secustack

Sicherheit im Cloud Computing

am Beispiel OpenStack

Gliederung

- Cloud: IaaS-Layer
- Beispiel OpenStack
- Sicherheit
- Möglichkeiten zur Absicherung
- Entwicklung anhand von Angriffsvektoren

secustack

Cloud

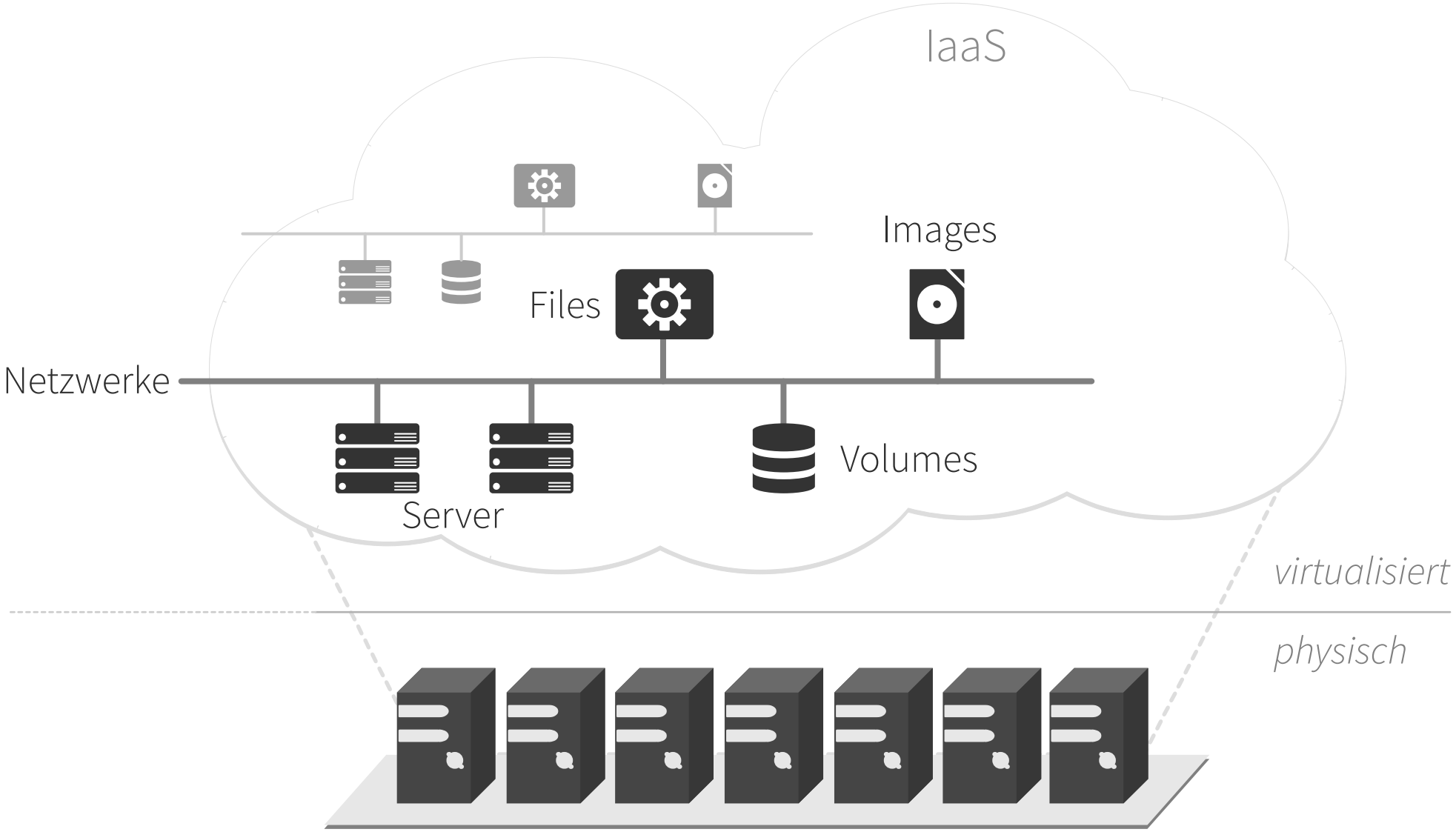
Infrastructure as a Service

Cloud

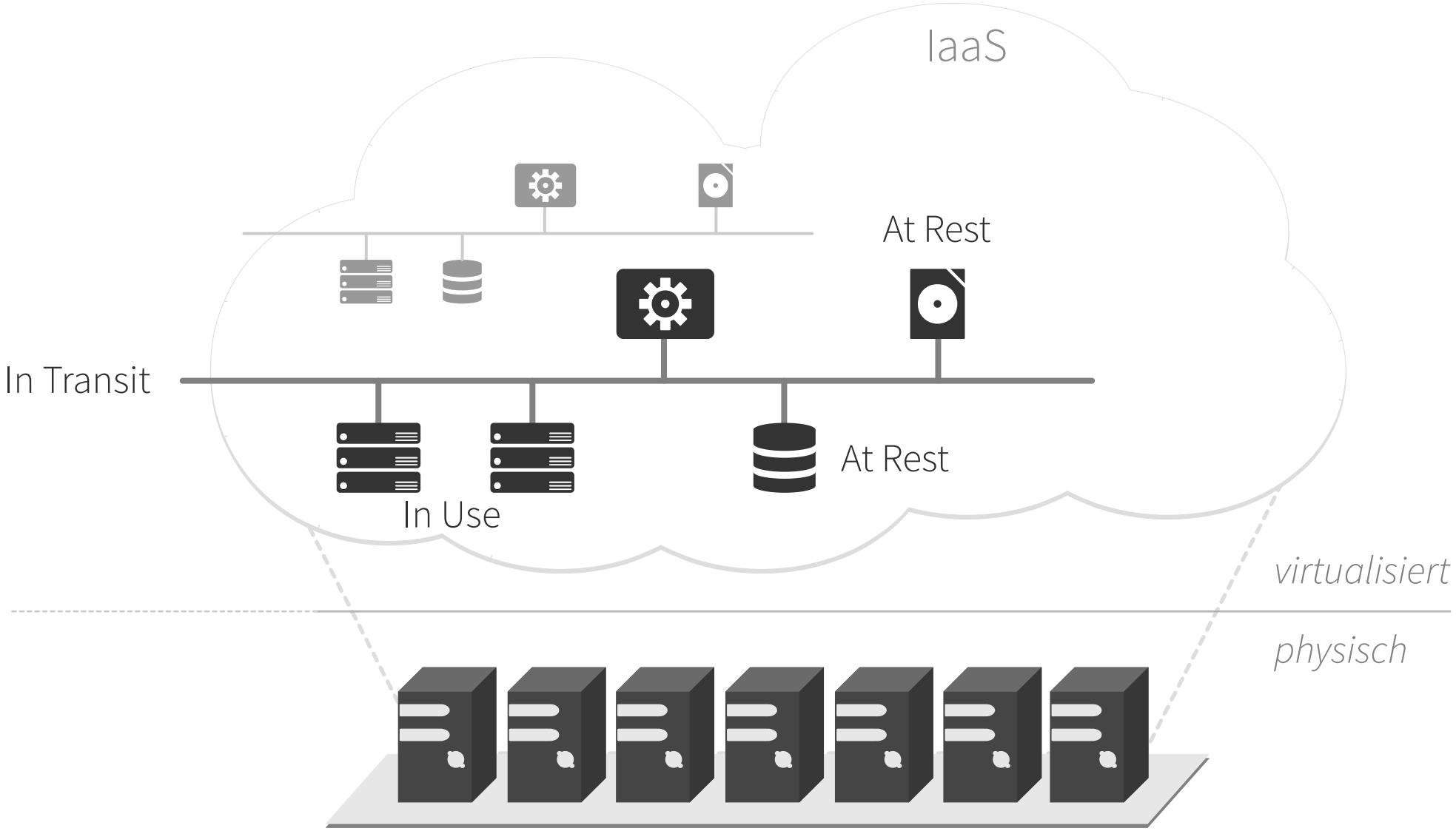
“ There is no cloud, it's just someone else's computer ”

Welche Objekte existieren im IaaS-Layer und müssen geschützt werden?

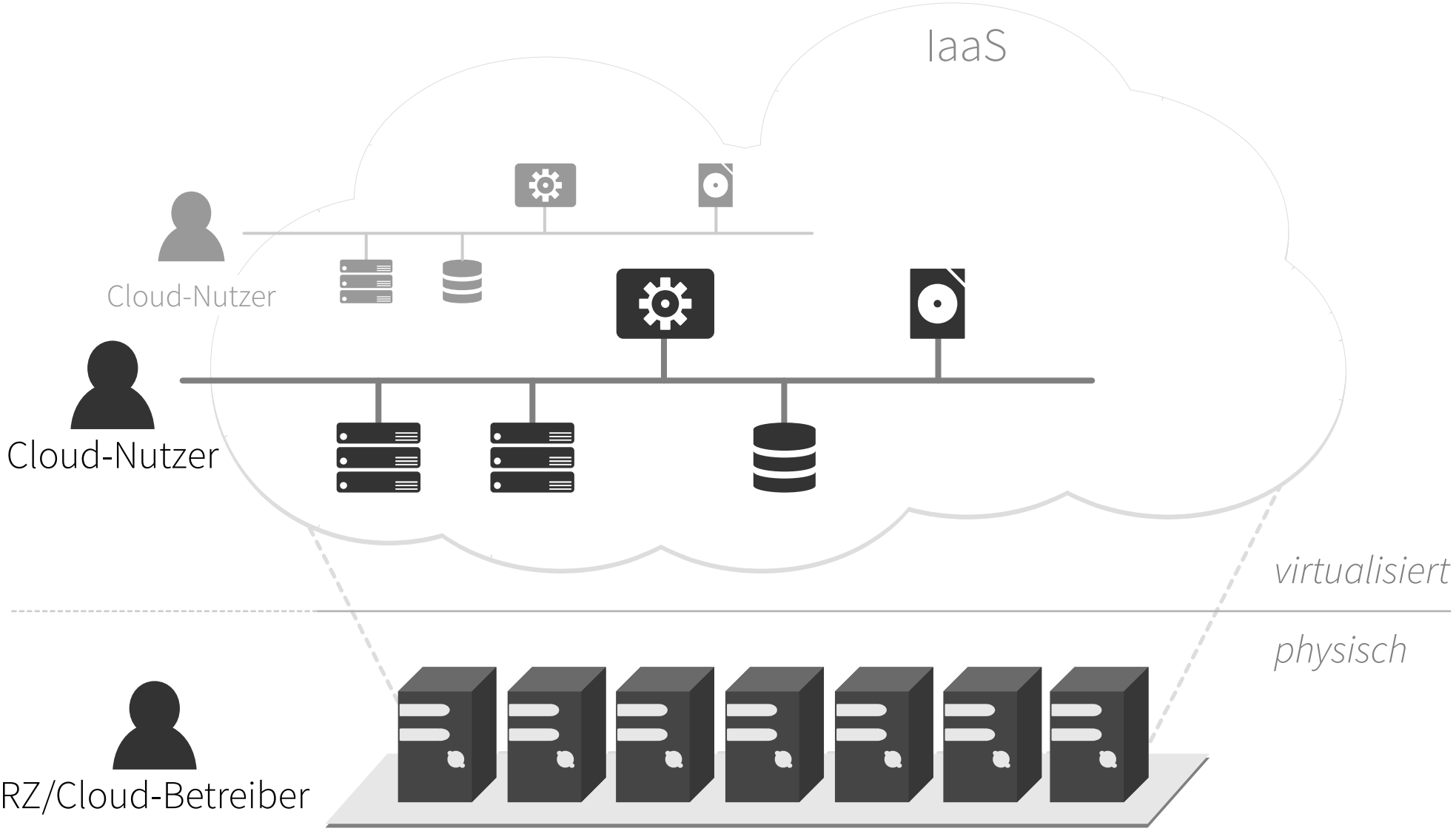
Cloud


IaaS
Images
Files
Netzwerke
Volumes
Server
virtualisiert
physisch

Welchen Zustand haben die Daten?



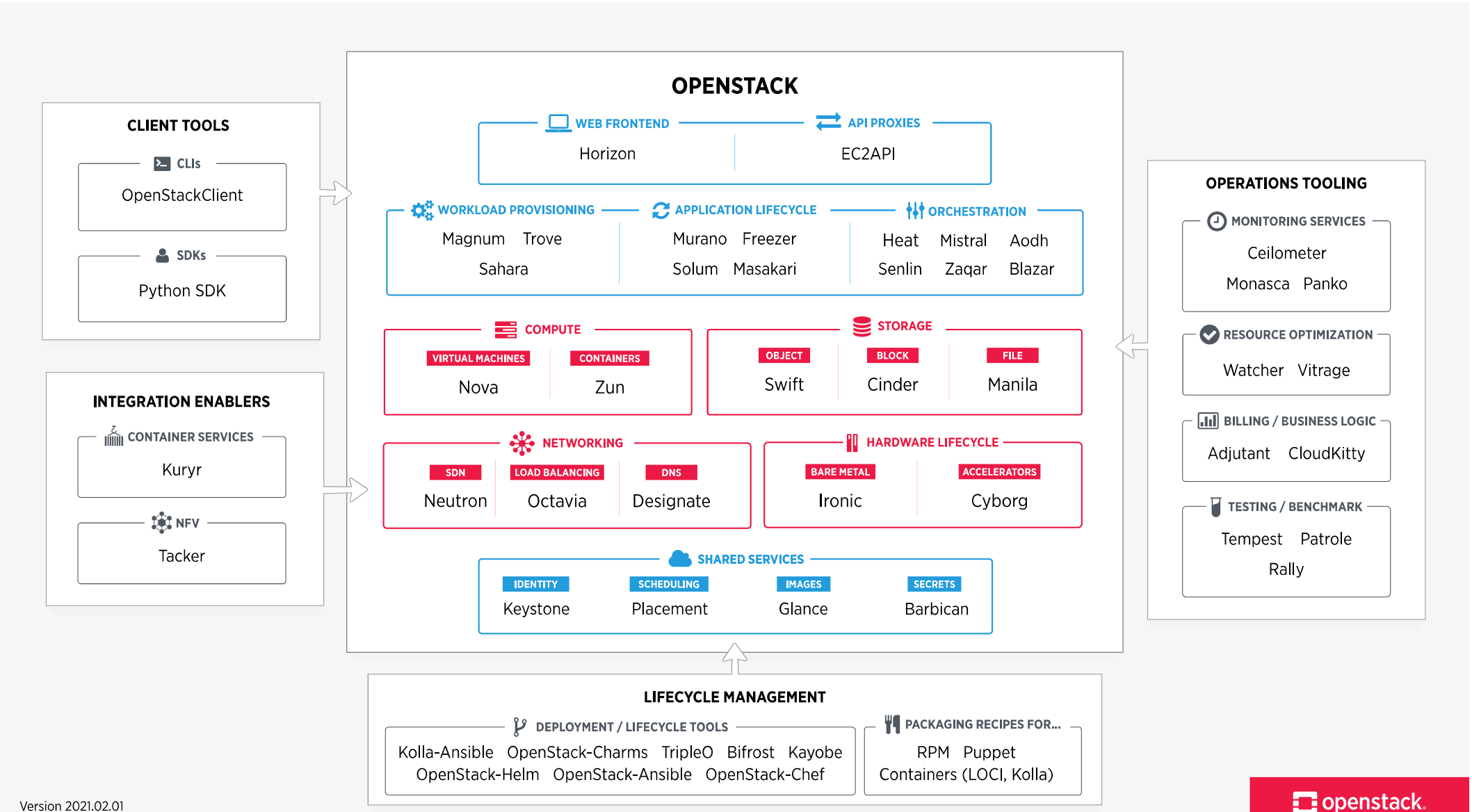
Wer interagiert mit der Cloud?



secustack

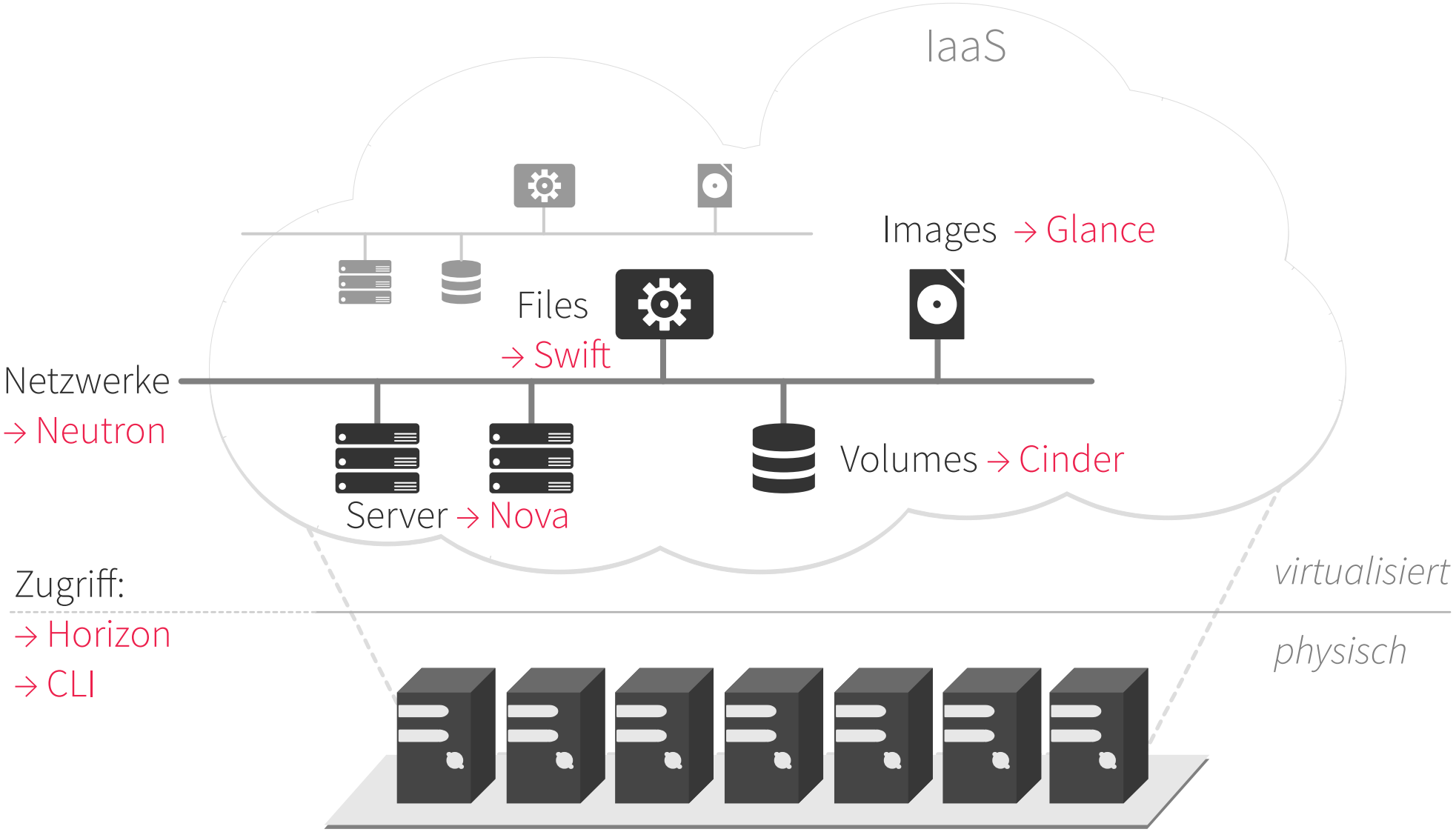
Beispiel OpenStack

Beispiel OpenStack



Version 2021.02.01

Beispiel OpenStack



Beispiel OpenStack

Netzwerk	→	Neutron
Server	→	Nova, Placement
Images	→	Glance
Volumes	→	Cinder
Key-Manager	→	Barbican
Identitätsdienst	→	Keystone
Frontend	→	Horizon
CLI	→	Openstack-Client
Templates	→	Heat

Beispiel OpenStack

Erforderliche Infrastrukturkomponenten:

- Datenbank (Speichern der Zustände von Hosts, Instancen, etc)
- Message-Dienst (z.B. RabbitMQ) zum Übermitteln von RPC-Nachrichten
- Cache (z.B. memcached)

Life-Cycle-Management für Installation, Konfiguration, Updates, Zertifikatsmanagement

Sicherheit

Sicherheit

Schutzziele:

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Authentizität
- Autorisierung

Angriffsvektor

Wer kann **wo** und **wie** angreifen?

Sicherheit

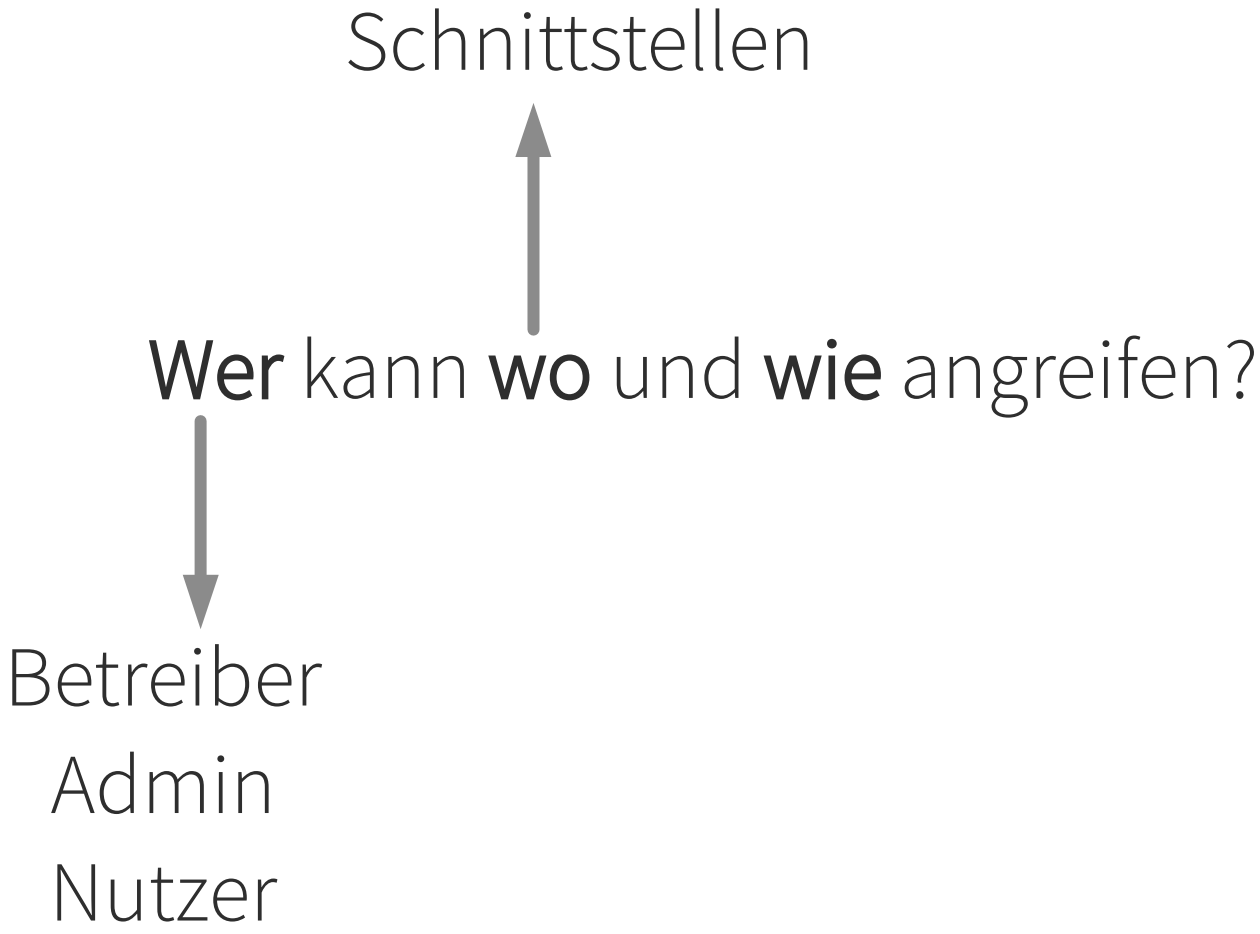
Wer kann **wo** und **wie** angreifen?

Betreiber

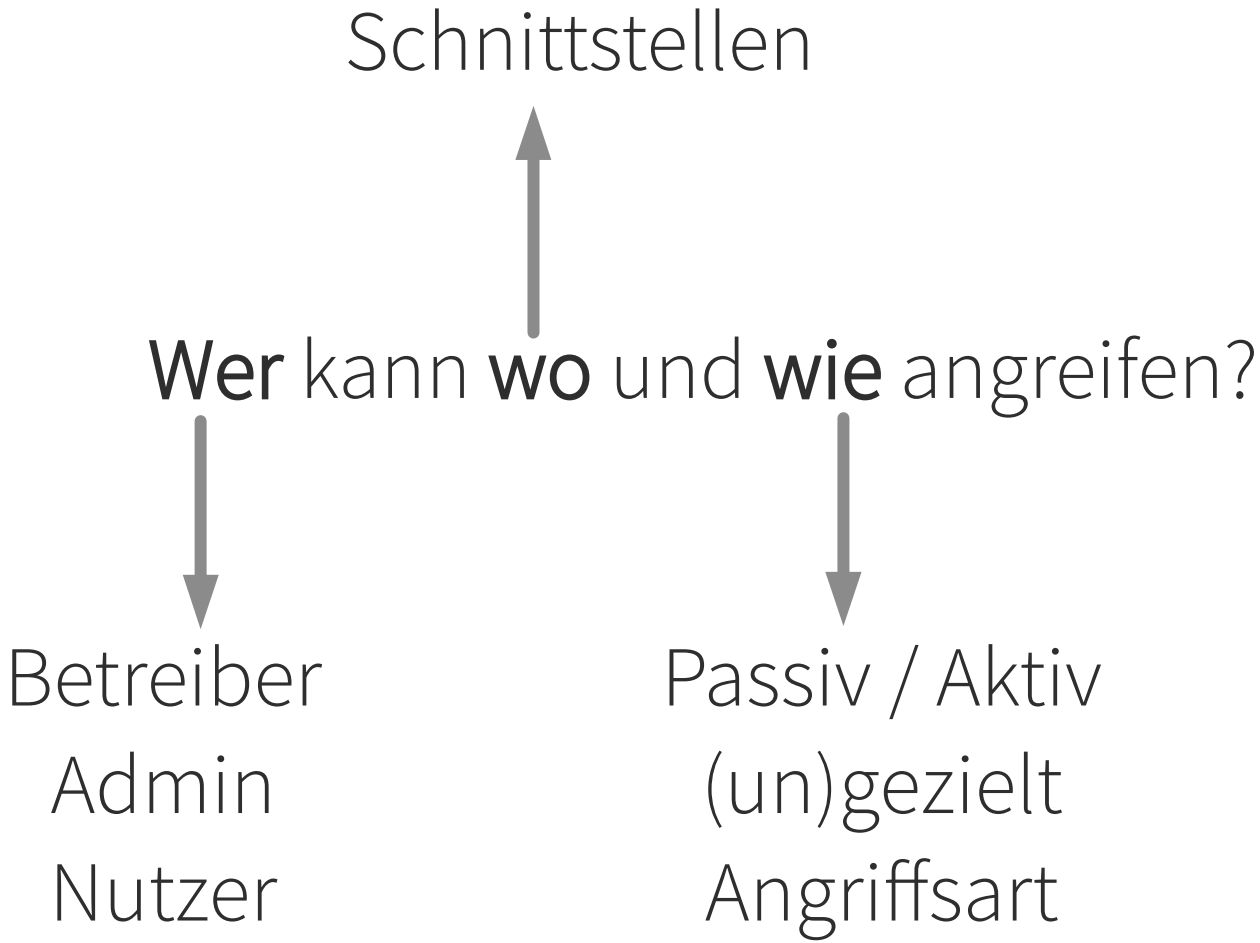
Admin

Nutzer

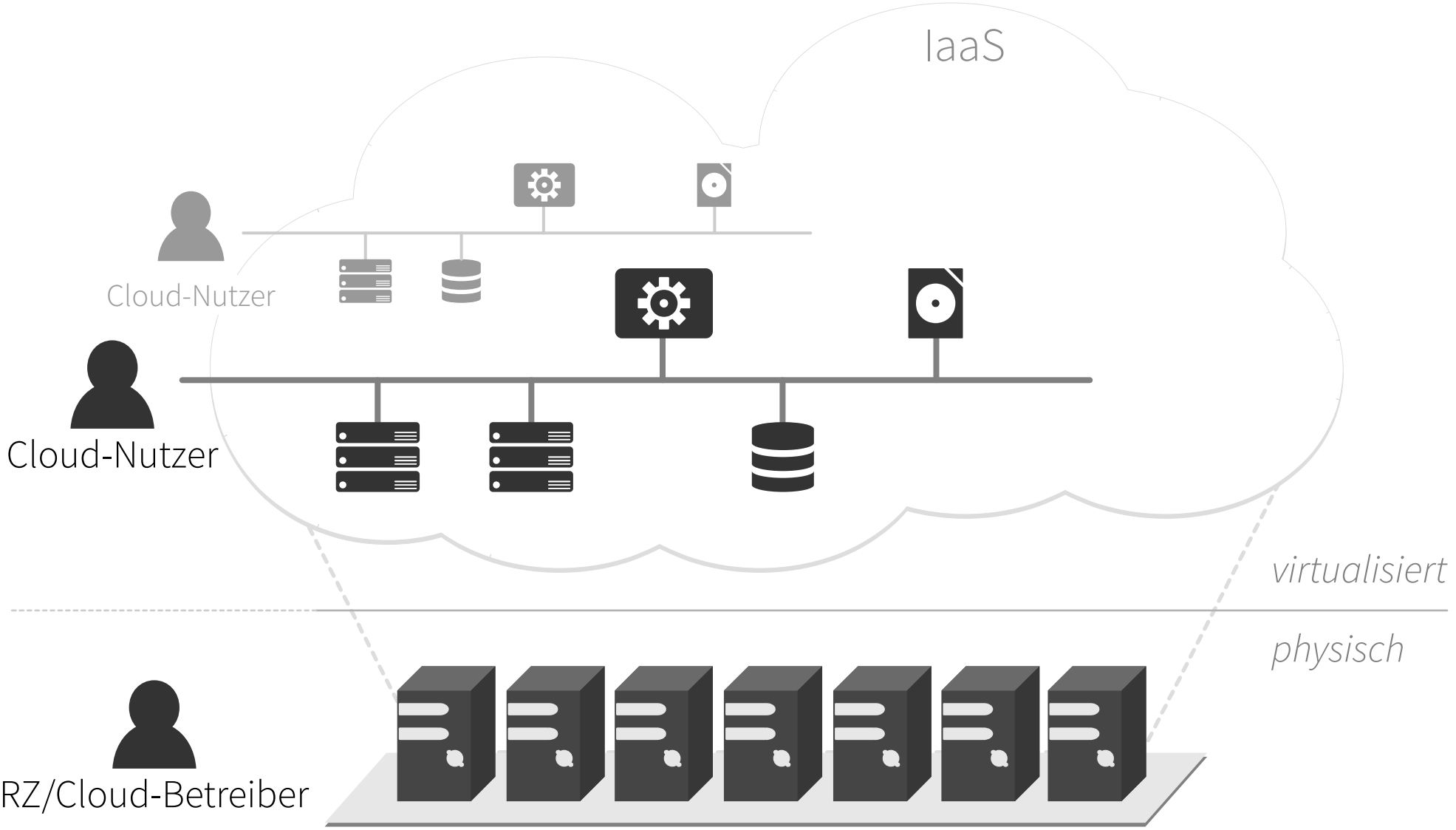
Sicherheit


Schnittstellen
Wer kann **wo** und **wie** angreifen?
Betreiber
Admin
Nutzer

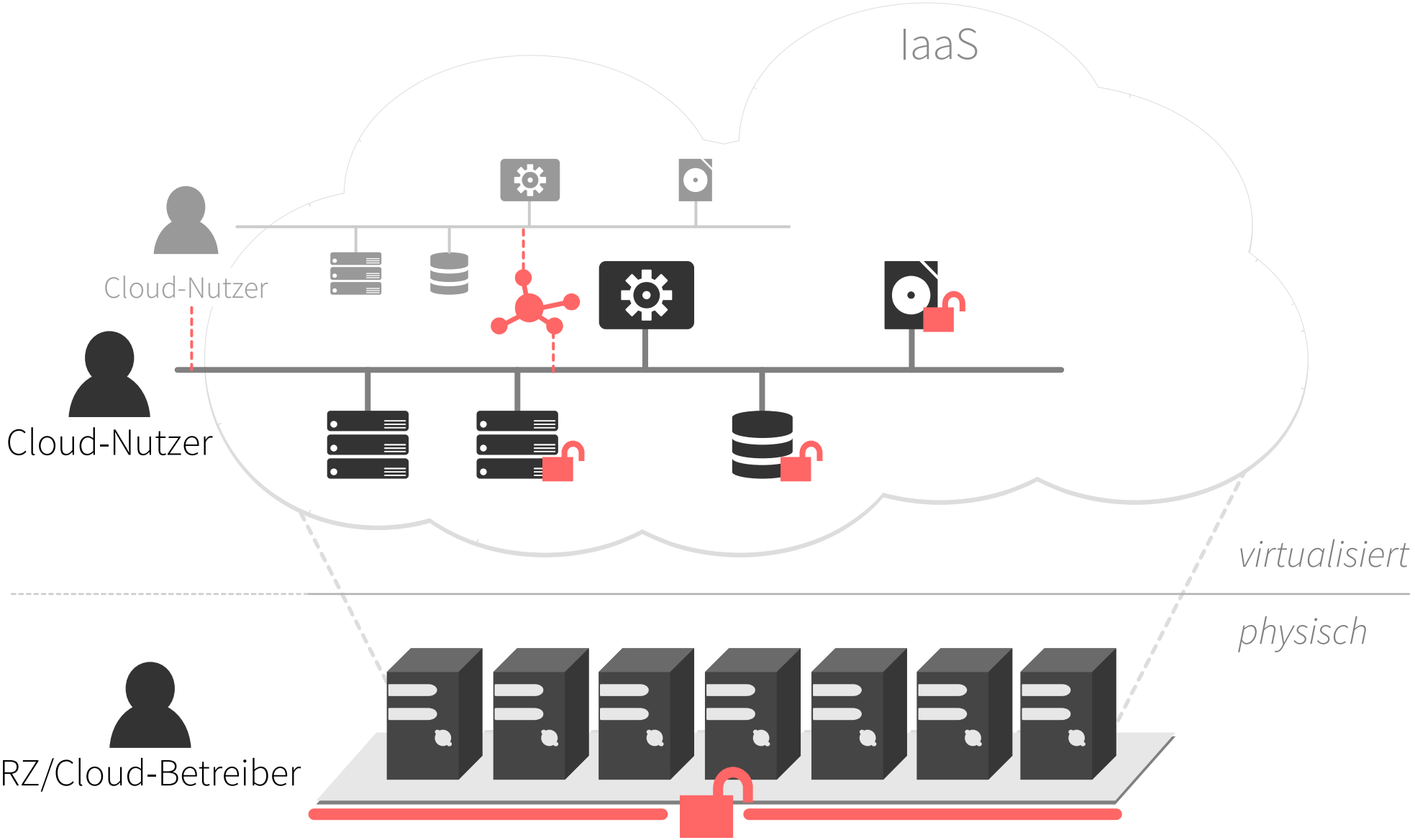
Sicherheit


Schnittstellen
Wer kann **wo** und **wie** angreifen?
Betreiber
Admin
Nutzer
Passiv / Aktiv
(un)gezielt
Angriffsart

Angriffsvektoren in Iaas?



Angriffsvektoren in Iaas - Beispiele



Absicherung des Cloud Computing

Absicherung der Nutzerdaten

Key Management Durch Nutzer

Sicherer Zugang Zur Cloud

Separation von Domänen/Projekten

Härtung und Absicherung der OpenStack Infrastruktur

Möglichkeiten zur Absicherung

Hardwareanpassungen

- Nutzung von HSMs
- Nutzung spezifischer Hardware für Netzwerke

Konfigurationsanpassungen

- TLS
- Verschlüsselte Datenbankverbindung
- Absicherung von RPC

Konfigurationsanpassungen

- Aktivierung von Barbican
- Aktivierung verschlüsselter Volumes

Codeanpassungen

- Verschlüsselung
- Zugangsbeschränkungen

Neue Konzepte

- Mandantentrennung
- VPN Realisierung in Hardware und Software

secustack

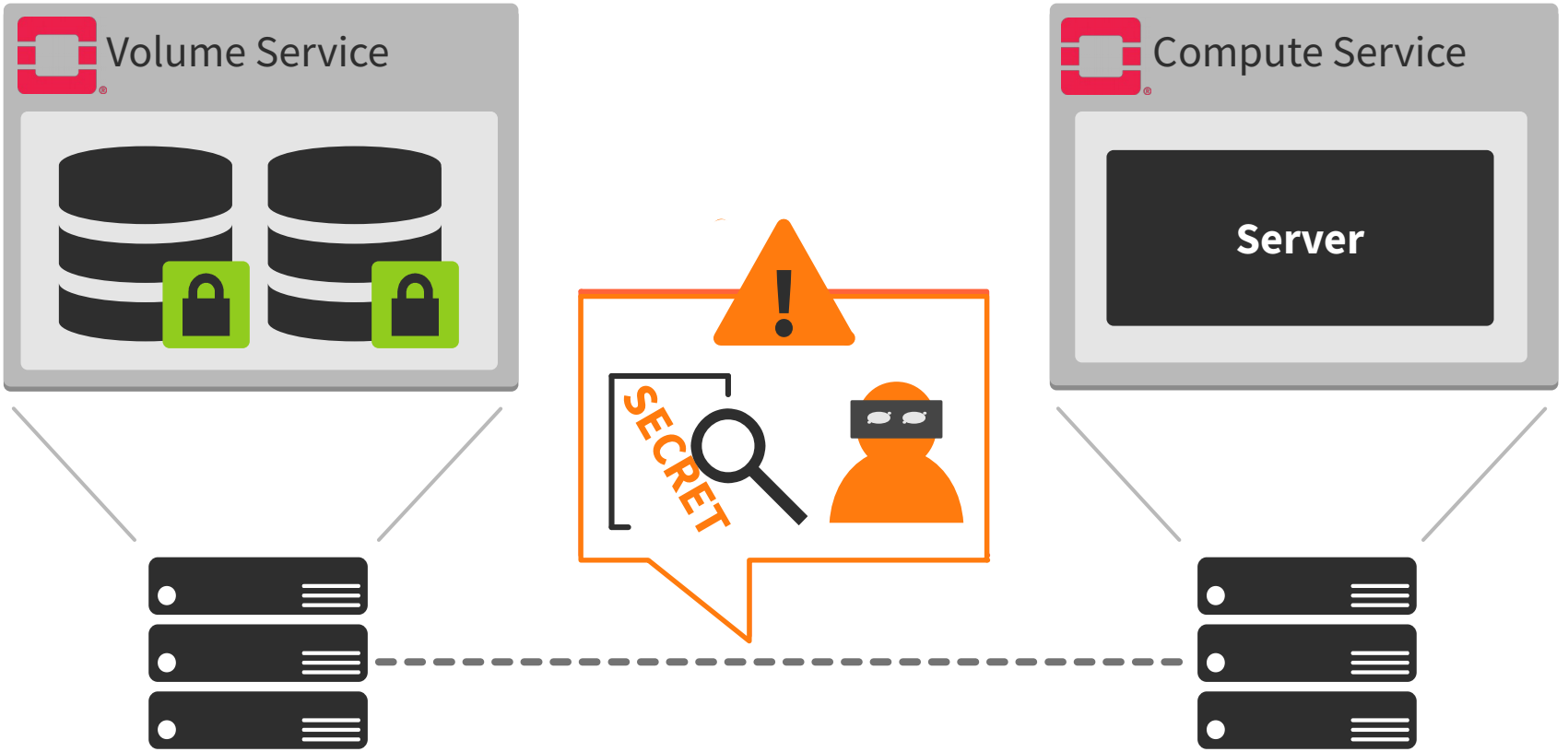
Entwicklung von Absicherungen

anhand von Angriffsvektoren

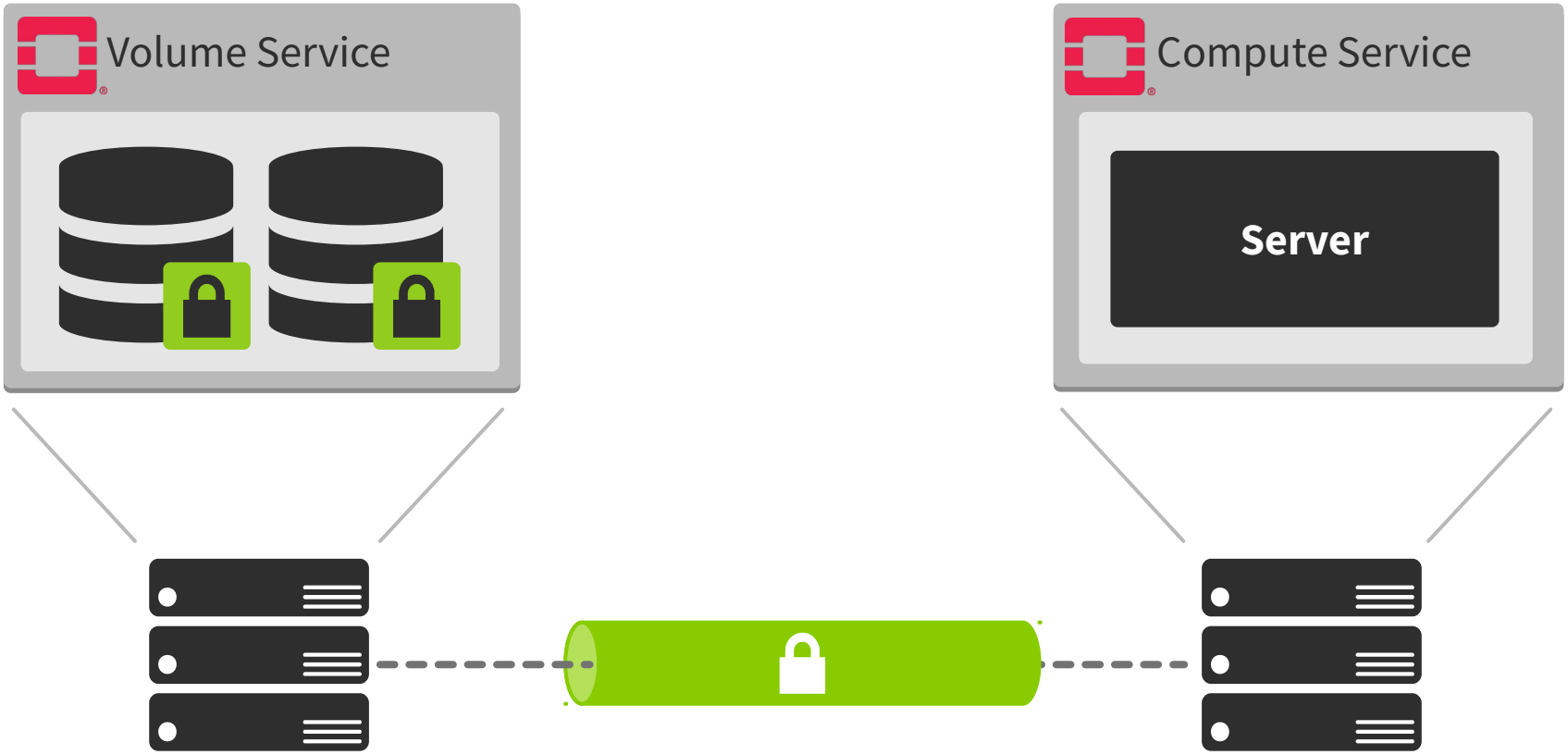
1. Kommunikationsabsicherung

AV: Man-In-The-Middle von Betreiberseite

1. Kommunikationsabsicherung



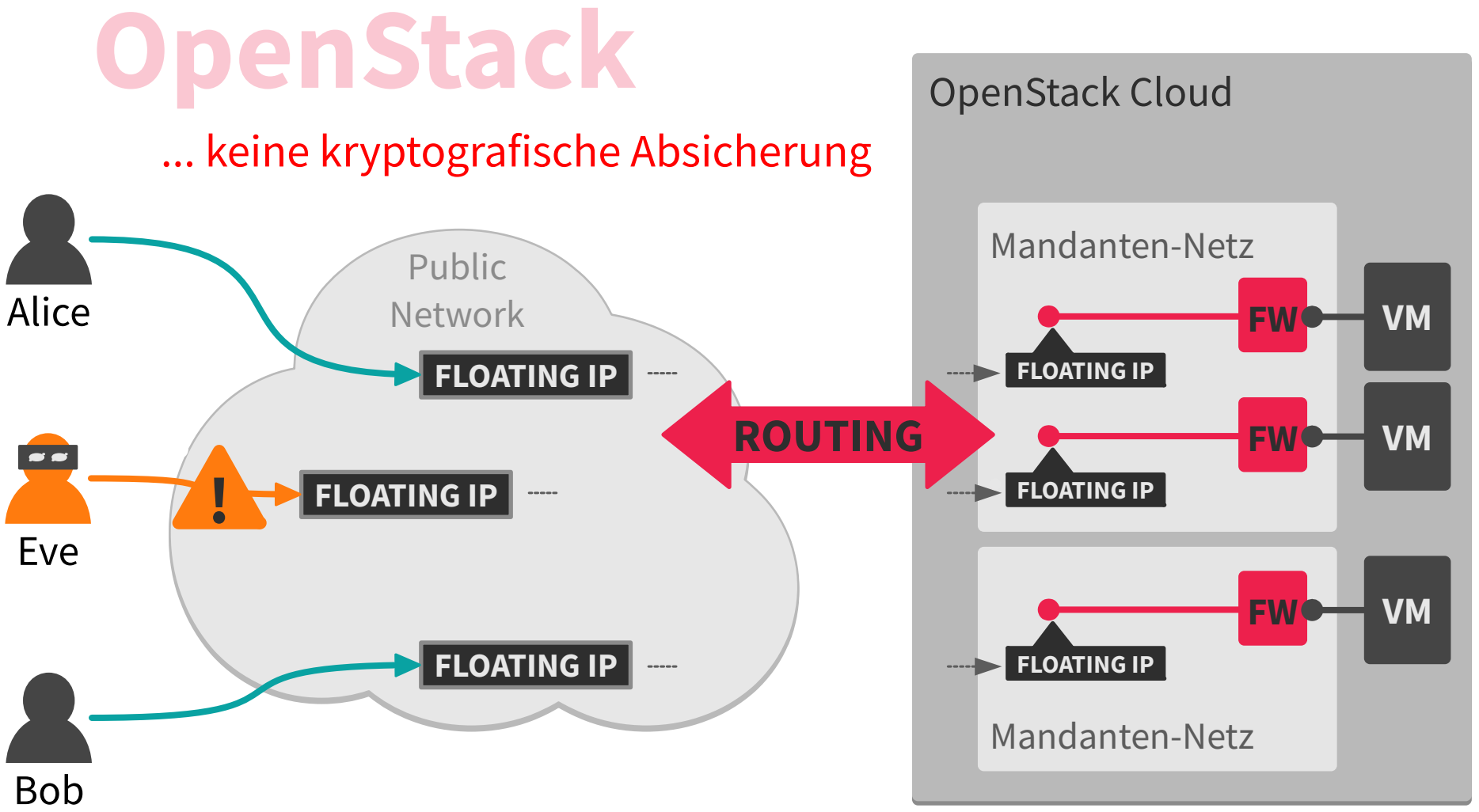
1. Kommunikationsabsicherung



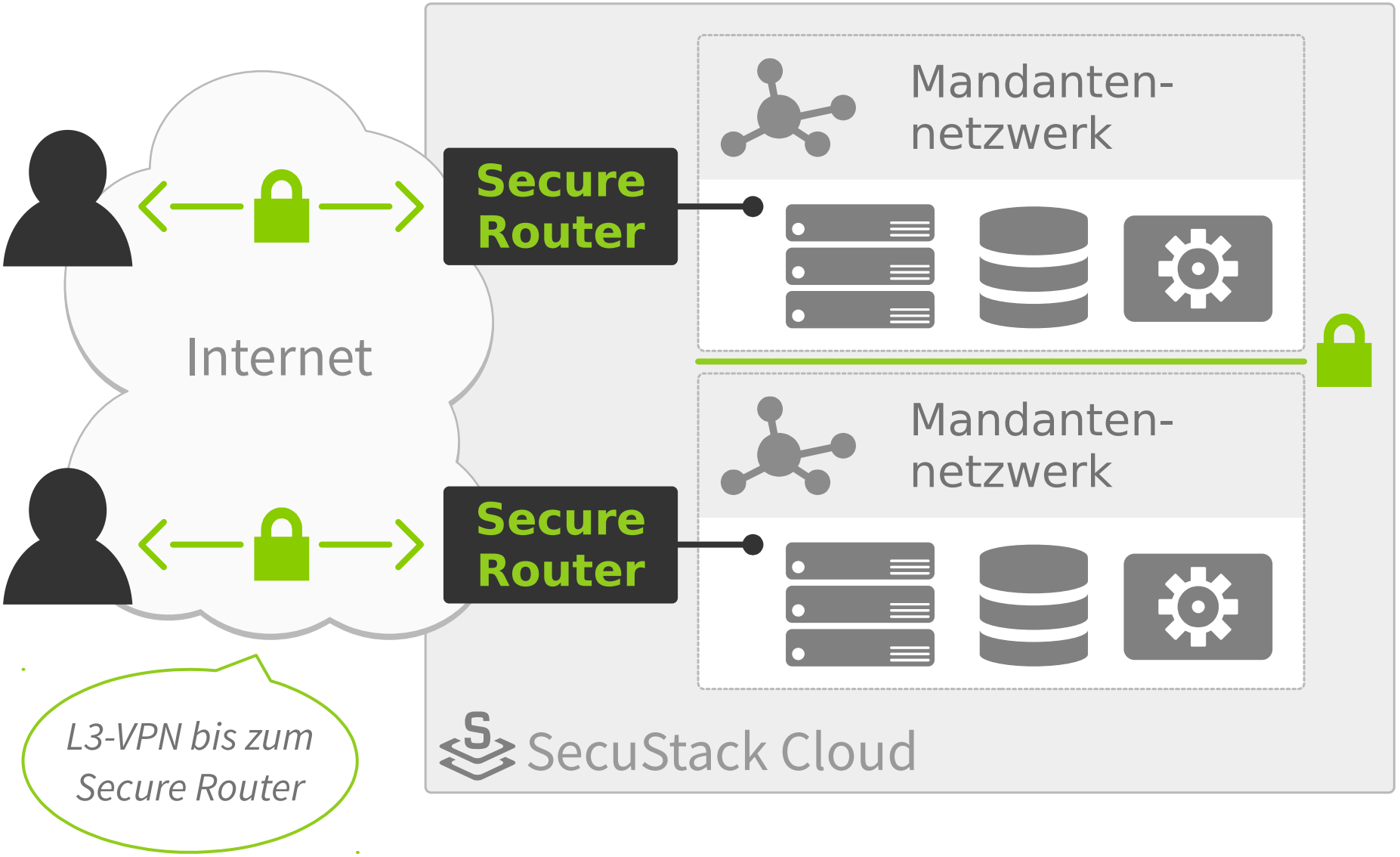
2. Verbindung Nutzer - Cloud

AV: Injection, MITM von Außen

2. Verbindung Nutzer - Cloud



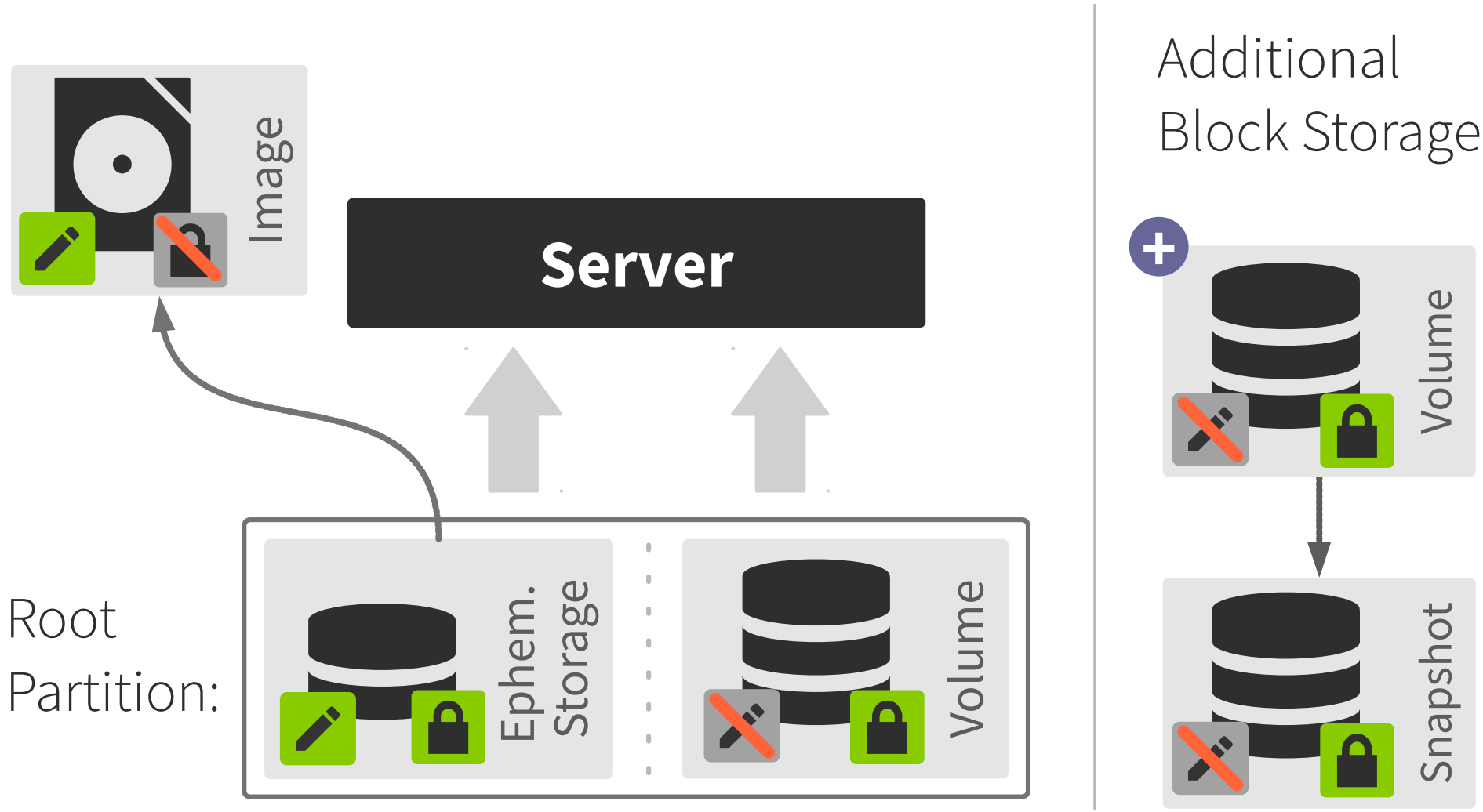
2. Verbindung Nutzer - Cloud



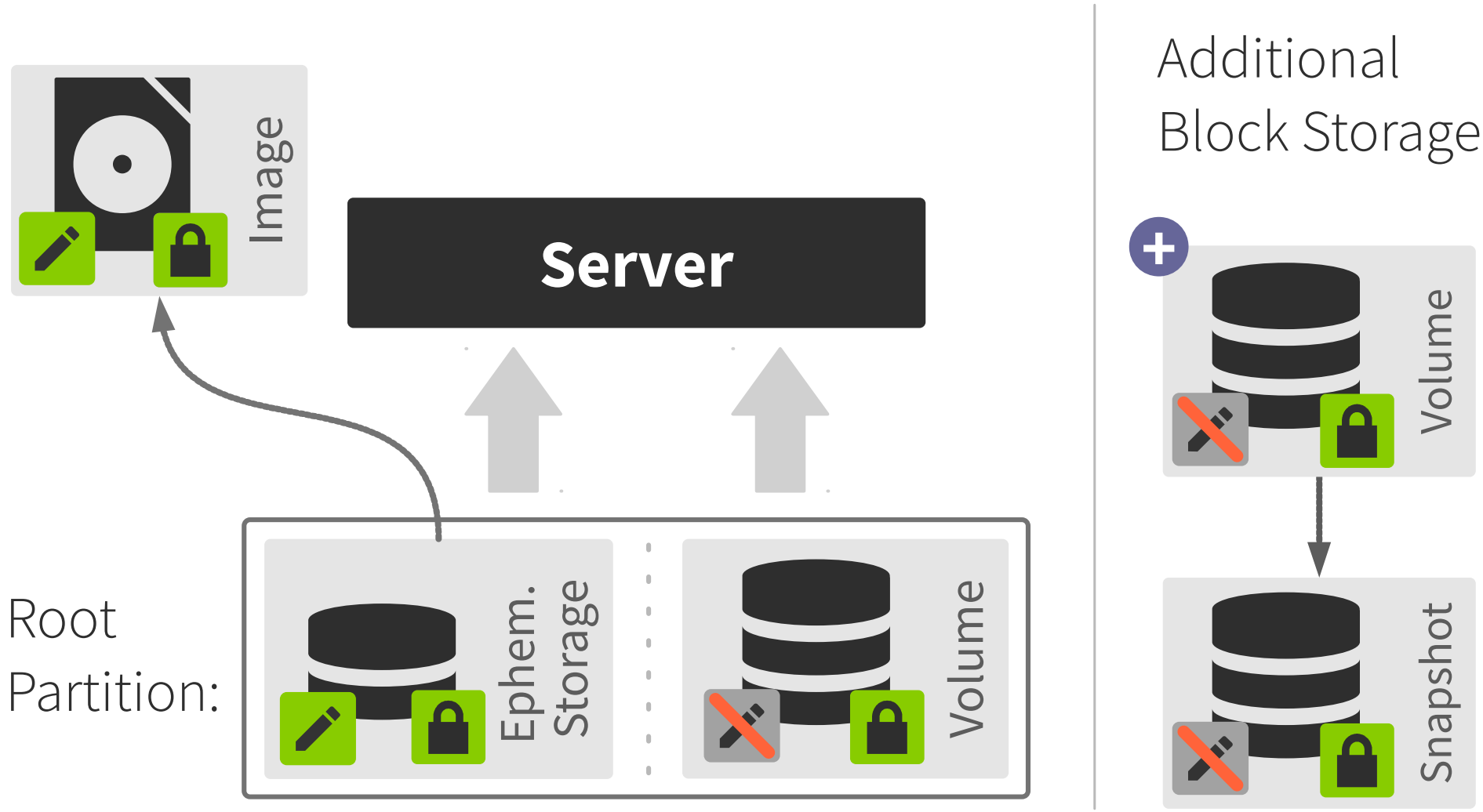
3. Verschlüsselung von Nutzerdaten

AV: Lesen/Verändern der Daten durch Fremde

3. Nutzerdatenabsicherung - Status Quo



3. Nutzerdatenabsicherung - Status Quo



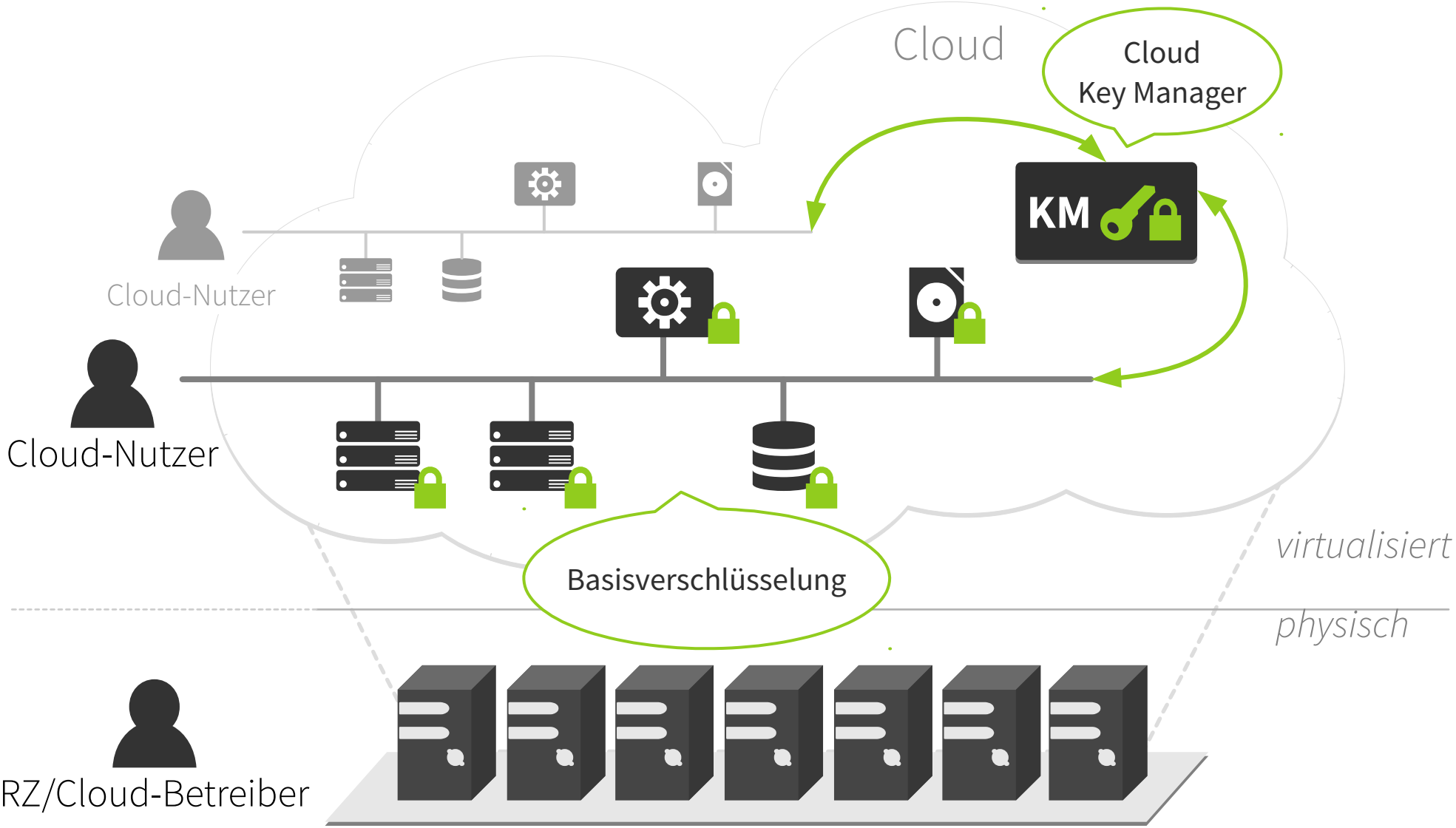
Signatur/Integrität

Verschlüsselung/Vertraulichkeit

3. Schlüsselverwaltung

Kryptographie ist wirkungslos, wenn das Schlüsselmaterial bekannt oder leicht zu bekommen ist.

3. Schlüsselverwaltung



3. Schlüsselverwaltung

OpenStack

Generierung

Cloud-Key-Manager generiert Schlüssel automatisch

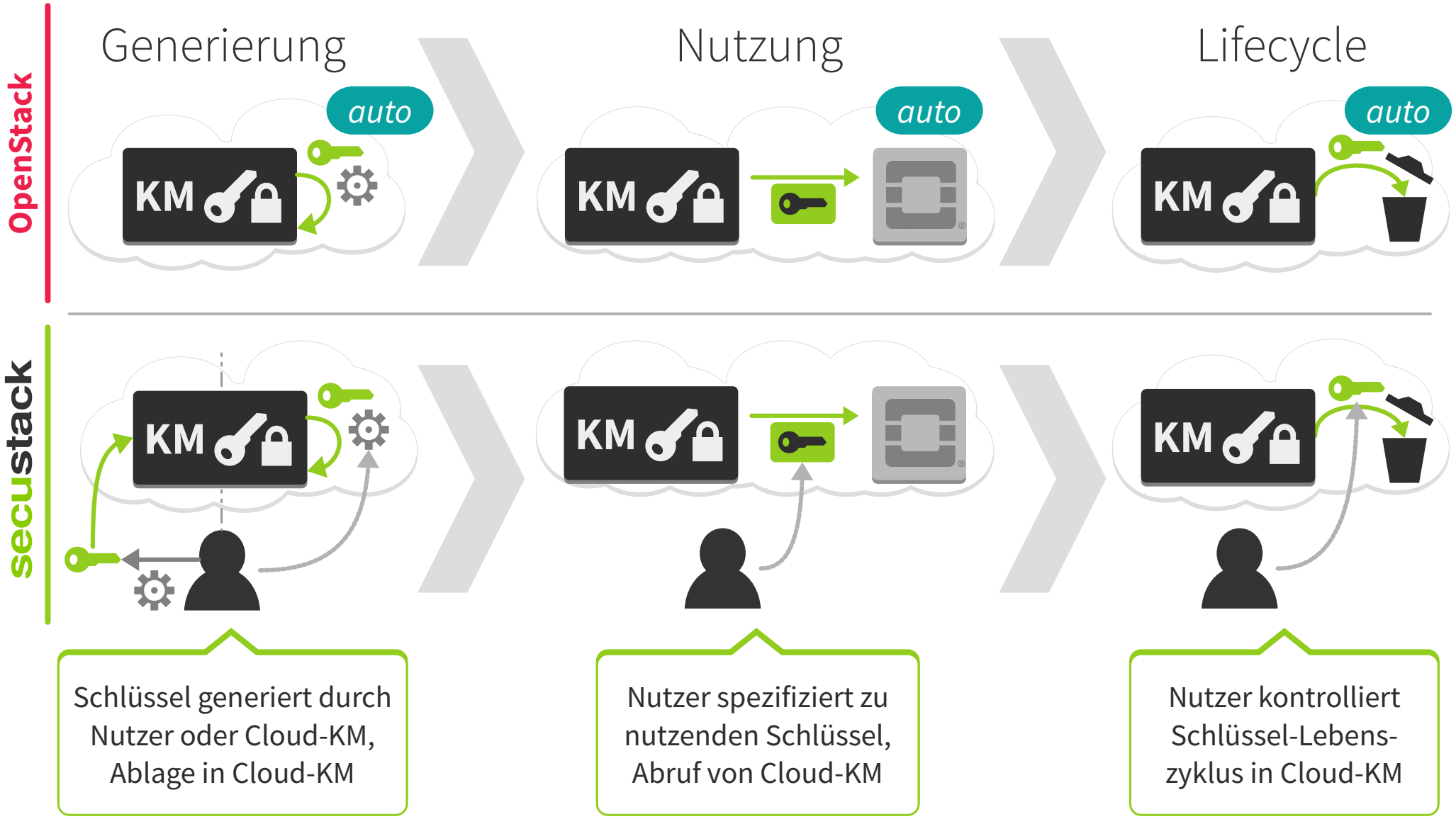
Nutzung

Cloud-Key-Manager überträgt Schlüssel an OpenStack-Dienst

Lifecycle

Cloud-Key-Manager handhabt Schlüssel-lebenszyklus

3. Schlüsselverwaltung

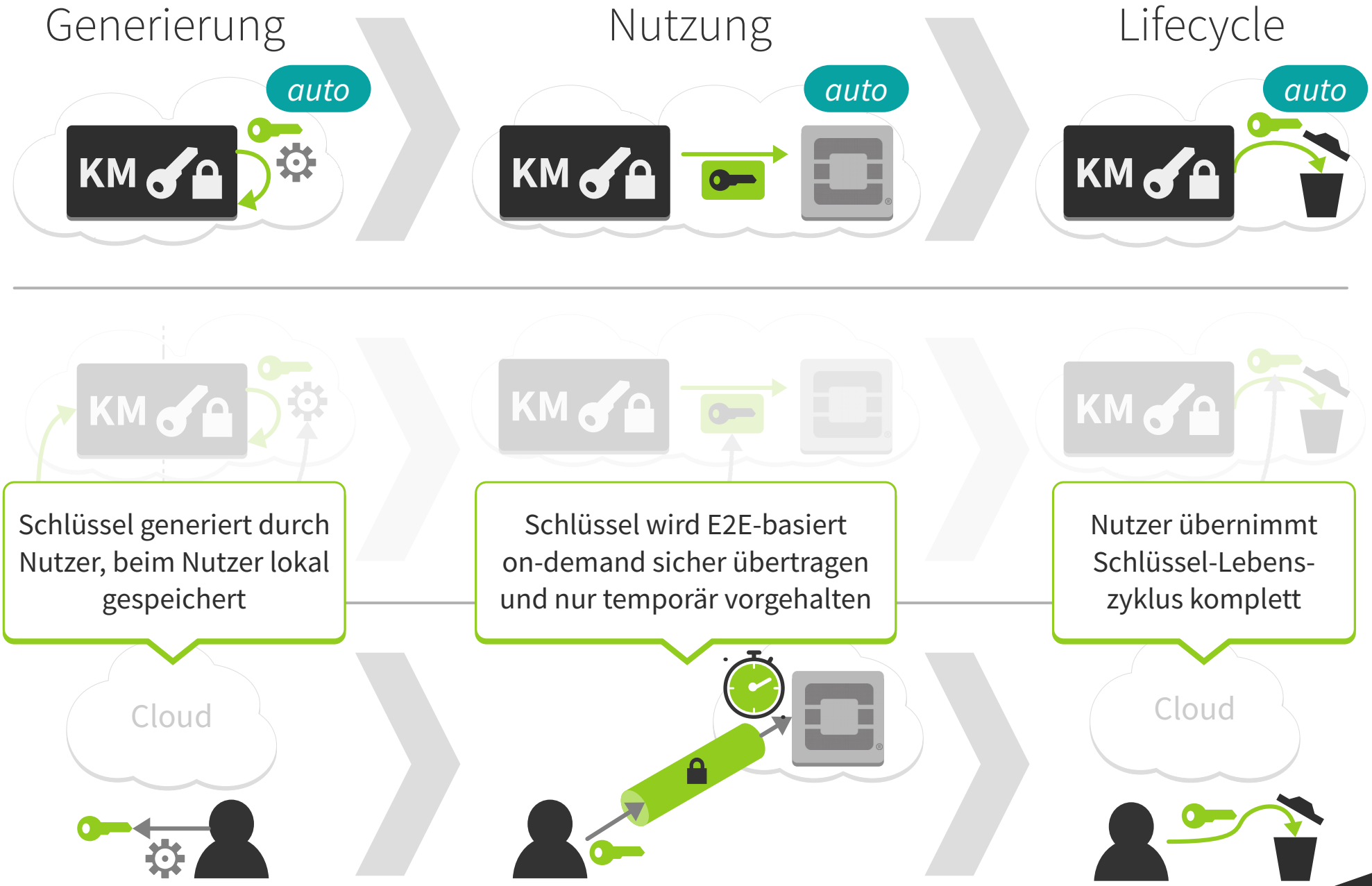


*Cloud-KM = Cloud-Key-Manager

3. Schlüsselverwaltung

OpenStack

secustack

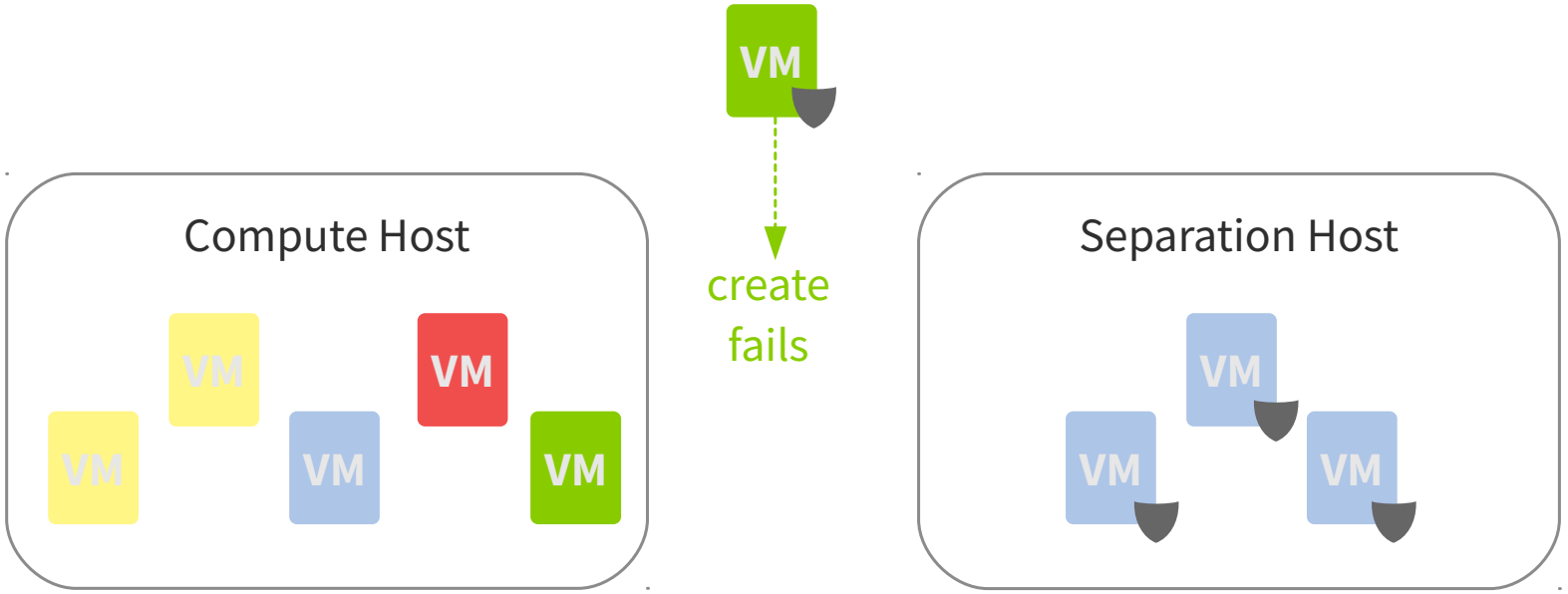


4. Kompromittierung eines Compute Host

AV: Ausbruch aus VM durch Nutzer

Isolation

- Unwahrscheinlicher Angriffsvektor
- Isolation von besonders sensiblen Daten In Use
- Basierend auf Project-Zugehörigkeit



Alternative Möglichkeiten

- Entwicklung neuer Hypervisor unter Sicherheitsaspekten
- Nutzung der Enklaventechnologie → SGXaaS für VM

Zusammenfassung:

- Angriffsvektoren bestimmen: Wer, Wo, Wie?
- Absicherung durch Hardware-, Konfigurations- und Codeanpassungen
- meist eine Kombination an Anpassungen nötig
- Alle vorgestellten Maßnahmen sind präventiv
- Wichtig sind auch detektive und reaktive Maßnahmen