



Security Service Edge (SSE) Critical Capabilities:

Die Cloud schützen, wenn Schatten-IT zur Norm wird





AIRBUS

205M+
Mobil-
geräte

Schneider
Electric

170M+
Mobile
Apps

Allianz 

16.5k+
SaaS
Apps

Henkel

1,600+
Threats
Families

- Gegründet 2007 mit Fokus auf mobiler Sicherheit
- 2021 Erweiterung um den Schutz von Cloud-Daten in einer integrierten Plattform; Übernahme von Cipher Cloud
- Globale Präsenz mit weltweitem Vertrieb und Support

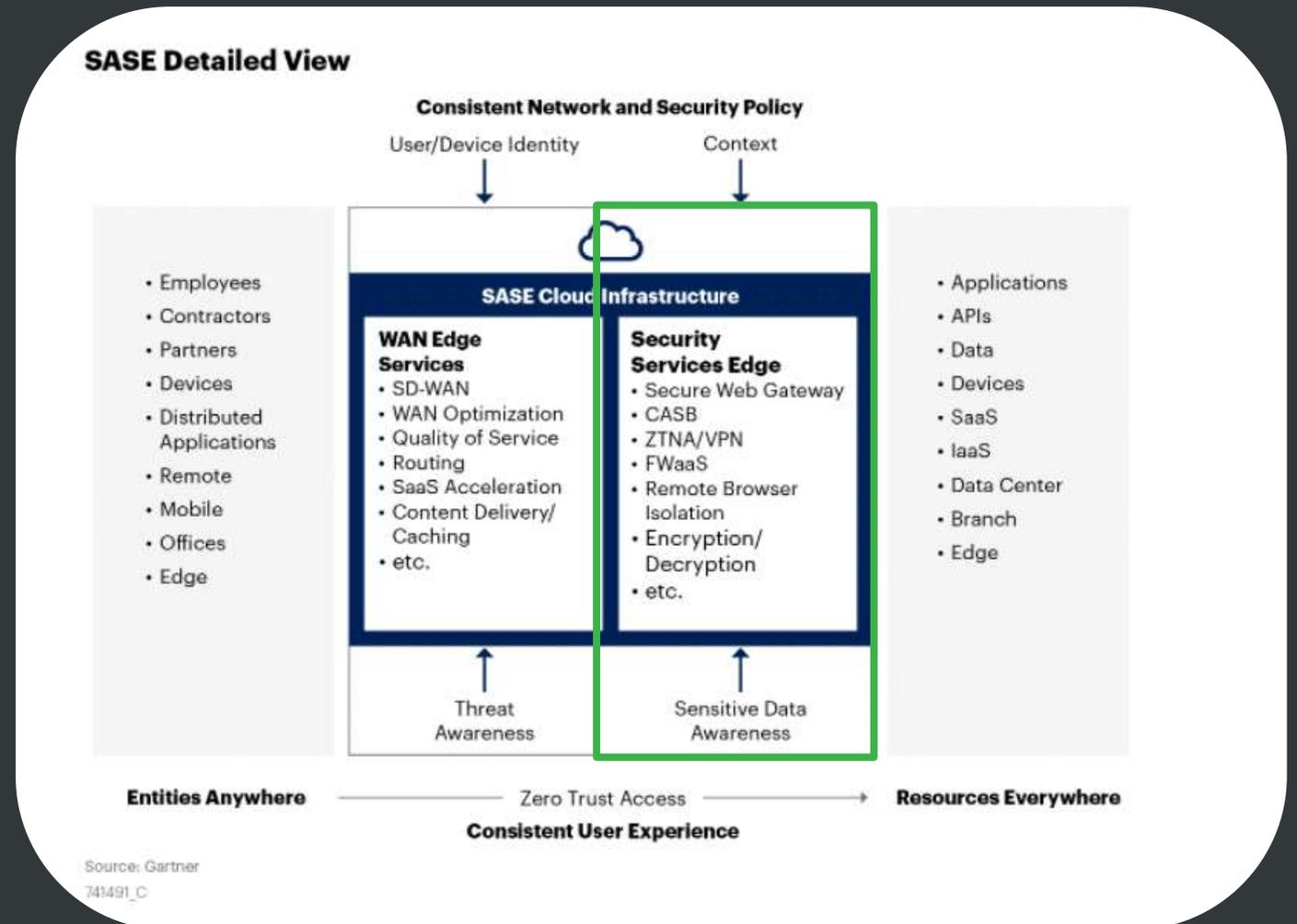
- Weltweit über 500.000 Unternehmen gesichert
- Betreuung in allen wichtigen internationalen Märkten

Security Service Edge (SSE): Die Sicherheitselemente des SASE-Frameworks

SSE sichert den Zugang zum Web, zu Cloud-Diensten und privaten Anwendungen.

Die Fähigkeiten umfassen:

- Zugriffskontrolle
- Bedrohungsschutz
- Datensicherheit
- Sicherheitsüberwachung
- Akzeptable Nutzungskontrolle



Neue Arbeitsmodelle erfordern neue Ansätze

Hybride Arbeitsmodelle sind die Norm



Befähigung & Sicherheit hybrider
Mitarbeiter für eine bessere
Endbenutzererfahrung

Apps und Daten liegen in der Cloud



Modernisierung der IT-
Sicherheitsinfrastruktur, die
granulare Kontrolle und
betriebliche Effizienz bietet

Moderne Bedrohungen entwickeln sich weiter



Erkennen & Minimieren von Cyber-
Bedrohungen, um unberechtigten
Zugriff und Datenverletzungen zu
verhindern

Cloud-Sicherheitsrisiken, vor denen sich Unternehmen schützen müssen



**RANSOMWARE
ATTACKS**



**DATA LEAKAGE VIA
COLLABORATION**



INSIDER THREATS



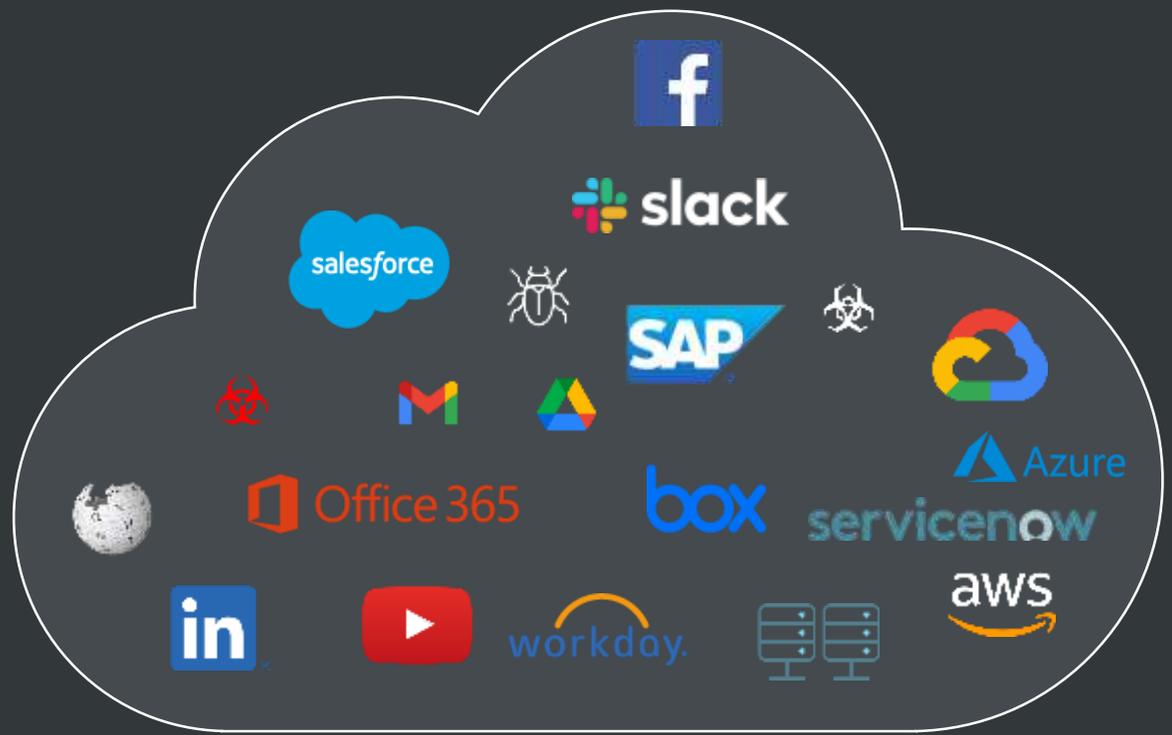
**COMPROMISED
ACCOUNTS**



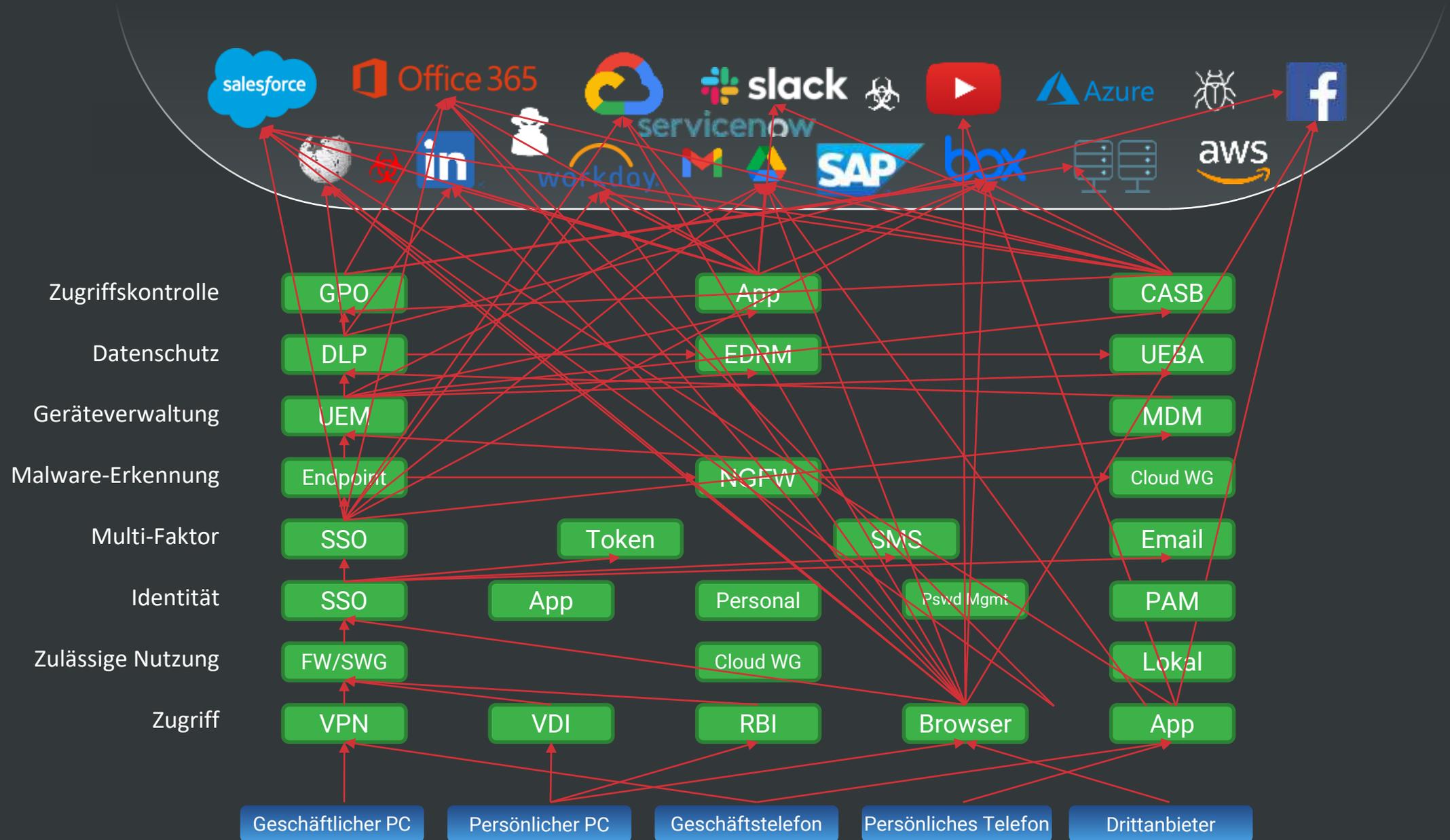
**COMPROMISED
DEVICES**

Über alle Benutzer - Geräte - Aktivitäten - Daten hinweg

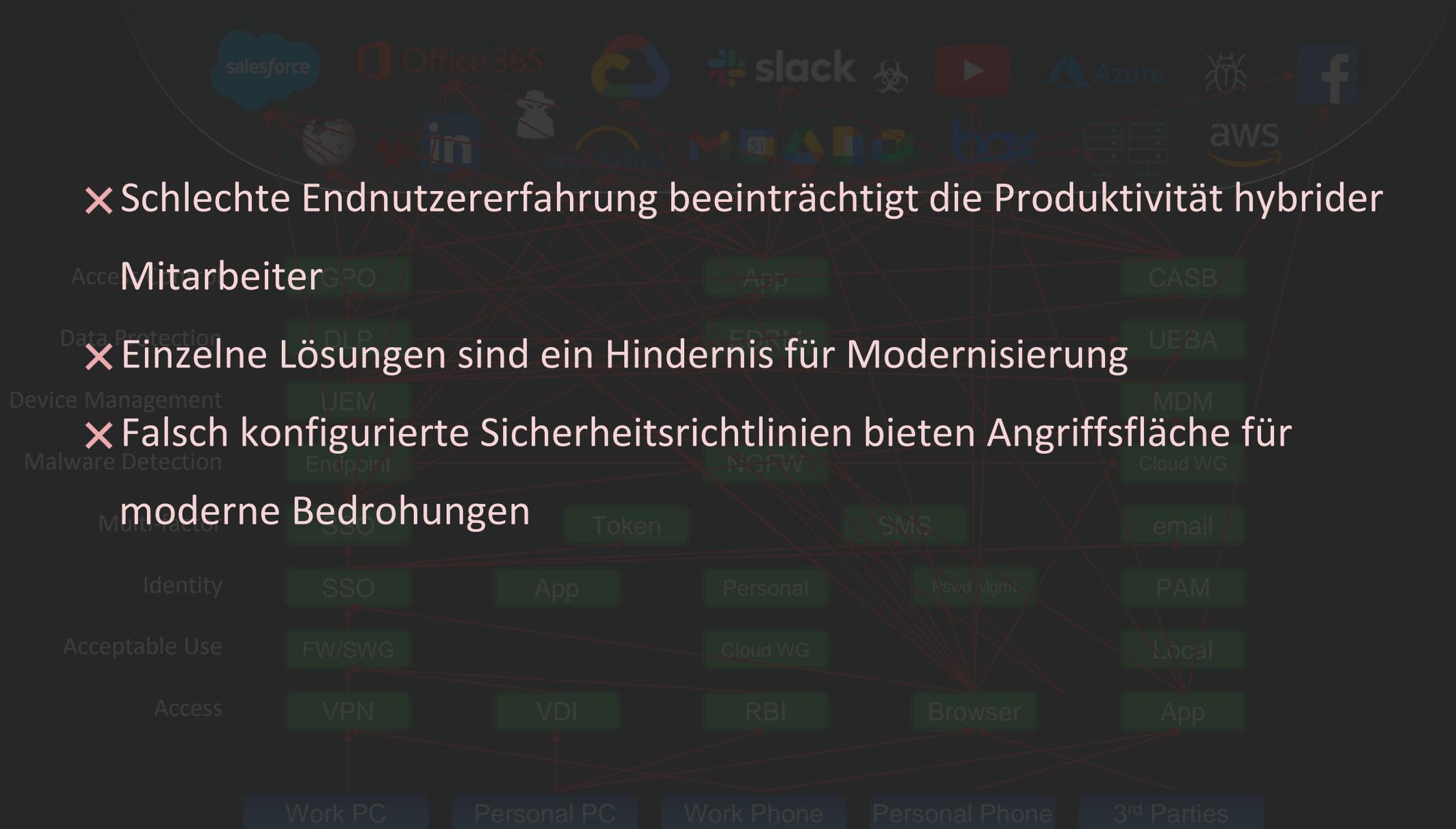
sowie alle Anwendungen - SaaS, Privat, E-Mail und Web



Einzelne Produkte führen zu Verwaltungschaos, Sicherheitslücken und mangelhafter Benutzerfreundlichkeit



Existing chaos results in security gaps, poor user experience



✗ Schlechte Endnutzenerfahrung beeinträchtigt die Produktivität hybrider

Mitarbeiter

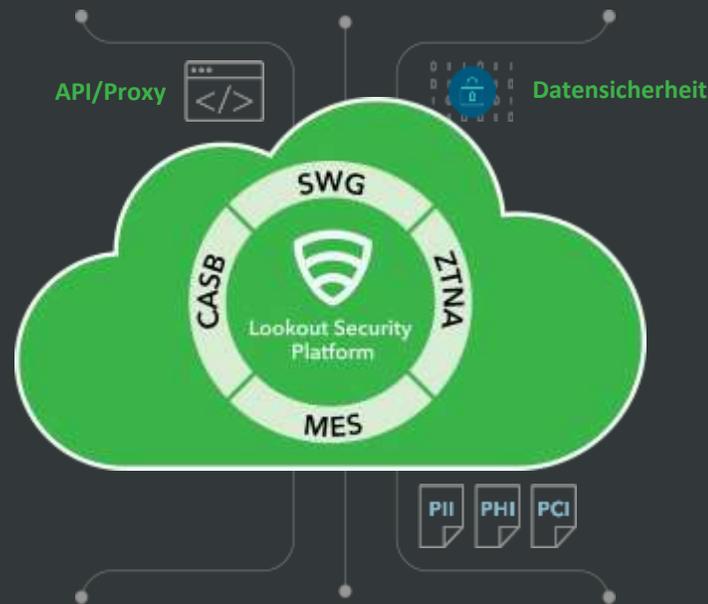
✗ Einzelne Lösungen sind ein Hindernis für Modernisierung

✗ Falsch konfigurierte Sicherheitsrichtlinien bieten Angriffsfläche für
moderne Bedrohungen

Integrierter Ansatz für Sicherheit in der Cloud



- Single-Proxy-Architektur für optimales Endbenutzererlebnis und vereinfachte Verwaltung
- Sicherheitseffizienz mit intelligenten und kontextabhängigen Richtlinien
- Schutz von Investitionen durch ein umfassendes Ökosystem
- Durchgängige Überwachung & Transparenz für alle Anwendungen und Daten



Geschäftlicher PC

Persönlicher PC

Geschäftstelefon

Persönliches Telefon

Drittanbieter

PII PHI PCI



Treffen Sie uns auf einen Drink an
Stand 7-518, um über Cloud-Sicherheit
zu sprechen

