



Case Study:

Baukonzern schützt Daten vor internen & externen Bedrohungen





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

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

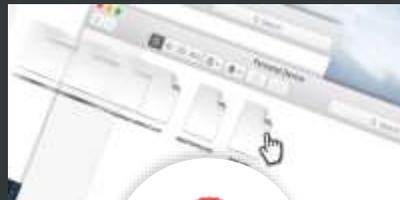
Cloud-Sicherheitsrisiken, vor denen sich Unternehmen schützen müssen



**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

Zum Kunden

- Bauunternehmen mit 4,000+ Mitarbeitern & 1,000+ Auftragnehmer bundesweit
- Lokale, papierbasierte Arbeitsabläufe wurden durch digitale Lösungen ersetzt

Herausforderungen

- Nutzung nicht genehmigter IT-Anwendungen
- Schutz sensibler Dokumente, die auf ein nicht verwaltetes Partner- oder BYOD-Gerät heruntergeladen werden
- Schutz vor Viren oder Malware in der Cloud

Ziel:

**Effizienz der Cybersicherheit steigern
und Unternehmensrisiken reduzieren**

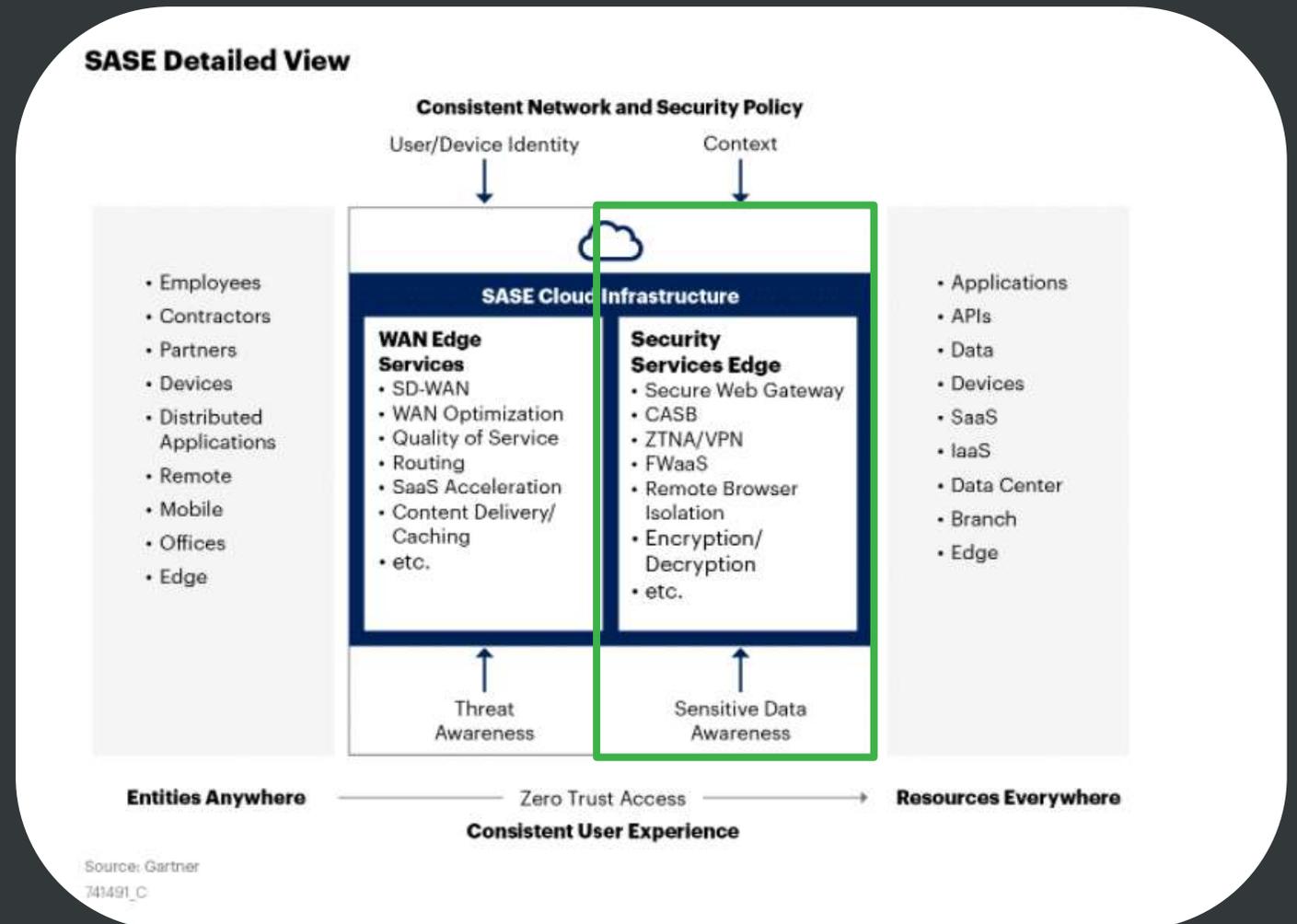


Security Service Edge (SSE): Die Sicherheitselemente des SASE-Frameworks

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

Die Fähigkeiten umfassen:

- Zugriffskontrolle
- Bedrohungsschutz
- Datensicherheit
- Sicherheitsüberwachung
- Akzeptable Nutzungskontrolle



Die Lösung zur Effizienzsteigerung der Cybersicherheit und Reduzierung von Unternehmensrisiken

- ✓ **Durchsetzung von DLP-Richtlinien:** Blockieren, einschränken oder erlauben des Zugriffs auf Daten in Google Drive und Box.
- ✓ **EDRM-Anzeigen bieten ein Höchstmaß an Schutz:** Durch Dateiverschlüsselung und die Durchsetzung von Zugriffsrichtlinien können Partner Informationen sicher erstellen, anzeigen und ändern und sie gleichzeitig vor unbefugtem Zugriff, unbefugter Nutzung und Verbreitung schützen.
- ✓ **Tracking von sanktionierten und nicht sanktionierten Apps:** Entdeckung, Verwaltung und Durchsetzung von Schatten-IT-Anwendungen durch Tracking von 16.000 Anwendungen in der Knowledge Base.
- ✓ **Mit AVAM Bedrohungen abwehren:** Das Hochladen infizierter Dateien blockieren und verdächtige Dateien zur weiteren Untersuchung durch das interne Sicherheitsteam unter Quarantäne stellen.

Mit Lookout weiter auf dem Weg in die Cloud

Nachdem **drei der kritischsten SaaS-Anwendungen** angemessen **abgesichert** sind, ist das IT-Team bereit, die Plattform auf andere Komponenten auszuweiten. Dank des **einheitlichen Plattformansatzes** von Lookout können sie **bestehende Datenschutzrichtlinien auf neue Anwendungen übertragen**.



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

