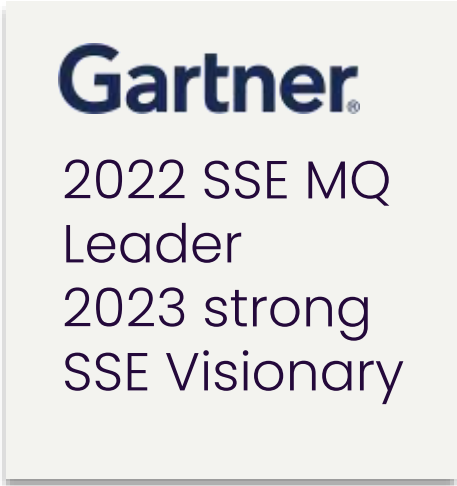
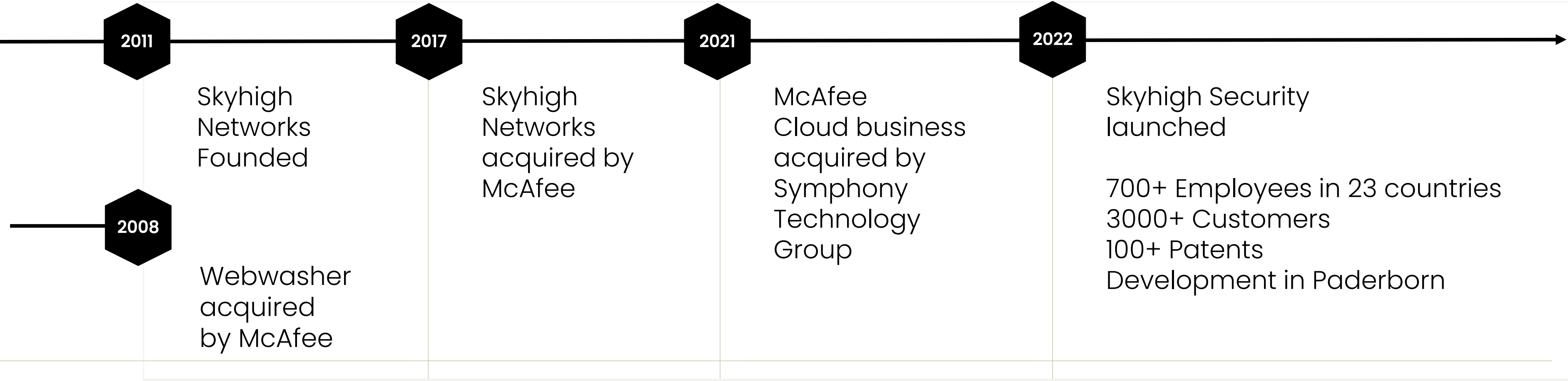


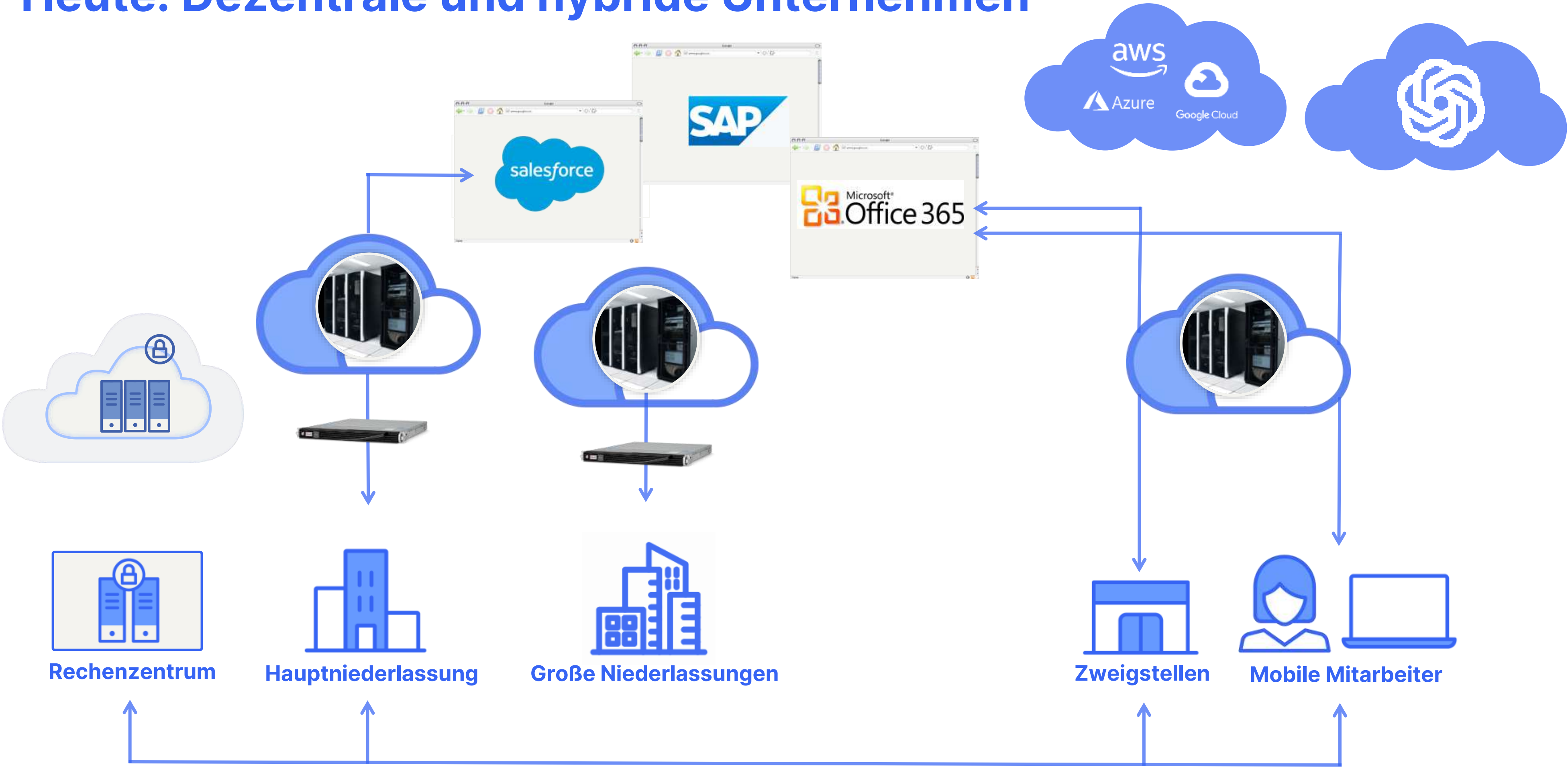
Der Schutz sensibler Daten in Zeiten der hybriden Arbeitswelt, Cloudnutzung und KI

Thomas Wethmar, Regional Director DACH

Skyhigh Security at a Glance



Heute: Dezentrale und hybride Unternehmen



Shadow IT, AI und Data Security (on prem und in der Cloud) im Kontext einer Security Service Edge Plattform



Secure Web Gateway + Cloud Access Security Broker + Zero Trust Network Access

Sicherer Zugriff auf
das Web, Cloud
Services und
private
Applikationen

Erweiterter Schutz
und Visibilität der
Daten in
sanktionierten
Anwendungen

Identifizieren und
Schutz von Data
in use, in motion,
und at rest

Schutz vor Malware
und Erkennen von
kompromittierten
Accounts und
Angriffen von innen

Ermöglicht
eine hybride
Workforce

Umsetzen von Zero-
Trust-Prinzipien

Skyhigh Security Service Edge (SSE) Portfolio



SWG

Skyhigh Secure Web Gateway

Skyhigh Cloud Firewall (FWaaS)

CASB

Skyhigh Cloud Access Security Broker

ZTNA

Skyhigh Private Access

CNAPP

Skyhigh Cloud-Native Application Protection Platform



Skyhigh Cloud Platform

Intuitive Dashboard · Advanced Data Loss Prevention · Unified Policy Management · Unified Threat Prevention

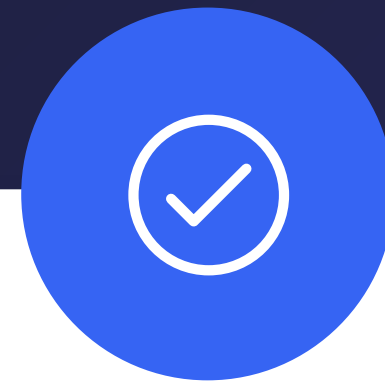
Die Herausforderung: Immer mehr Daten bewegen sich in der Cloud



**Immer mehr sensitive Daten
liegen in der Cloud**

61 %

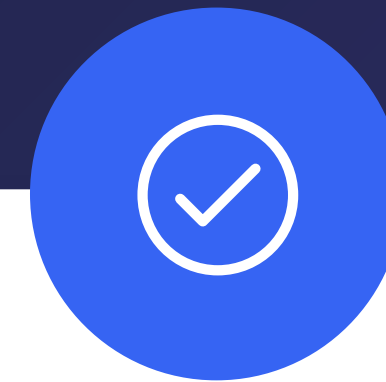
der Befragten berichten,
dass sensitive Daten in der Cloud
liegen (48 % in 2019)¹



**Shadow IT hat Einfluss auf
Datensicherheit**

75 %

der Befragten berichten,
dass Shadow IT die
Datensicherheit beeinträchtigt.
(50 % in 2019)



Datenverlust in der Cloud

80 %

der befragten Unternehmen und
Organisationen sind schon
von ungewolltem Datenabfluss in
der Cloud betroffen gewesen

1. Skyhigh Security "The Data Dilemma: Cloud Adoption and Risk Report", 2023. 2. Ibid. 3. Ibid.

Trends



Daten

Der Schutz der Daten genießt höchste Priorität – besonders in regulierten Industriezweigen.

Plattform

Einheitlicher Schutz von Daten über die Cloud, das Web, Applikationen und eigene Ressourcen (einschließlich ZTNA) wird immer bedeutender.

Konsolidierung spart Kosten und erhöht die Visibilität.

Hybrid

Flexibilität ist wichtig bei dem Weg in die Cloud – nicht jeder Kunde möchte einen harten Schnitt, sondern das Tempo selbst bestimmen.

KI

Die Fragestellung, wie mit der Nutzung von KI-Diensten umgegangen wird, gewinnt eine immer größere Bedeutung.

Datenschutz und Compliance als Herausforderung

Geistiges Eigentum / IP

SEC Form 10-K

DSGVO / GDPR

BaFin

PCI / DSS

CCPA / CPRA

Patientendaten

Personenbezogene Daten / PII

Gartner® Predictions for the Future of Generative AI Use



40 %

2024 werden 40 % der Unternehmens-Applikationen integrierte Konversations-AI haben, Anstieg von 5 % in 2020.

30 %

2025 werden 30 % der Unternehmen eine AI-unterstützte Entwicklungs- und Test-Strategie implementiert haben, Anstieg von 5 % in 2021.

60 %

2026 werden generative Design-AIs 60 % der Design-Anforderungen für neue Webseiten und mobile Applikationen automatisieren.

Skyhigh Use Cases for Generative AI



1

Granulare Visibilität

- Identifizieren Sie, ob und welche AI-Apps von den Mitarbeitern genutzt werden.
- Erlangen Sie einen Überblick über die Risiko-Einstufungen von AI-Apps und der übertragenen Datenmenge
- Identifizieren Sie, welche Mitarbeiter welche AI-Apps nutzen und welche Daten sie übermitteln.

2

Monitor & Control

- Entscheiden Sie, welche AI-Apps erlaubt sind
- Entscheiden Sie, was User übermitteln dürfen.

3

Schutz von unternehmens- kritischen Daten

- Verhindern Sie Datenverlust durch die Einführung erweiterter DLP-Policies um AI-Applikationen zu sanktionieren.
- Deaktivieren der Konversations-Historie und Limitierung von Daten-Uploads
- Coaching und Schulung von Mitarbeitern über die Nutzung von AI-Applikationen

Shadow IT, AI und Data Security (on prem und in der Cloud) im Kontext einer Security Service Edge Plattform



Secure Web Gateway + Cloud Access Security Broker + Zero Trust Network Access

Sicherer Zugriff auf
das Web, Cloud
Services und
private
Applikationen

Erweiterter Schutz
und Visibilität der
Daten in
sanktionierten
Anwendungen

Identifizieren und
Schutz von Data
in use, in motion,
und at rest

Schutz vor Malware
und Erkennen von
kompromittierten
Accounts und
Angriffen von innen

Ermöglicht
eine hybride
Workforce

Umsetzen von Zero-
Trust-Prinzipien

Skyhigh Security Service Edge (SSE) Portfolio



SWG



Skyhigh Secure Web Gateway



Skyhigh Cloud Firewall (FWaaS)

CASB



Skyhigh Cloud Access Security Broker

ZTNA



Skyhigh Private Access

CNAPP



Skyhigh Cloud-Native Application Protection Platform



Skyhigh Cloud Platform

Intuitive Dashboard · Advanced Data Loss Prevention · Unified Policy Management · Unified Threat Prevention



Halle 7, Stand 7-152

Sie möchten mehr erfahren?

Besuchen Sie uns!

Thomas Wethmar, Regional Director DACH