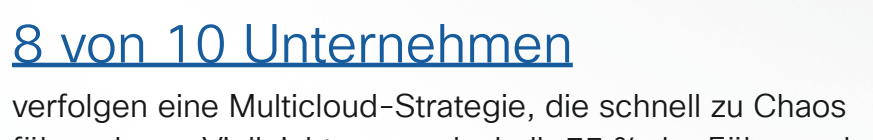


# Benutzeranforderungen in einer hybriden Multicloud-Welt erfüllen

Moderne Arbeitsweisen erschweren die Cybersicherheit. Hier einige Tipps für eine verbesserte Security Resilience in der Multicloud.

## Unsere Arbeitswelt verändert sich rasant. Kann die Sicherheit mithalten?



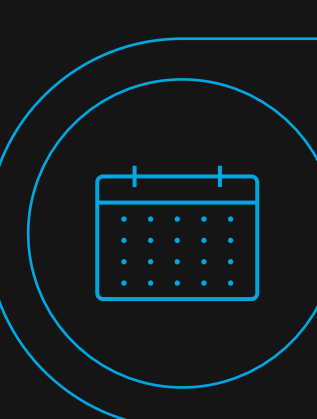
### 8 von 10 Unternehmen

verfolgen eine Multicloud-Strategie, die schnell zu Chaos führen kann. Vielleicht sagen deshalb 75 % der Führungskräfte, dass ihr Unternehmen inzwischen **zu komplex ist, um echte Sicherheit zu gewährleisten**.

Hybride Arbeit gehört mittlerweile jedoch zum Standard. **Mehr als die Hälfte aller MitarbeiterInnen** möchten sich unabhängig vom Zeitpunkt, Standort und Gerät einloggen können. 85 % der CIOs möchten ihnen diese Möglichkeit geben. Aber sind sie selbst bereit für die Umstellung?

## Komplexität führt zu Sicherheitschaos

**Komplexität und Sicherheit, das passt eigentlich nicht zusammen.** Ein durchschnittliches Security-Team arbeitet mit **40 bis 50 Tools**. Der Einsatz mehrerer Cloud-Plattformen erschwert dabei die Erkennung von Bedrohungen und Schwachstellen.



### 280 Tage

Durchschnittliche Zeit bis zur Identifizierung und Eindämmung einer Sicherheitsverletzung

## Komplexe IT führt zu komplexer Sicherheit.

- Sicherheits- und Netzwerk-Silos
- Anbieterabhängigkeit
- Geringe Transparenz
- Stark beeinträchtigte User-Experience

## Angreifer wissen das – und nehmen vor allem hybride Arbeitsplätze ins Visier

**125 %** mehr Cyberangriffe im Jahr 2021 **4/5** erfolgreiche Web-App-Verletzungen sind auf gestohlene Anmeldedaten zurückzuführen

## Kennen Sie das? Chaos lässt sich schlecht verbergen.



## 4 Elemente für eine vereinfachte, einheitliche Security-Umgebung

Es bringt nichts, neuen Problemen mit alten Strategien zu begegnen. Diese neuartigen Herausforderungen erfordern ein Umdenken im Hinblick auf den Abgleich von Netzwerk und Sicherheit in Ihrem Unternehmen.

- Cloud-nativ**  
Erfüllen Sie alle Anforderungen indem Sie mit Cloud-Security alle BenutzerInnen, Netzwerke, Apps und Daten schützen.
- Einheitlich**  
Die Vereinheitlichung von Richtlinienmanagement, Produktkonsolen und Dashboards sorgt für eine effizientere End-to-End-Sicherheit.
- Reibungslos**  
Transparente, kontinuierliche Sicherheit, die im Hintergrund agiert.
- Offen**  
Umfangreiche APIs für eine umfassende Integration und ein robustes Entwicklungs-Ecosystem, damit sich die Umgebung an die Herausforderungen des Unternehmens anpassen kann.

## Die Cisco Security Cloud

Die **Cisco Security Cloud** entspricht der Vision von Cisco für End-to-End-Sicherheit in Multicloud-Umgebungen. Diese offene, einheitliche Plattform soll **Sicherheit für alle BenutzerInnen, Netzwerke und Anwendungen gewährleisten** – egal, wie komplex die Umgebung ist.



**Die Vorteile der Public Cloud nutzen – ganz ohne Nachteile**  
Anbieterabhängigkeit war gestern. Dank API-Integration, einem Ecosystem für EntwicklerInnen und einem Marktplatz bleibt die Cisco Security Cloud für alle BenutzerInnen, Netzwerke, Apps und Daten offen und kann jederzeit erweitert werden.

**Umfassende Einblicke in alle Bedrohungen und Schwachstellen**  
Wir beseitigen Silos und sorgen so über Netzwerke, Clouds, Endpunkte und Anwendungen hinweg für Transparenz und aussagekräftige Einblicke.

**Intent-Based und KI-gesteuerte Security**  
Sie können Benutzer- und Geräteidentität, Gerätestatus, Schwachstellen und mehr kontinuierlich verifizieren. Über eine einheitliche Engine können BenutzerInnen Richtlinien zentral festlegen und anwenden.

**Die Vorteile der Automatisierung**  
Im Vergleich zu manuellen Prozessen lassen sich Datensicherheitsverletzungen **74 Tage schneller** eindämmen.

**Ein reibungsloses Erlebnis für alle**  
Ermöglichen Sie effektive Sicherheitsfunktionen, die unbemerkt im Hintergrund ausgeführt werden, z. B. durch **Single Sign-On**, eine leicht zu replizierende **Microservices-basierte Architektur** zum Schutz aller Verbindungen, und mehr.

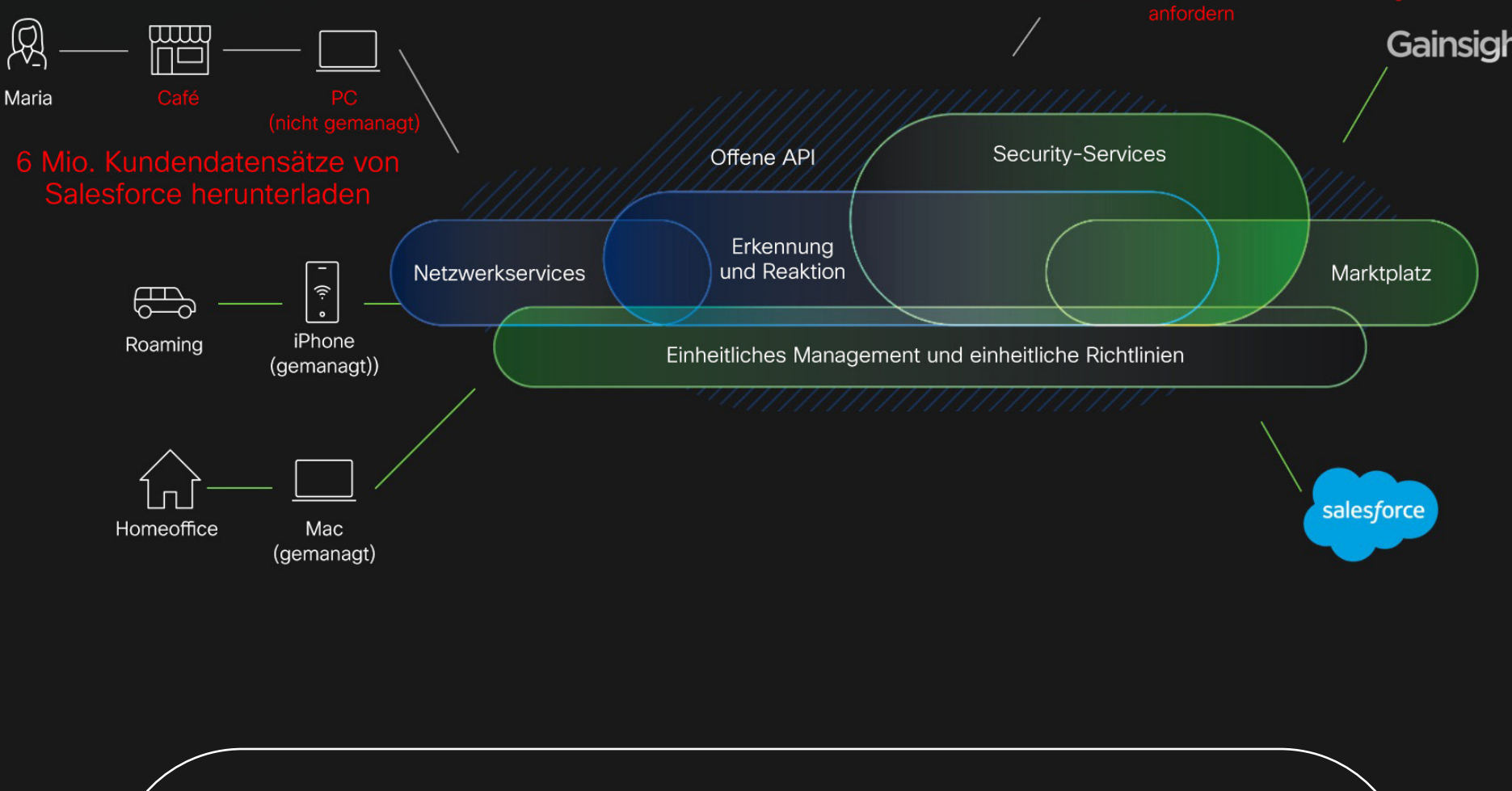
**Mehr Effizienz, mehr Vorteile**  
Sowohl SecOps, NetOps, ITOps als auch DevOps profitieren.

## Umfassender Schutz

- On-Premises**  
Monitoring- und Schutzfunktionen für Rechenzentren, Desktop-Office-Systeme sowie Laptops und mobile Geräte im Homeoffice
- In der Cloud**  
Standortunabhängige Integration aller Plattformen und Software, die Sie für das operative Geschäft brauchen
- Hybrid**  
Umfassender Schutz dank End-to-End-Abdeckung

## Sicherheit und Konnektivität im gesamten Unternehmen

Kontinuierlicher, vertrauenswürdiger Zugriff



Weitere Informationen erhalten Sie in unserem E-Book zur Cisco Security Cloud  
Sind Sie bereit für die hybride Multicloud?