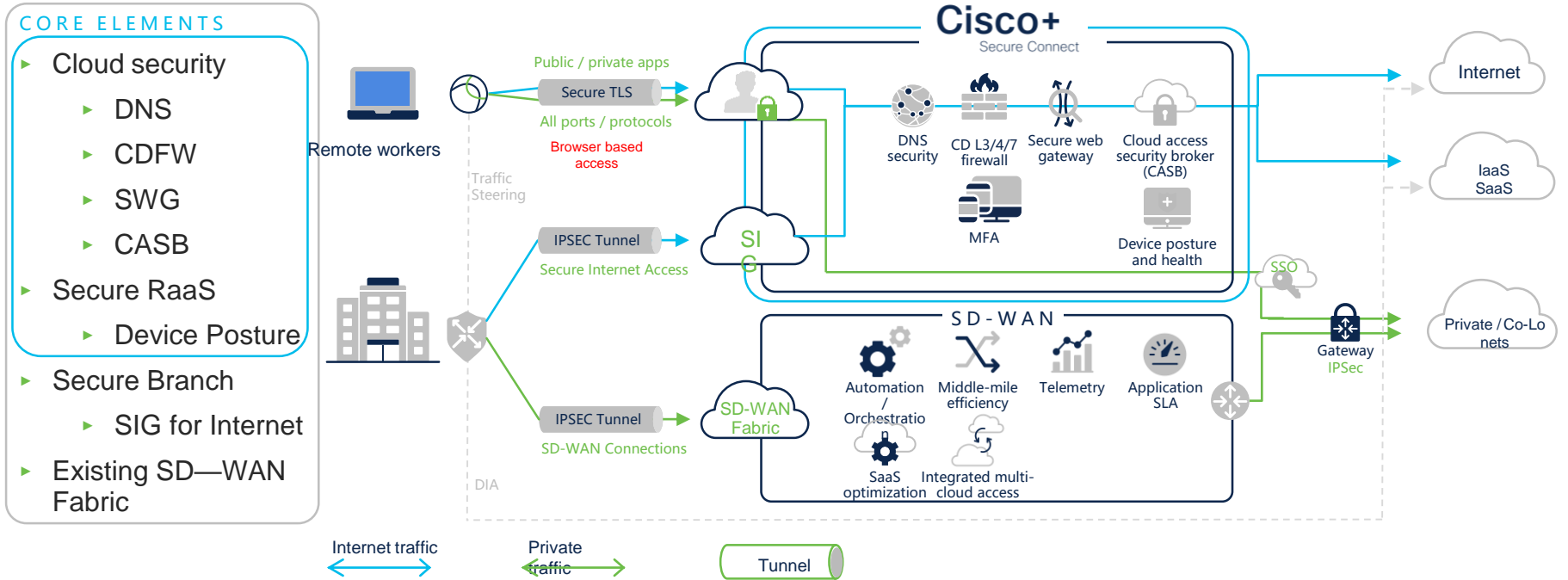


Applications

1. Security mit einem abgesetztem Perimeter



1. Security mit einem abgesetztem Perimeter



2. Reaktion auf sich entwickelnde Bedrohungen

Reporting / Core Reports
App Discovery

295 Tc

Download PDF 1 - 50

5,091 apps discovered

- 4,925 unreviewed apps
- 36 apps under audit
- 65 apps not approved
- 65 apps approved

Flagged Categories

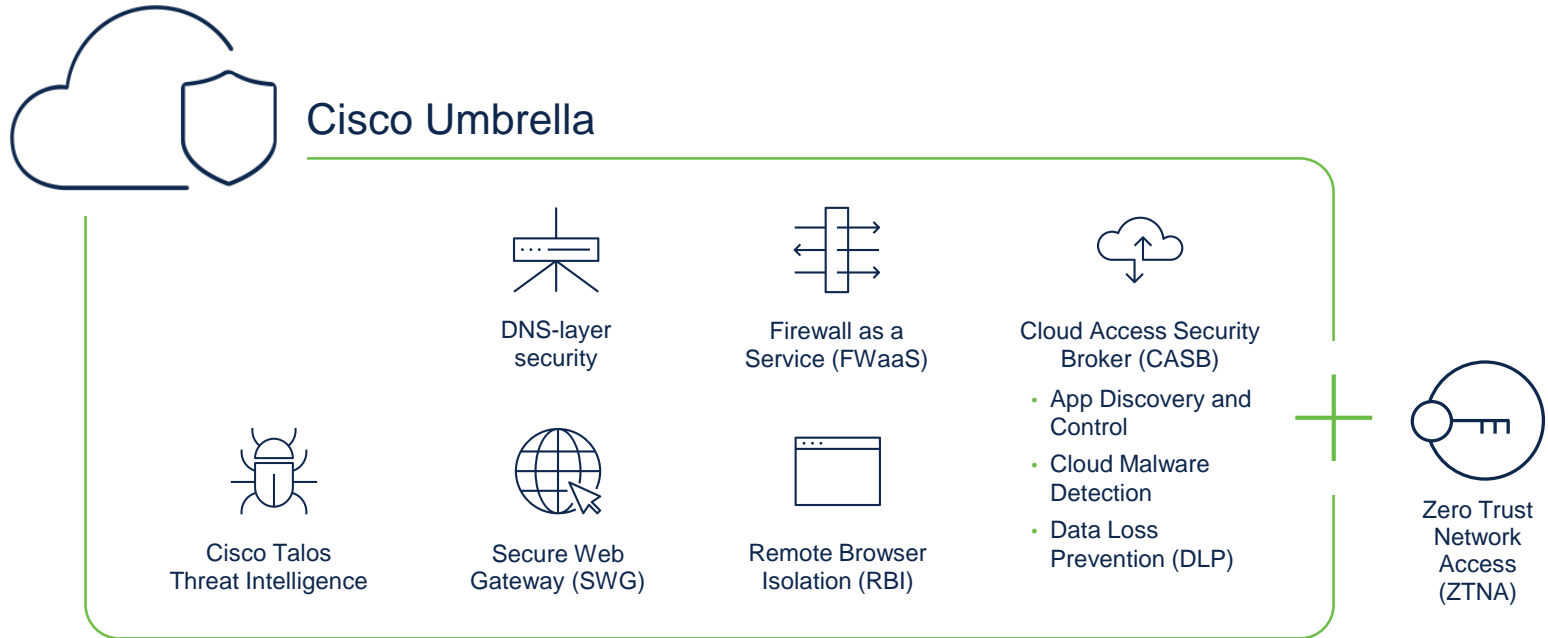
Category	Count	Description
Anonymizer	23 unreviewed apps	Anonymizer apps introduce risk to your network because they enable users to bypass security controls.
P2P	27 unreviewed apps	P2P apps represent high risk because they can be used to transmit files infected with viruses and malware.
Games	137 unreviewed apps	Online games present risk as well as potential productivity loss. In many enterprise environments they are discouraged.

Flagged Apps (3 of 23)

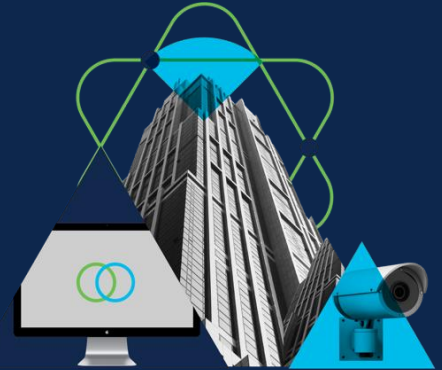
App Name	Risk Level	Usage	Risk Group	Issues
GfyCat	High	Cloud Storage app used by 22 identities	Financial Viability	Service providers at risk due to low financial viability may be unable to continue to protect uploaded data.
Redbooth	High	Collaboration app used by 20 identities	Financial Viability	Service providers at risk due to low financial viability may be unable to continue to protect uploaded data.
Soda PDF Online	High	Office Productivity app used by 19 identities	Document Converters	Converters require data upload; corporate data may be exposed.



2. Reaktion auf sich entwickelnde Bedrohungen



3. Zugang zu Ressourcen mit den geringsten Rechten ermöglichen



Grant the right level of network access to users and devices

Network authentication and authorization



Classify and segment users, devices and apps on your network

Network segmentation



Contain infected endpoints and revoke network access
By

Continuously monitoring and responding to threats

3. Zugang zu Ressourcen mit den geringsten Rechten ermöglichen

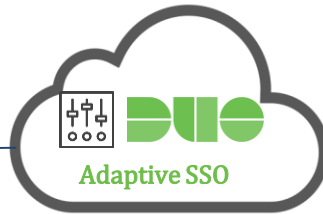
Device Health Checks

- 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

Solution:

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



Enforce Trust-Based Access

Solution:

Durchsetzung von Zugriffsrichtlinien für jede Anwendung mit adaptiven und rollenbasierten Zugriffskontrollen



Continuously Verify Trust

Solution:

Kontinuierliche Überwachung risikobehafteter Geräte mit Endpoint Health & Management Status

WHY Cisco??





**Integration statt
Einzelbetrachtung**



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

Security Operations

XDR

Managed Detection and Response Services

Threat Visibility & Hunting

Security, Orchestration, Automation and Response

Asset Inventory

Vulnerability Mgmt

Incident Response and Remediation Services

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

PRIVATE CLOUD EDGE (MSP or CUSTOMER)

Reliable | Scalable | Flexible | Visibility

SDWAN

SDWAN | Firewall | VisibilityCloud | DDoS

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

On-Premises

SASE/SDWAN

Scalable | Flexible | Visibility | Comprehensive Security

Network Edge

SDWAN | Firewall | Visibility

ZERO TRUST

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

Logging | DDoS protection | Flow Analytics | Firewall | Identity | Segmentation | Web Security

IoT/OT SECURITY

Secure Critical Infrastructure | Unified IT and OT

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

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



SECURE