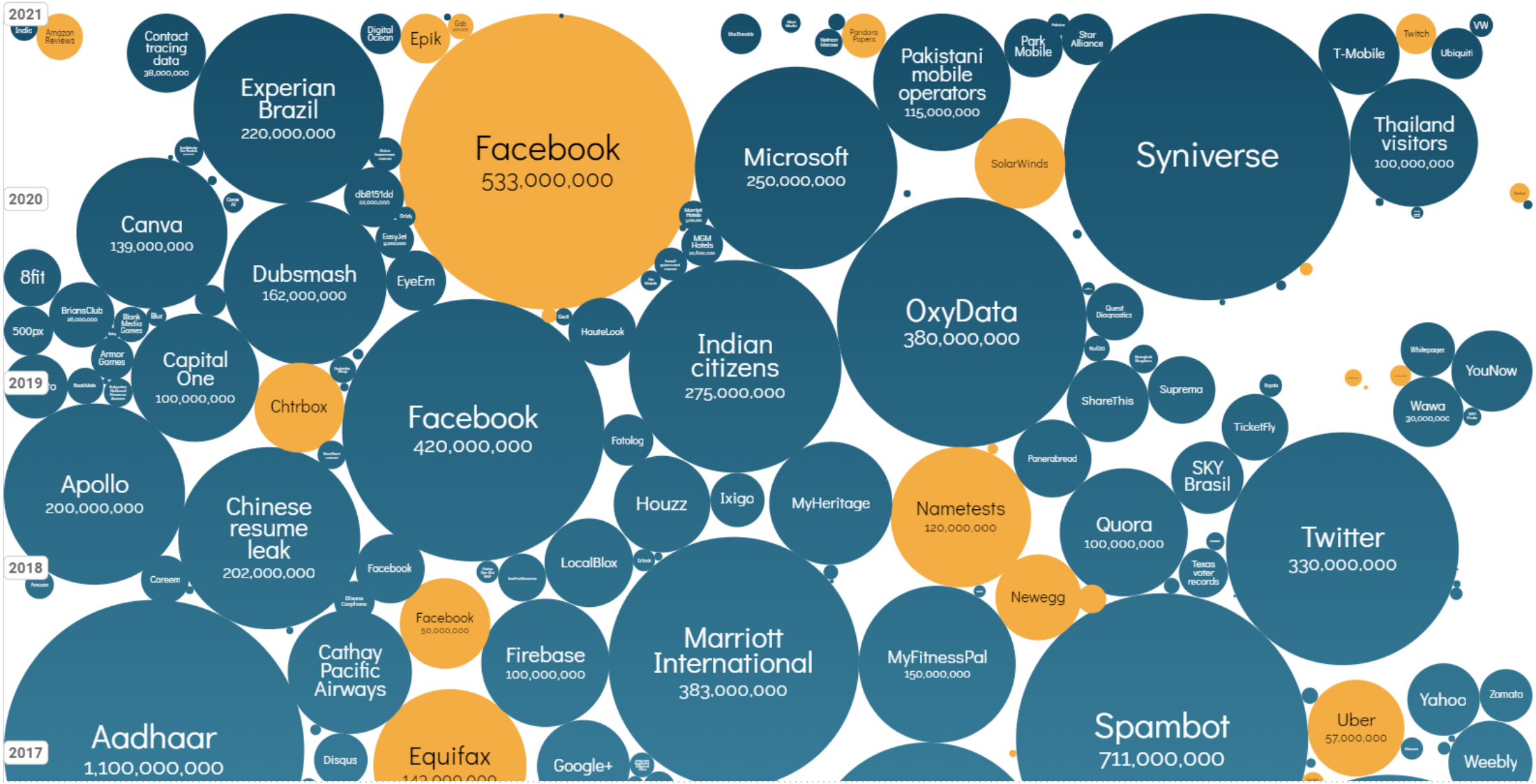
items

HYBRID WORK

NEW SECURITY DEMANDS FOR MODERN ENVIRONMENTS

WORLD'S BIGGEST DATA BREACHES & HACKS

items



Quelle: World's Biggest Data Breaches & Hacks — Information is Beautiful

BSI

Die Lage der IT-Sicherheit in Deutschland 2021

RANSOMWARE/DDOS

Deutliche Ausweitung cyber-krimineller Erpressungsmethoden

Neuer Trend

+ 360 % Daten-Leak-Seiten

Schweigegeld-Erpressung

Lösegeld-Erpressung

Schutzgeld-Erpressung

13 Tage lang konnte ein Universitätsklinikum nach einem *Ransomware*-Angriff keine Notfall-Patienten aufnehmen.

144 MIO. neue Schadprogramm-Varianten

+22 % gegenüber 2020: 117,4 MIO.

DURCHSCHNITTLICH **394.000** neue Schadprogramm-Varianten pro Tag

2020: 322.000

IM HÖCHSTWERT **553.000**

2020: 470.000

DOPPELT SO VIELE

***BOT*-INFEKTIONEN DEUTSCHER SYSTEME**

pro Tag im Tagesspitzenwert

20.000 > 40.000

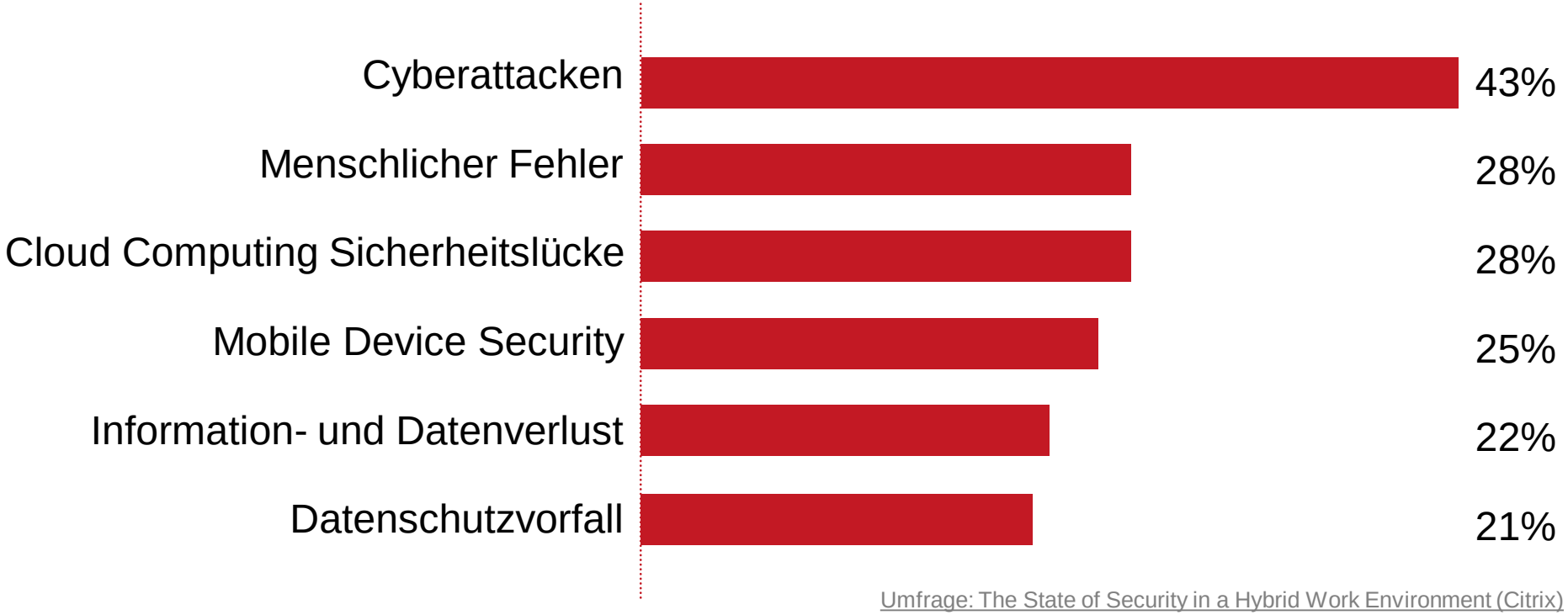
98 %

aller geprüften Systeme waren durch Schwachstellen in **MS Exchange** verwundbar.

Quelle: Die Lage der IT-Sicherheit in Deutschland 2021 (bund.de)

TOP BEDROHUNGEN

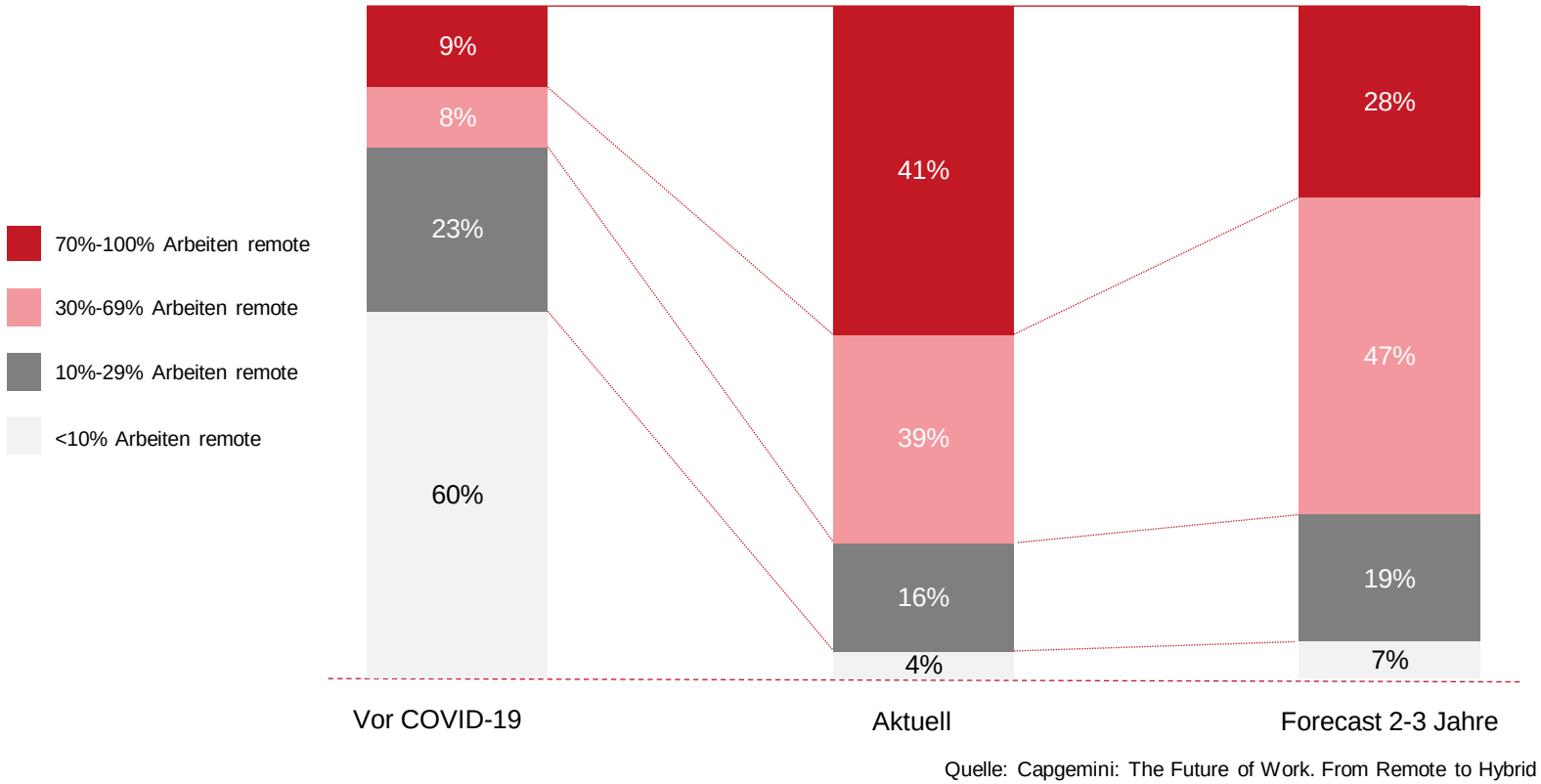
BEIM SCHUTZ VON HYBRID-, REMOTE- ODER HOMEOFFICE-MITARBEITERN



Umfrage: The State of Security in a Hybrid Work Environment (Citrix)

HYBRID WORK

REMOTE WORK IS HERE TO STAY



Quelle: Capgemini: The Future of Work. From Remote to Hybrid

Die Pandemie sorgte für eine Beschleunigung der Digitalisierung

Remote Work wurde innerhalb kürzester Zeit die neue Normalität

Schnelles Onboarding in Cloud-Szenarien unterstützen die Transformation

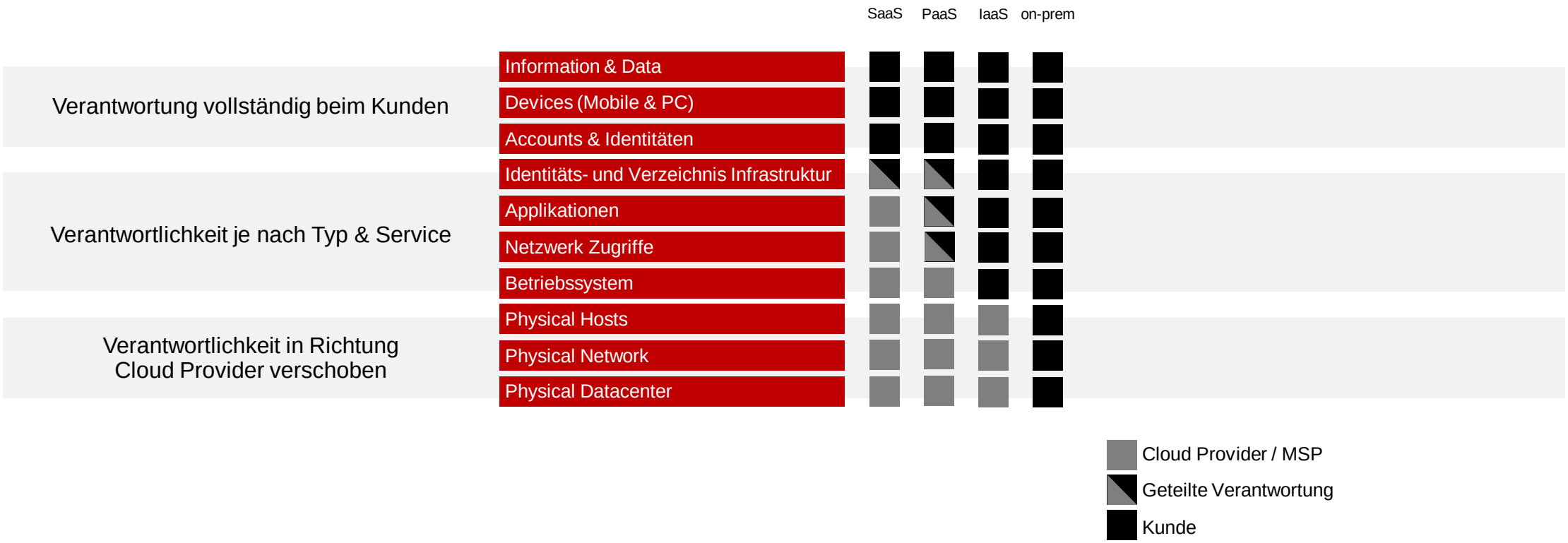
HYBRID WORK

ALTE WELT VS. NEUE WELT

Benutzer sind Mitarbeiter	>	Mitarbeiter, Partner, Kunden, Dienstleister, Bots
Managed Devices	>	Bring your own, IoT & Partner Devices
On-premises Apps	>	Explosion von Cloud Apps und Services
Trusted Networks	>	Remote Work, Partner & Public Networks
Büro und Kernarbeitszeiten	>	Arbeiten von überall, zu jeder Zeit
Zusammenarbeit vor Ort	>	Hybride Zusammenarbeit mittels Cloud-basierender Kollaboration-Tools

SHARED RESPONSIBILITY MODEL

MIGRATION IN DIE CLOUD – WER IST VERANTWORTLICH?



TRADITIONELLES SECURITY MODELL

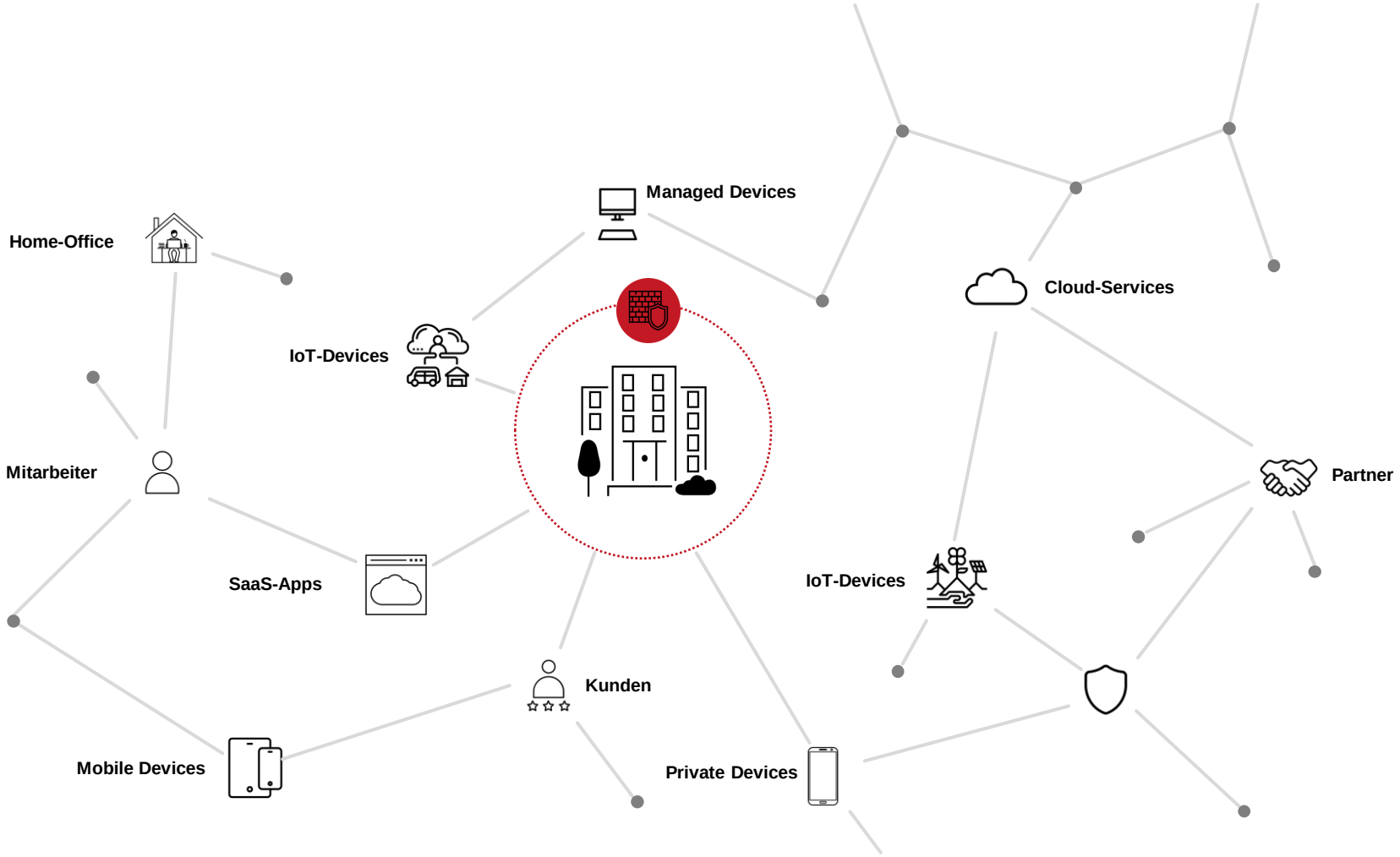
FOKUS AUF DEN NETWORK PERIMETER

Benutzer, Geräte, Apps und
Daten hinter einer Firewall / DMZ

- Schutz der on premises Infrastruktur vor dem Zugriff von außen
- Netzwerktrennungen innerhalb des Perimeters als Bedrohungsschutz
- Benutzer, Geräte, Apps & Daten innerhalb des Perimeters gelten als vertrauenswürdig und sicher

HEUTIGE HERAUSFORDERUNGEN

NETWORK PERIMETER NUR EIN TEIL DER STRATEGIE



ZERO TRUST

NEVER TRUST, ALWAYS VERIFY

Expliziter Zugriff

Hinzunahme von allen verfügbaren Datenpunkten und Signale zur Sicherstellung der Authentifizierung und Autorisierung.

Identitäten, Gerätestatus, Standort, Anomalien, Verhalten, Datenklassifizierungen

Geringste Berechtigungen

Zugriff auf Daten und Systeme auf geringste Berechtigungen reduzieren und nur dann, wenn er für den Moment benötigt wird.

Just-in-Time & Just-Enough-Access

Von Kompromittierung ausgehen

Ausbreitung vermeiden und Ausmaß reduzieren.

Segmentierung des Zugriffs über Netzwerk, Benutzer, Geräte und Applikationen.

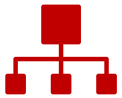
Ende zu Ende-Verschlüsselung und Erhöhung der Sichtbarkeit mittels Analyse und Erkennen von Bedrohungen.

Identity

Devices

Apps

Infrastructure

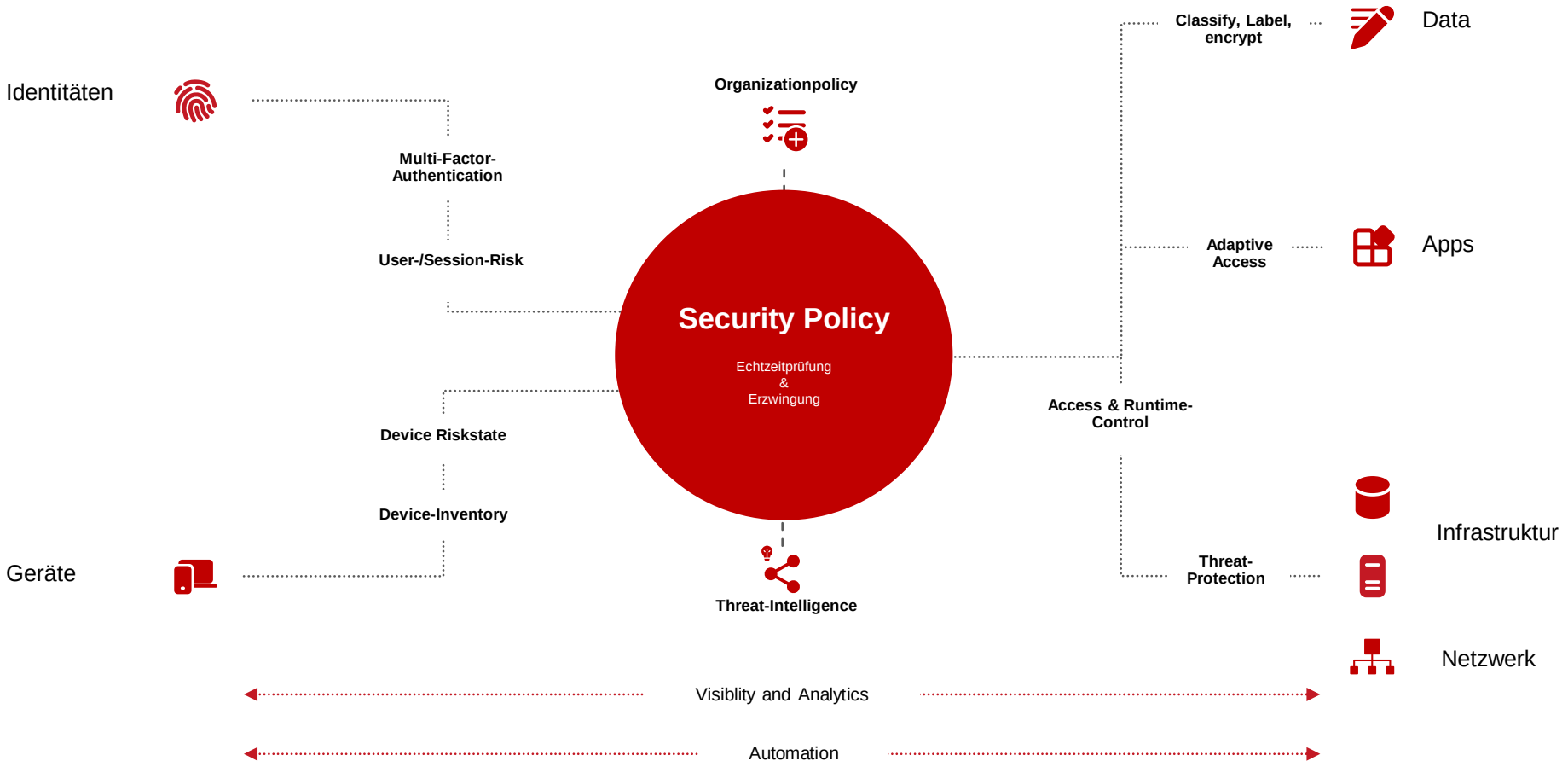


Network

Data

ZERO TRUST

NEVER TRUST, ALWAYS VERIFY



TOP SICHERHEITSMAßNAHMEN

UM REMOTE- UND HYBRID-ARBEITSKRÄFTE ZU SCHÜTZEN

Umfrage: The State of Security in a Hybrid Work Environment (Citrix)

IT-SICHERHEIT: NICHT NUR EINE FRAGE DER TECHNIK

SONDERN INSBESONDERE EINE FRAGE DER ORGANISATORISCHEN PROZESSE

Informationssicherheits-Managementsystem

Plan ⟶ Do ⟶ Check ⟶ Act

Security Prozesse & Richtlinien

Sensibilisierung und Training der Endanwender

E-Learning, Enduser Attack Simulation Training

Menschen

Umsetzung von Zero Trust

Expliziter Zugriff, geringste Berechtigungen, Analyse und Verschlüsselung

Zero Trust

VIELEN DANK

www.itemsnet.de @items_GmbH