



BEHÖRDENCLOUD ZUGELASSEN FÜR GEHEIM MIT L4RE

Dr.-Ing. Michael Hohmuth, Geschäftsführer Kernkonzept GmbH

In meinem Talk

- 01 Über Kernkonzept
- 02 Vorteile einer Cloud
- 03 Geheime Cloud unmöglich mit klassischem Hypervisor
- 04 Neue Architektur für geheime Cloud
- 05 Mehrere Informationsräume ohne Neuverkabeln

Wer ist Kernkonzept?

Inhabergeführt,
Sitz in Dresden

Gegründet 2012,
stetig wachsend

Spin-off der TU
Dresden

Internationales
Team von 30

Umfassende
Erfahrung seit
1996

Forschungsnah
und innovativ

Betriebssystem-
Spezialisten

Reifes L4Re
Operating System
Framework

Adressierte Märkte



**AUTO-
MOTIVE**



**HIGH
ASSURANCE**



**CYBER
SECURITY**



**SECURE
ENDPOINT**



**SMART
HOME**



**SECURE
CLOUD**



**INDUSTRIAL
IOT**



AVIONICS

Vorteile der Cloud

Kosten-
ersparnisse

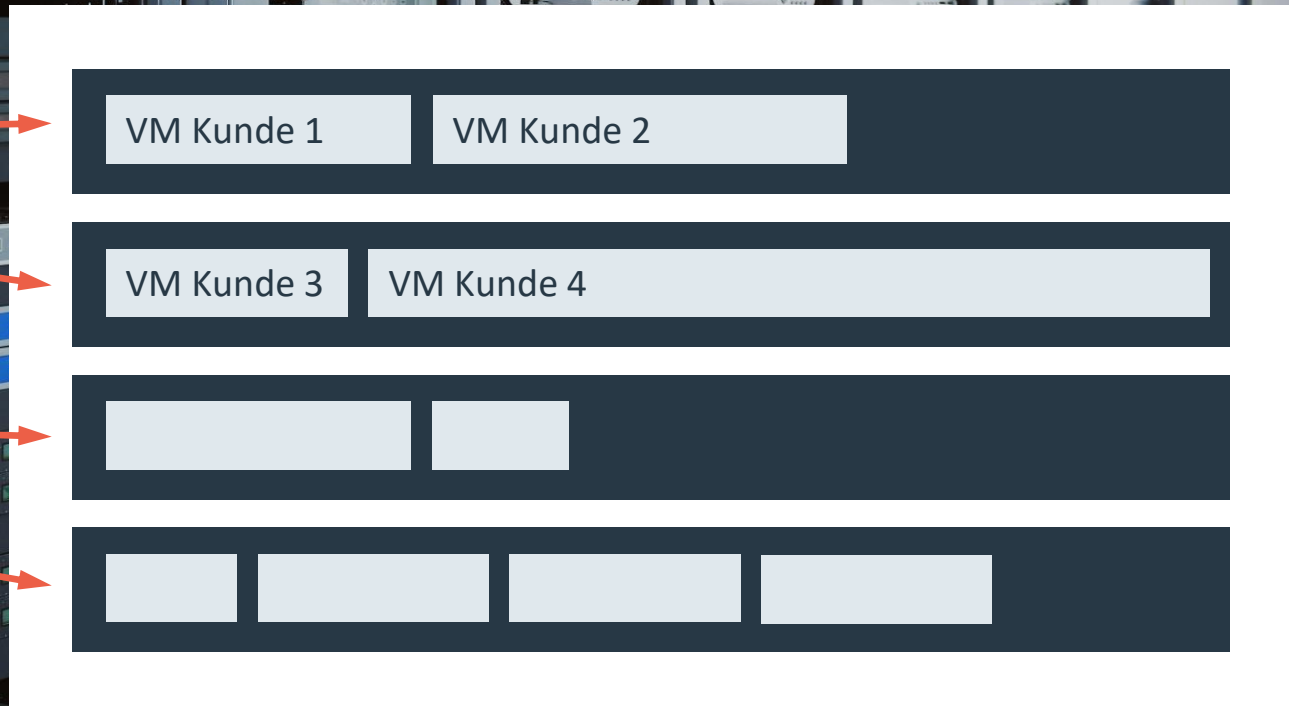
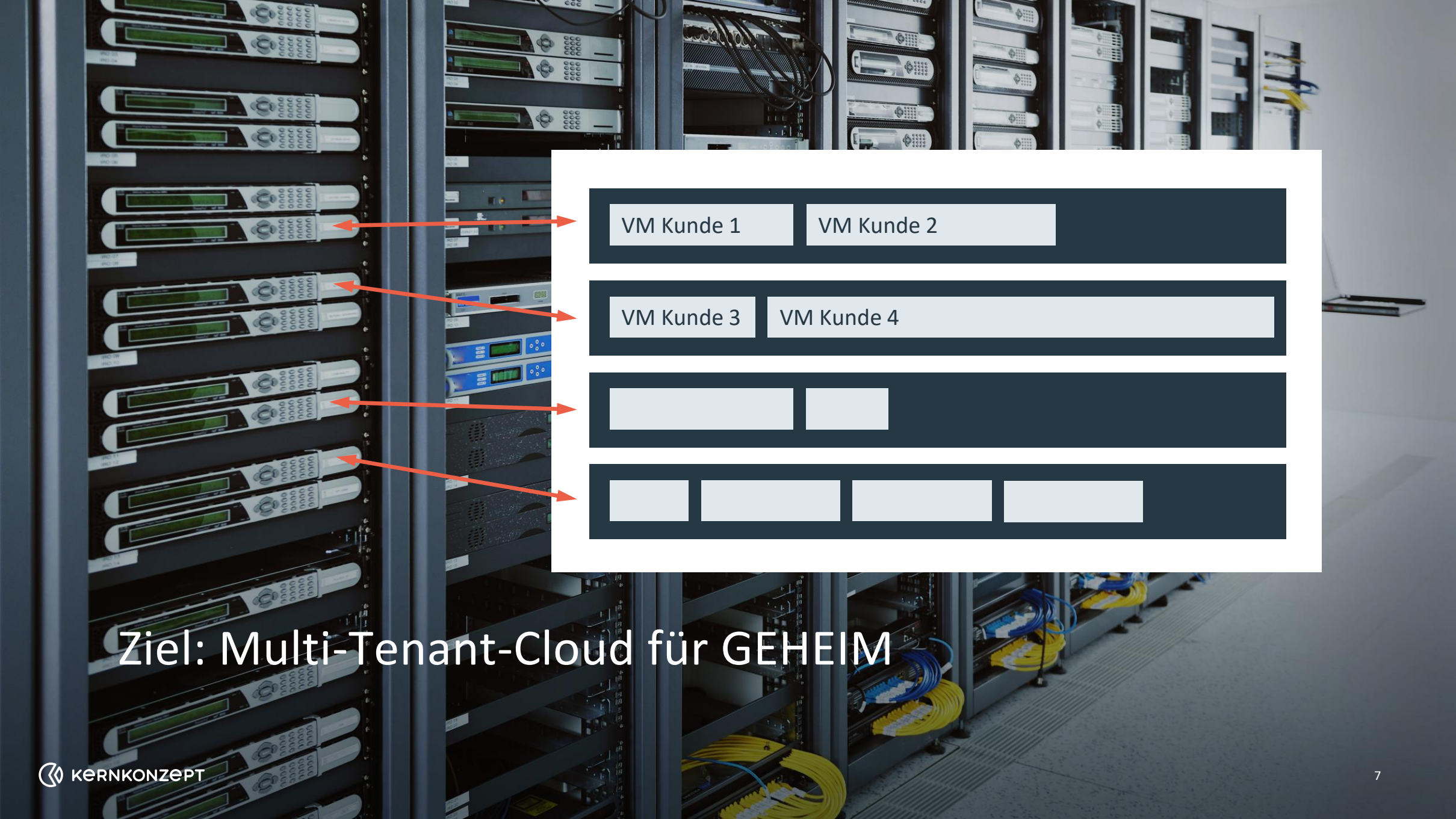
Zentrale
Administration

Flexible
Reaktion auf
Lastensituation

Höhere
Sicherheit

Ausfallsicherheit

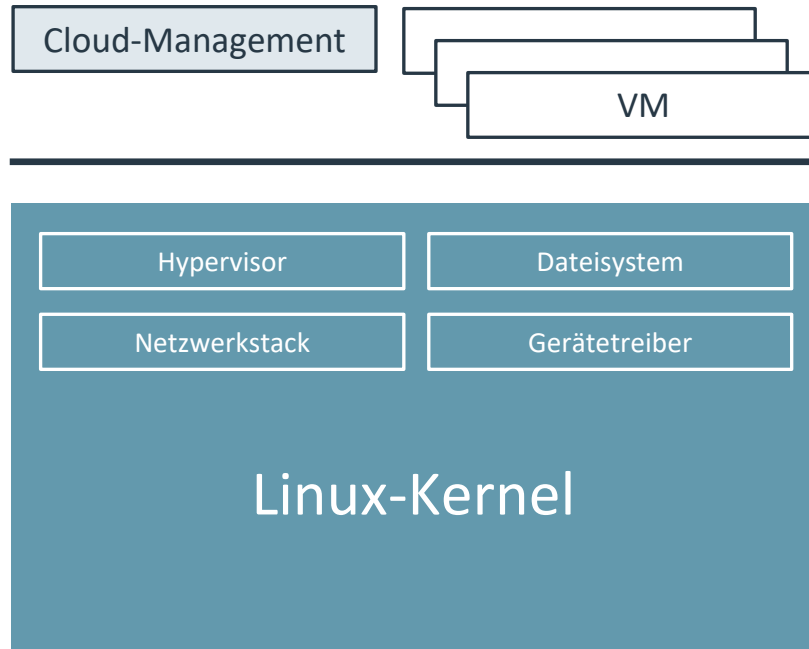
State of the Art



Ziel: Multi-Tenant-Cloud für GEHEIM

Monolithischer Hypervisor

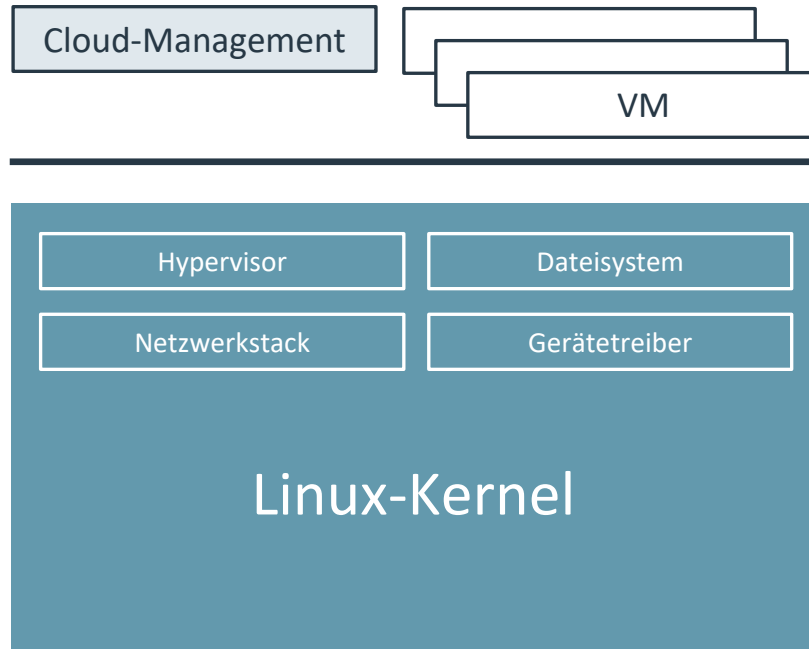
+ Klassische Cloud



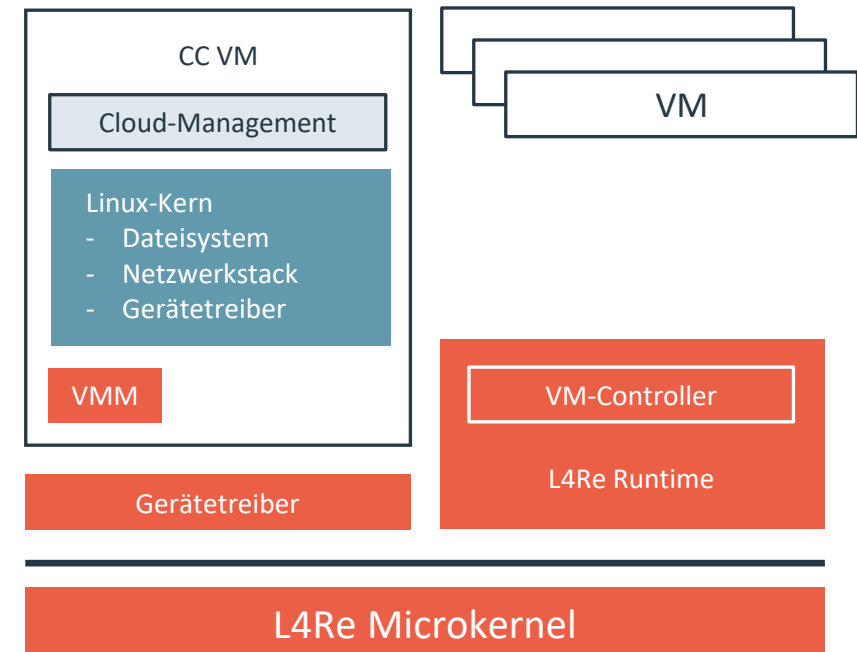
- + Zu große Trusted Computing Base
- + Isolation kann nicht verlässlich durchgesetzt werden
- + Nicht zulassungsfähig

Vertrauenswürdige Isolation

+ Klassische Cloud

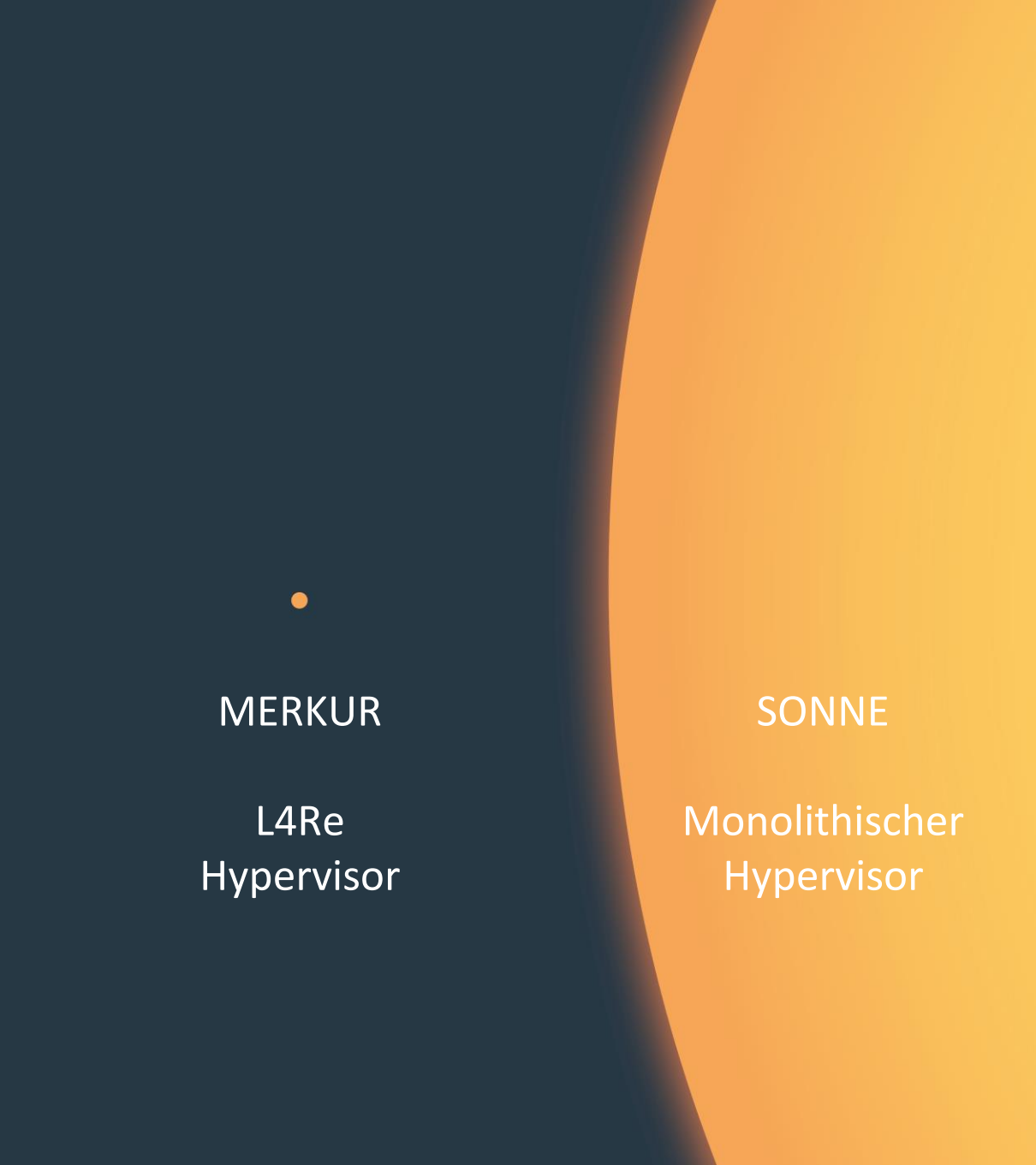


+ L4Re-Cloud



TCBs im Vergleich

- + Monolithischer Hypervisor:
viele Mio. Zeilen Code
- + L4Re: 30.000 Zeilen Code



MERKUR

L4Re
Hypervisor

SONNE

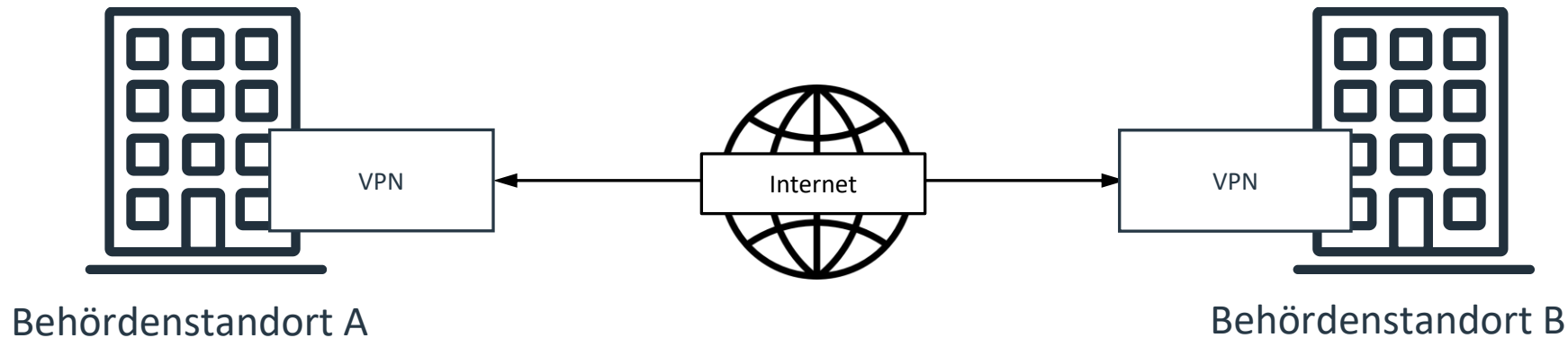
Monolithischer
Hypervisor

Problemstellung

- + Für eine Behörde muss die sichere Kommunikation mit der VM sichergestellt sein

Virtual Private Network (VPN)

- + Überbrückt nicht vertrauenswürdige Netze mit Crypto
- + VPN-Geräte sind zugelassen und am Markt





VPN 1

VM Kunde 1

VPN 2

VM Kunde 2

VPN 3

VM Kunde 3

VPN 4

VM Kunde 4

Mit VPN-Appliances

A man with short brown hair and a beard, wearing a black t-shirt and blue suspenders, is focused on a silver laptop. He is standing in a server room, with a dense array of orange and blue network cables plugged into a rack of server units behind him. The cables are bundled and organized, creating a complex web of lines. The lighting is soft and focused on the man and his work.

Verkabelung – Fehleranfälligkeit



VPN 1

VM Kunde 1

VPN 2

VM Kunde 2

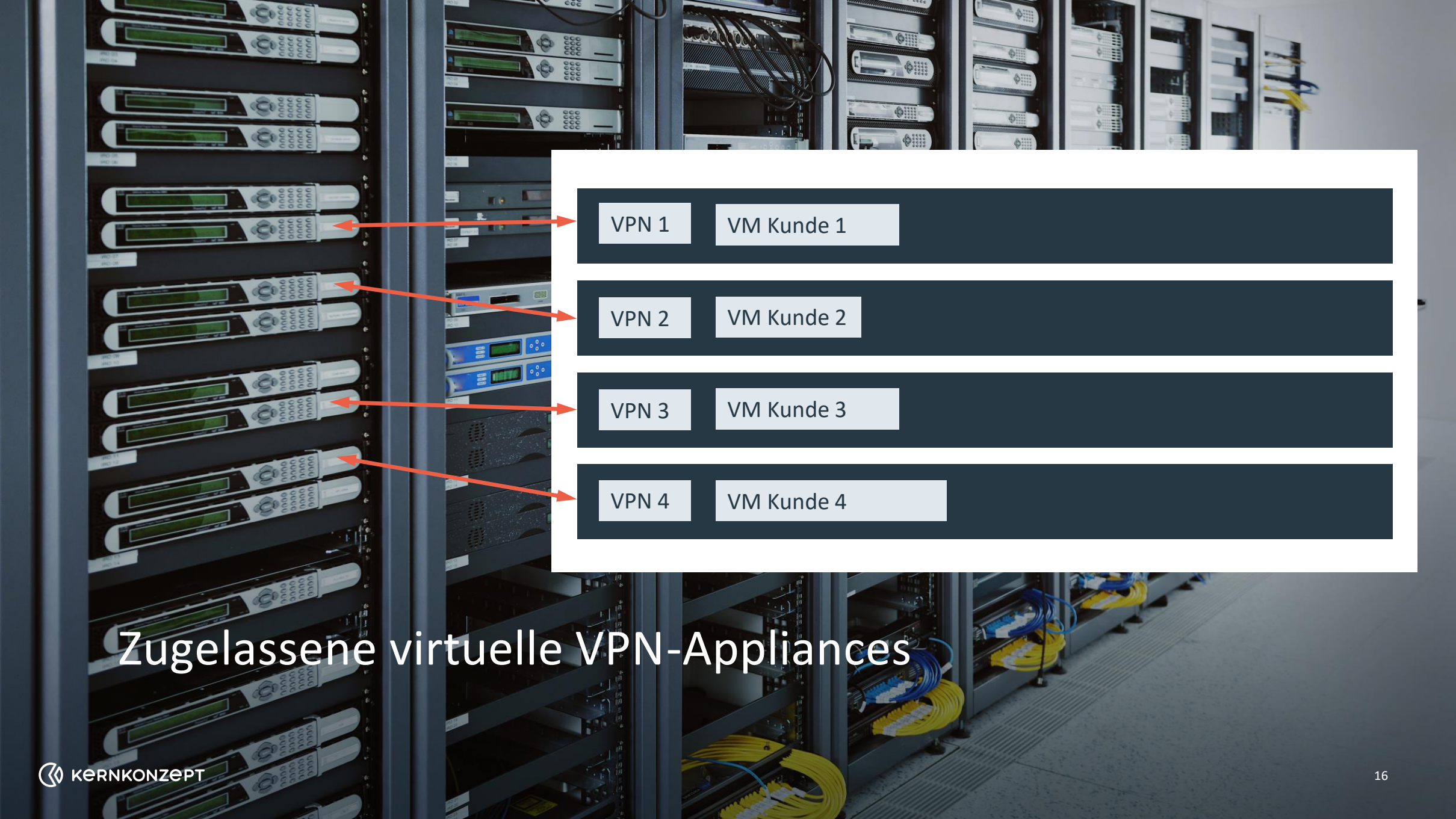
VPN 3

VM Kunde 3

VPN 4

VM Kunde 4

Mit VPN-Appliances



Zugelassene virtuelle VPN-Appliances

Schlüsseltechnologie: Virtueller VPN-Endpunkt

+ Zugelassener L4Re-Separationkernel

- Verschiebt zugelassenen VPN-Endpunkt aus separatem Gerät in virtuelle Maschine
- Separation durchgesetzt durch Microkernel
- Zulassungserhaltend
 - Ähnlicher Ansatz bereits in VS-TOP zugelassen und im Einsatz

ZUSAMMENFASSUNG

L4Re Hypervisor ermöglicht geheime Cloud

- + L4Re Hypervisor ermöglicht vertrauenswürdige Netzwerkverschaltung direkt im Hypervisor
 - Vertrauenswürdige Trennung von VMs
 - Vertrauenswürdige Netzwerkanbindung der VMs
 - Realisierung einer zulassungsfähigen geheimen Cloud



VIELEN DANK!

Bitte besuchen Sie uns an unserem Stand!

www.kernkonzept.com