secunet

# VS-Arbeitsplatz und resiliente Netze im sicheren Cloud Ökosystem

Omnisecure, 21.01.2025

Peter Rost und Michael Hohensee

secunet Security Networks AG
SysEleven GmbH

# Agenda

01

# Herausforderungen für die VS-IT

# Kontext: Herausforderungen für VS-IT

- IT-Konsolidierung Bund
- Netzstrategie 2030
- Zunehmende Bund-Länder-Kommunikation
- Sinkende Personaldecke in der öffentlichen Verwaltung
- Verwaltungsdigitalisierung
- Virtualisierung der Büro-Anwendungen
- Open-Source Software kommt ins Spiel
- Uneinheitliche Definitionen von Digitaler Souveränität
- BSI im Wandel

02

# VS-Arbeitsplätze

# VS-Arbeitsplätze


- In der Behörde: Desktop, Laptop, Tablet
- Unterwegs: Laptop, Tablet, Smartphone
- Auch mobil (fast) immer online
- Fat vs. Thin Client
- Oft mehrere Sicherheitsdomänen je Nutzer (Offen, VS-NfD, VS-V, GEHEIM)
- Performance der Clients, der Netze und der Anwendungs-Backends

03

# Resiliente VS-Netze

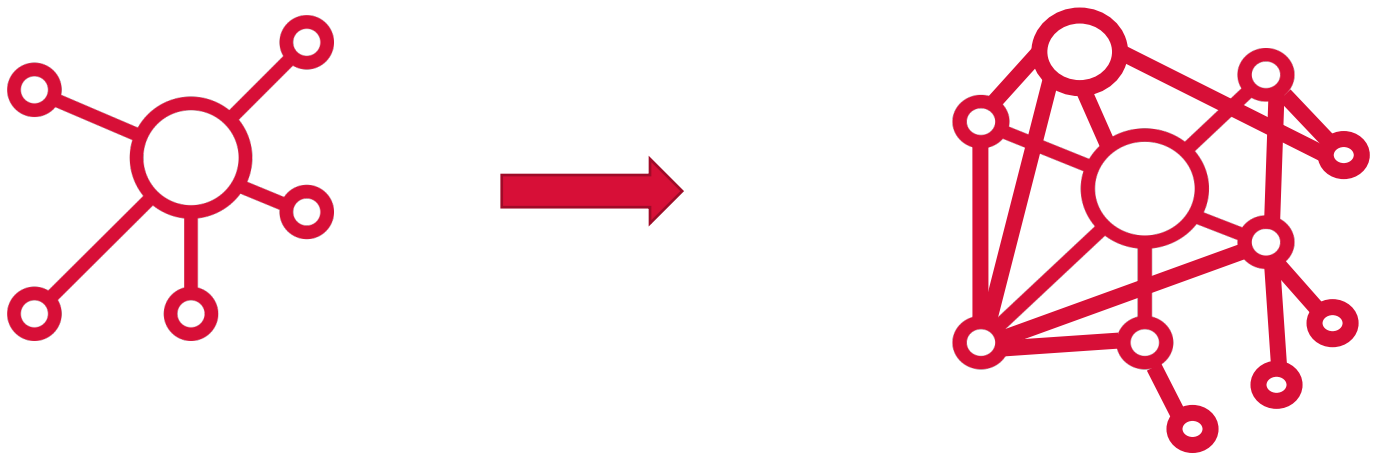
# Herausforderungen an Weitverkehrsnetze

| Anwendungsgetriebene Trends | Herausforderungen |
|---|---|
| ▪ Virtuelle Kommunikationsdienste | ▪ Mehr breitbandiger Video-Traffic, latenz-sensitiver Sprachtraffic |
| ▪ IT-Konsolidierung | ▪ Neue Mandanten führen zu höherem Gesamt-Traffic-Volumen im Netz und an den Internet-Übergängen / Client-Gateways |
| ▪ Verwaltungsdigitalisierung | ▪ IT-Dienste-Konsolidierung verlagert Traffic-Ströme hin zu anderen Standorten / Clouds |
| ▪ Noch mehr Remote Worker | ▪ Zehntausende neuer, teils remote arbeitender Clients pro Jahr mit dynamisch wechselnden Traffic-Patterns |
| ▪ Fernziel Zero Trust Network Access | ▪ 1:n Kryptoverbindungen statt 1:1 VPN-Zugang |

# Auswirkungen auf die Struktur der Weitverkehrsnetze

**WAN-Topologien werden stetig komplexer durch:**

- Hinzufügen neuer Standorte, Mandanten, mobiler User
- Einrichtung zusätzlicher Leitungen
  - Resilienzgetrieben (Backup-/Fallback-Verbindungen)
  - Performancegetrieben (Querverbindungen z.B. für ViKo/VoIP)
- Folge: Immer weniger reine Sternstrukturen, zunehmende Vermaschung



# Vom Client in die Cloud: wir brauchen resiliente und skalierbare VS-Netze

- Kosten der Netzwerk-Resilienz minimieren
  - Integration bisher separater Netzwerkelemente
  - Admin-Aufwand verringern durch Automatisierung von Sicherheitsbeziehungen
  - Investitionsnutzen maximieren durch VS-Multimandanten-Fähigkeit
- Performance maximieren (erfolgskritisch für SaaS aus der Cloud)
  - Direkte Wege zu den Dienste-Servern in die (Multi-)Cloud
  - Traffic-Verteilung und –Priorisierung je nach QoS-Anforderungen und Leitungsverfügbarkeit
  - Software-Beschleunigung und Feature-Verfügbarkeit für bereits beschaffte Hardware

# SOLID als Kryptotunnel-Automatisierungslösung

- **Automatische, optimale Krypto-Routenfindung** bei Hinzukommen neuer Strecken, Standorte und Geräte und bei Ausfällen/Engpässen im Netz
- **Automatische Konfiguration der neuen Routen und SAs** im Krypto-Overlay-Netzwerk durch die SOLID-Boxen
- Bis hin zur logischen und physischen **Vollvermaschung** (Any-to-any)
- Kurz: „Automatisches Routing“ für IPsec-VPN-Verbindungen –
  Im Prinzip baut SOLID für IPsec nach, was OSPF und BGP für IP (d.h. das WWW) leisten
- SOLID: Secure OverLay for IPsec Discovery

# Bisher: statische Cluster-Konfiguration

SINA Workstation S
SINA Mobile Smartphones
und Tablets

Internet

Standort Z

Loadbalancer

Cluster
SINA L3 Box S
(ohne SOLID)

Standort A

Server A

Standort B

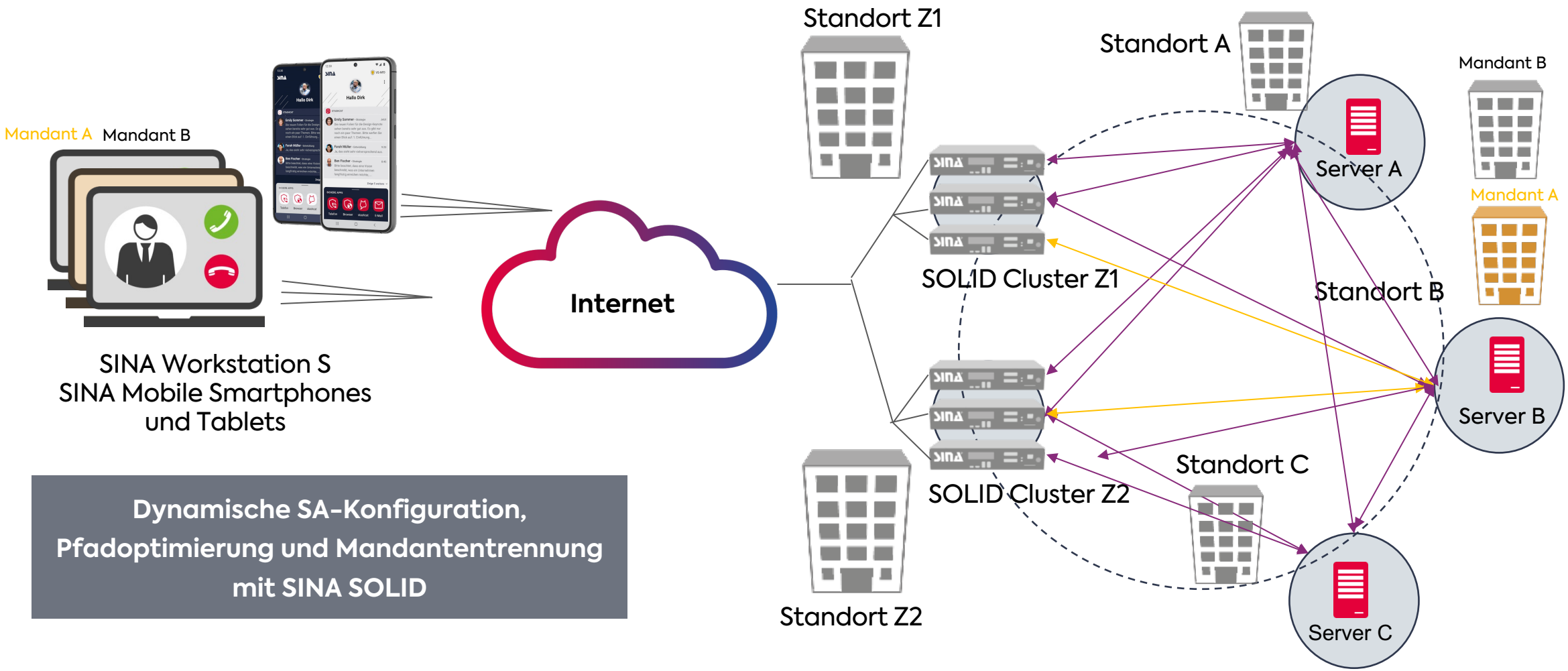
Standort C

Server C

**Zugriff auf die Server an den Standorten nur über zentrale Zugangsboxen**

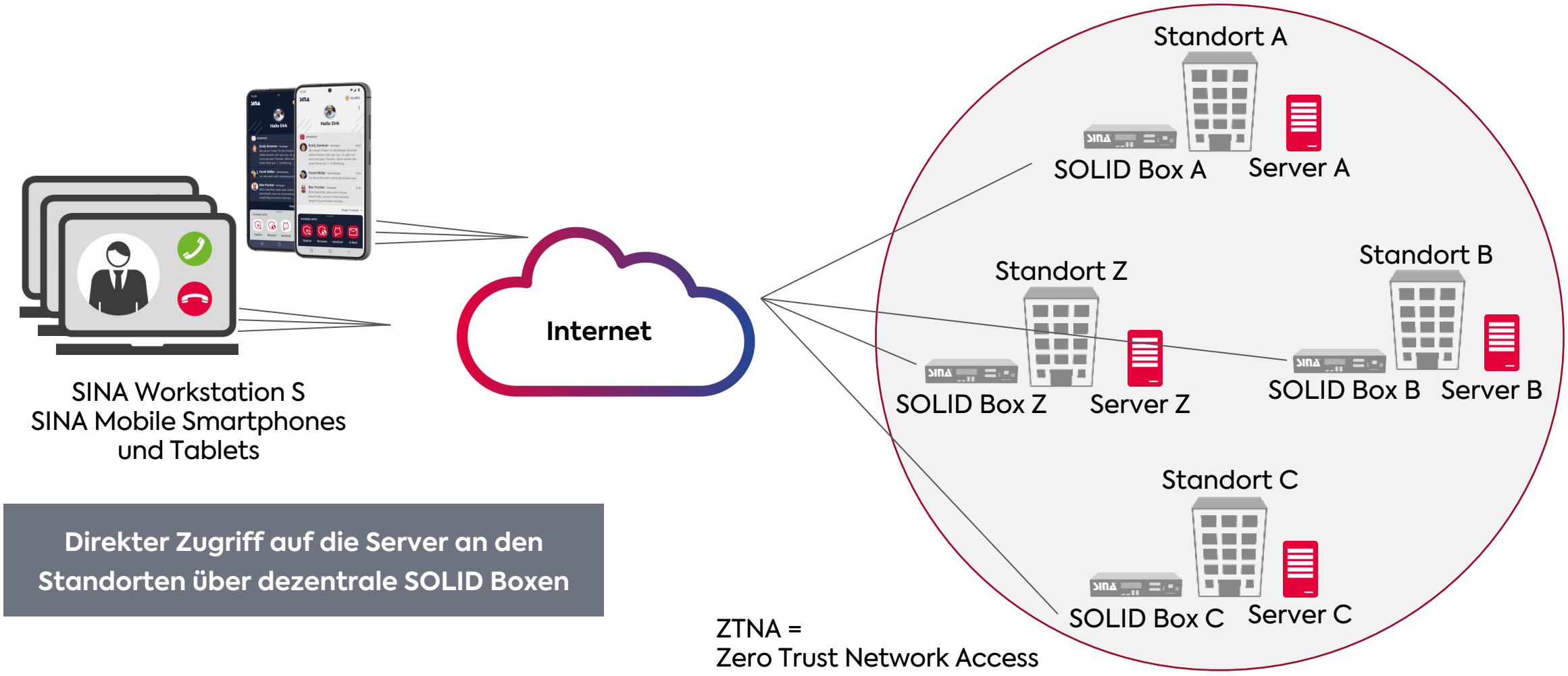
# Optimierung der SINA Client-Anbindung

SINA Workstation S mit geo-redundanten SOLID-Zugangs-Clustern und Mandantentrennung




**Dynamische SA-Konfiguration, Pfadoptimierung und Mandantentrennung mit SINA SOLID**

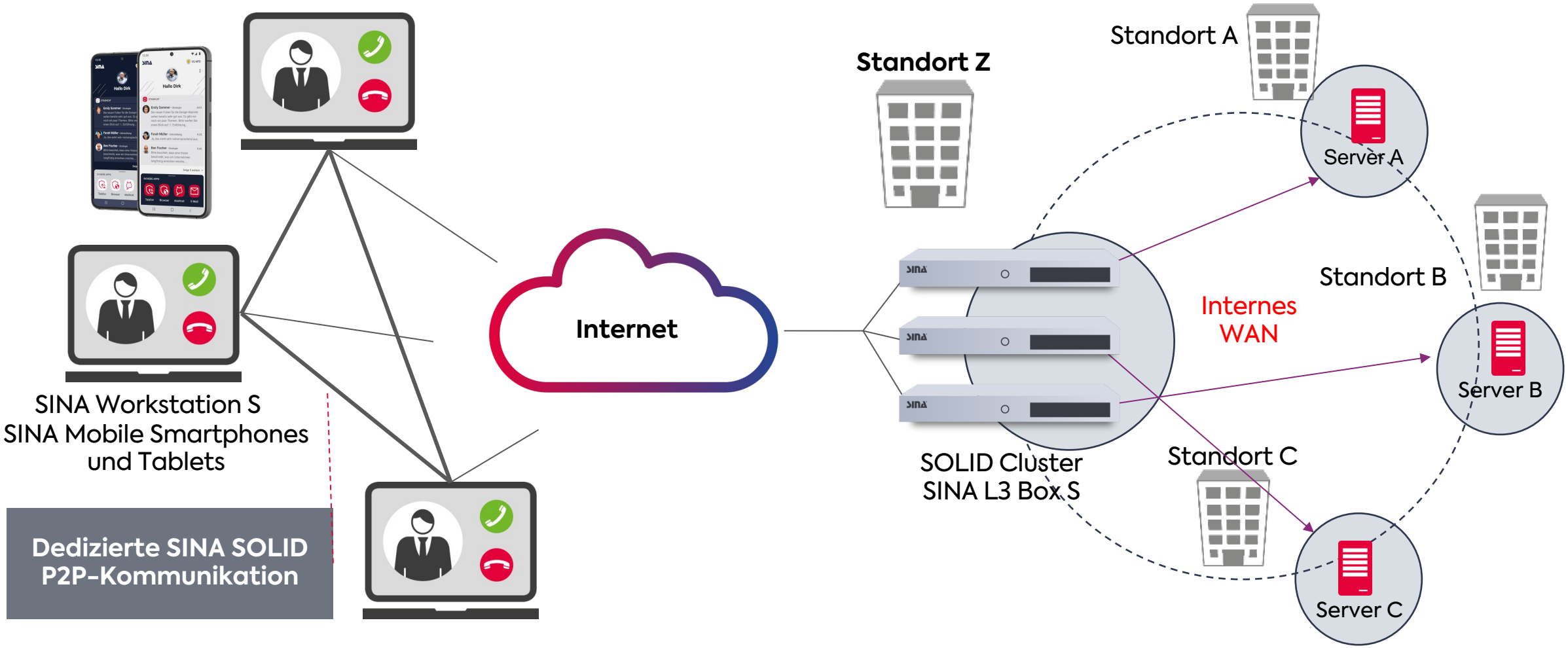
# SINA Clients sind integriert in SOLID-Ringe für ZTNA-Umsetzung dezentraler Server-Zugriffe




**Direkter Zugriff auf die Server an den Standorten über dezentrale SOLID Boxen**

ZTNA =
Zero Trust Network Access

# Ausblick: SINA Workstation S mit SOLID für dezentrale Client-to-Client-Kommunikation



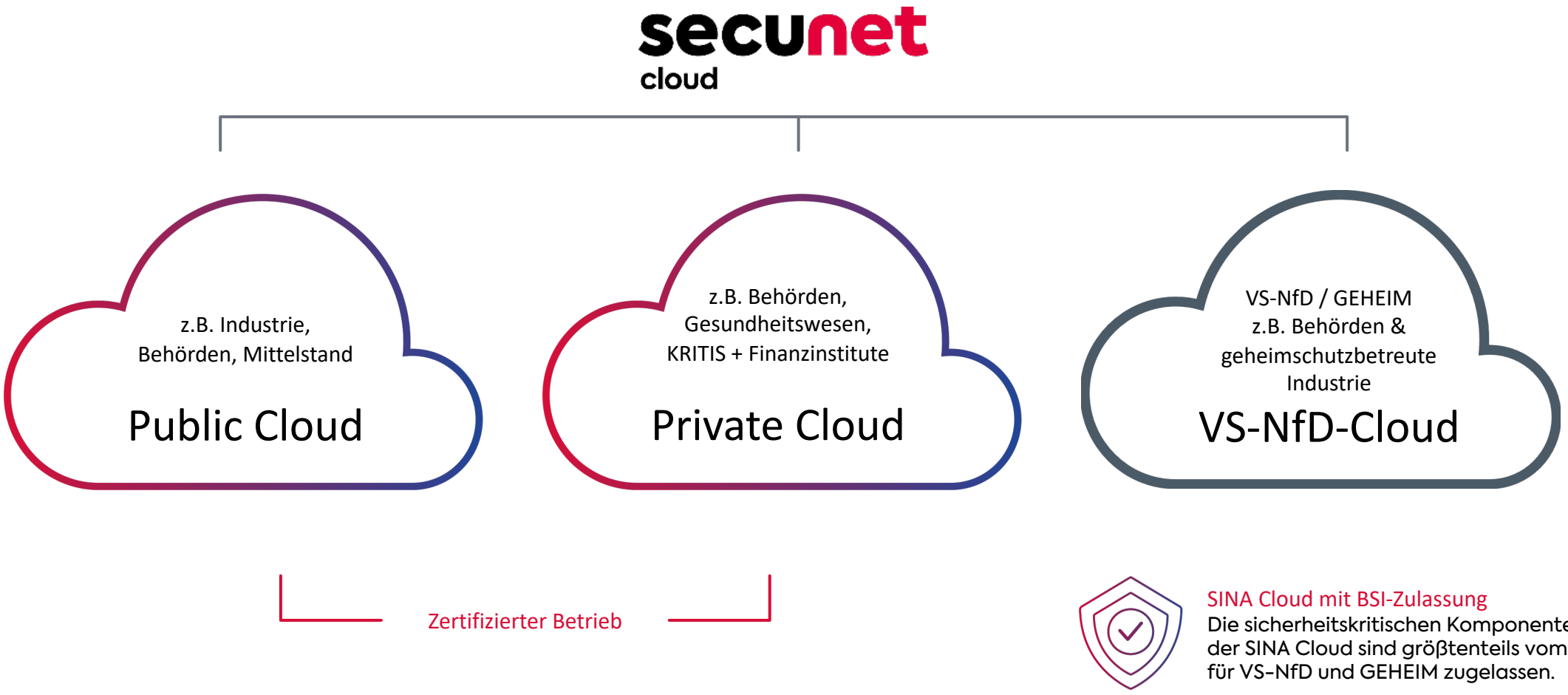
05

# Cloud-Ökosystem für die VS-Bearbeitung

# Unsere Vision für die Cloud

**Wir gestalten die digitale Zukunft und bieten Unternehmen, Behörden und regulierten Märkten eine sichere Cloud- und Container-Infrastruktur zum Schutz und zur Optimierung ihrer Arbeitsabläufe, Prozesse und Daten.**

# Eine Cloud für jedes Sicherheitsniveau




**SINA Cloud mit BSI-Zulassung**
Die sicherheitskritischen Komponenten der SINA Cloud sind größtenteils vom BSI für VS-NfD und GEHEIM zugelassen.

# SINA Cloud – Die sichere Cloud-Infrastrukturlösung

## **VS-IT-Systemverbund** - Gesamtheitliches IT-Sicherheitskonzept

Die sicherheitskritischen Komponenten der SINA Cloud sind größtenteils vom BSI für VS-NfD und GEHEIM zugelassen.

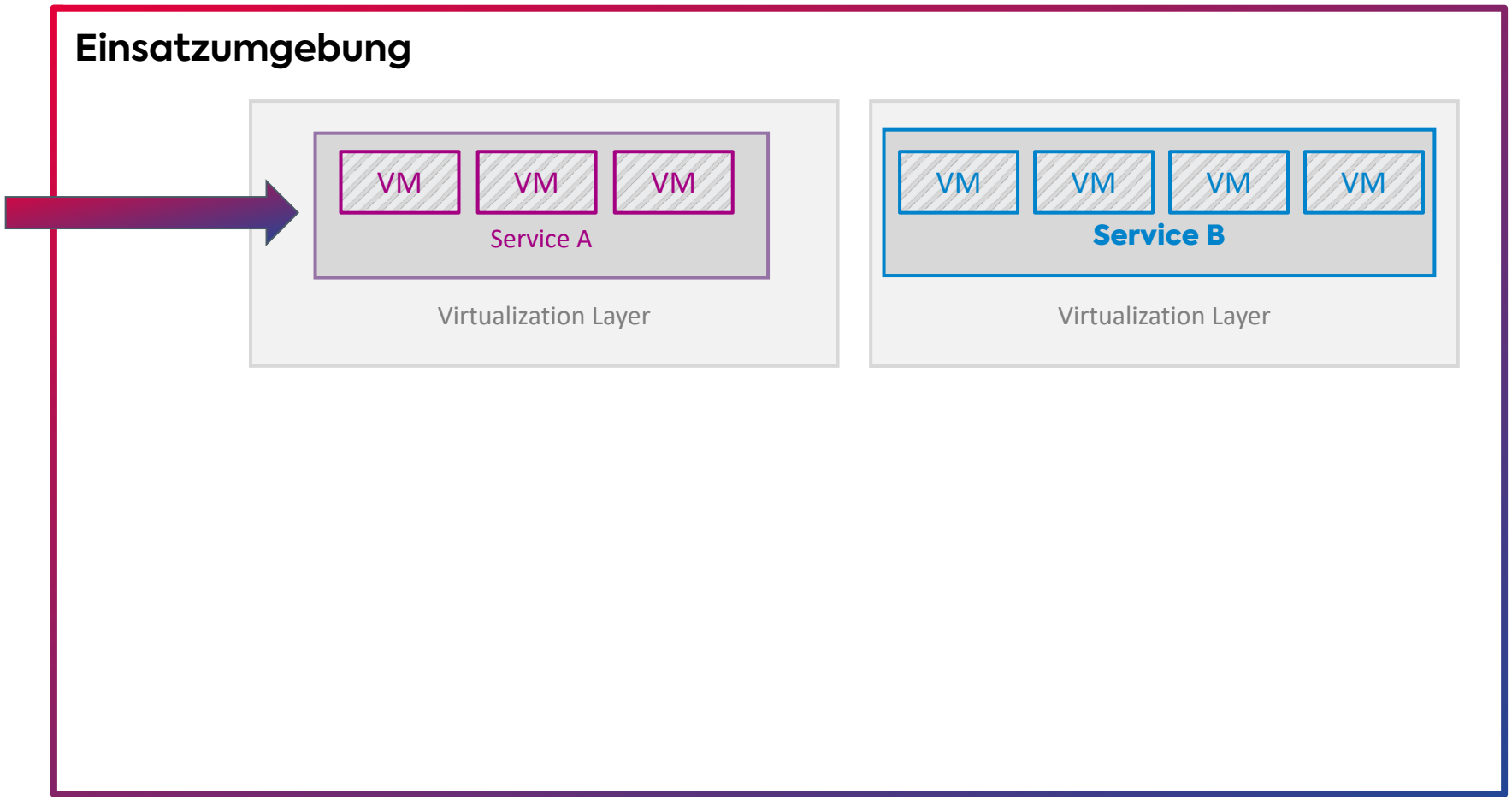
**Einsatzumgebung**

# SINA Cloud – Die sichere Cloud-Infrastrukturlösung

## **VS-IT-Systemverbund** - Gesamtheitliches IT-Sicherheitskonzept

Die sicherheitskritischen Komponenten der SINA Cloud sind größtenteils vom BSI für VS-NfD und GEHEIM zugelassen.

**Kundenindividuelles IT-Sicherheitskonzept**
Einfach umsetzbar - Leistung der secunet.



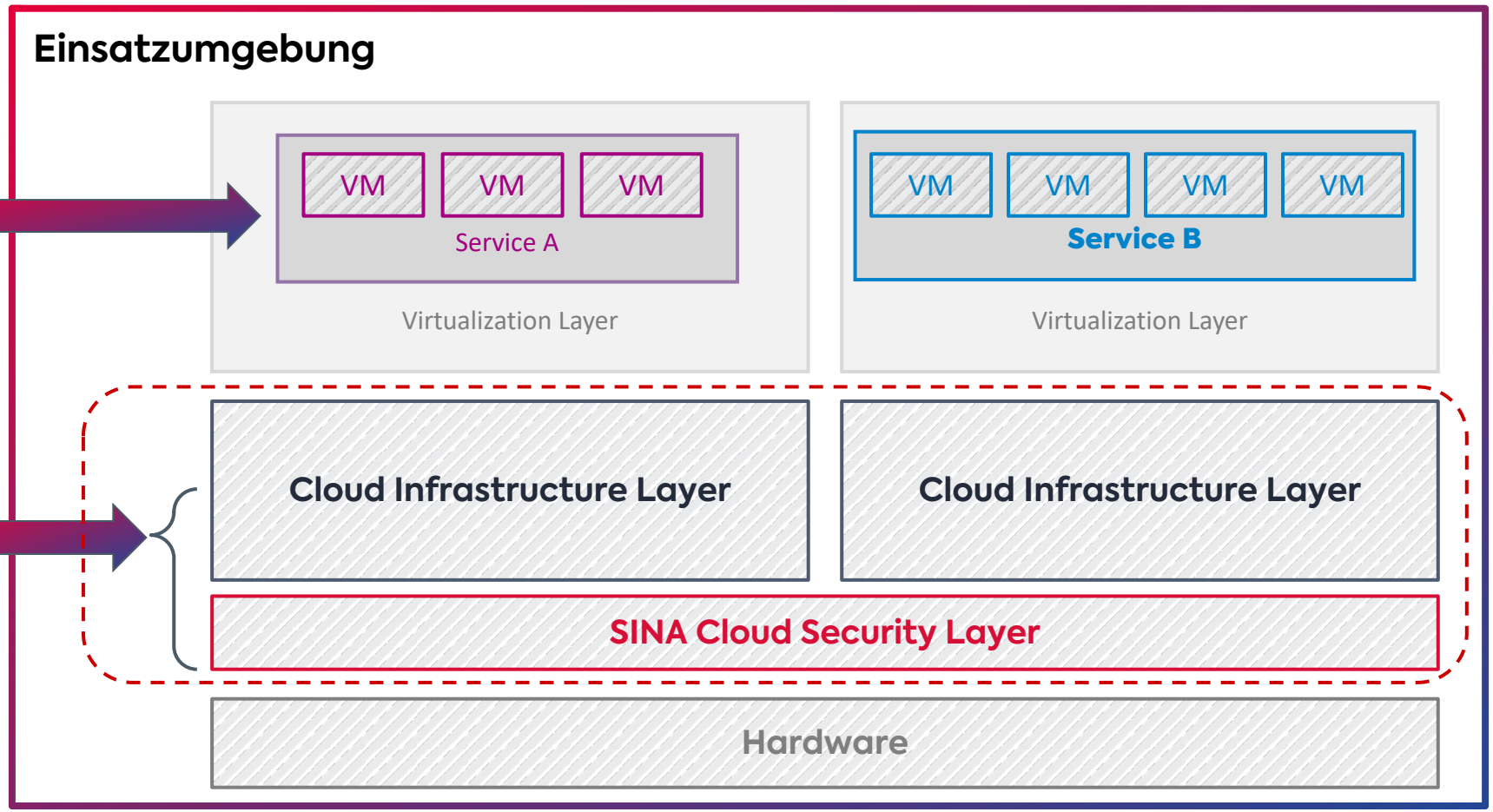
# SINA Cloud – Die sichere Cloud-Infrastrukturlösung

## **VS-IT-Systemverbund** - Gesamtheitliches IT-Sicherheitskonzept

Die sicherheitskritischen Komponenten der SINA Cloud sind größtenteils vom BSI für VS-NfD und GEHEIM zugelassen.

**Kundenindividuelles IT-Sicherheitskonzept**
Einfach umsetzbar - Leistung der secunet.

**Zulassung nach VSA für Sicherheitskomponenten**
Bestandteil der SINA Cloud.



# SINA Cloud – Die sichere Cloud-Infrastrukturlösung

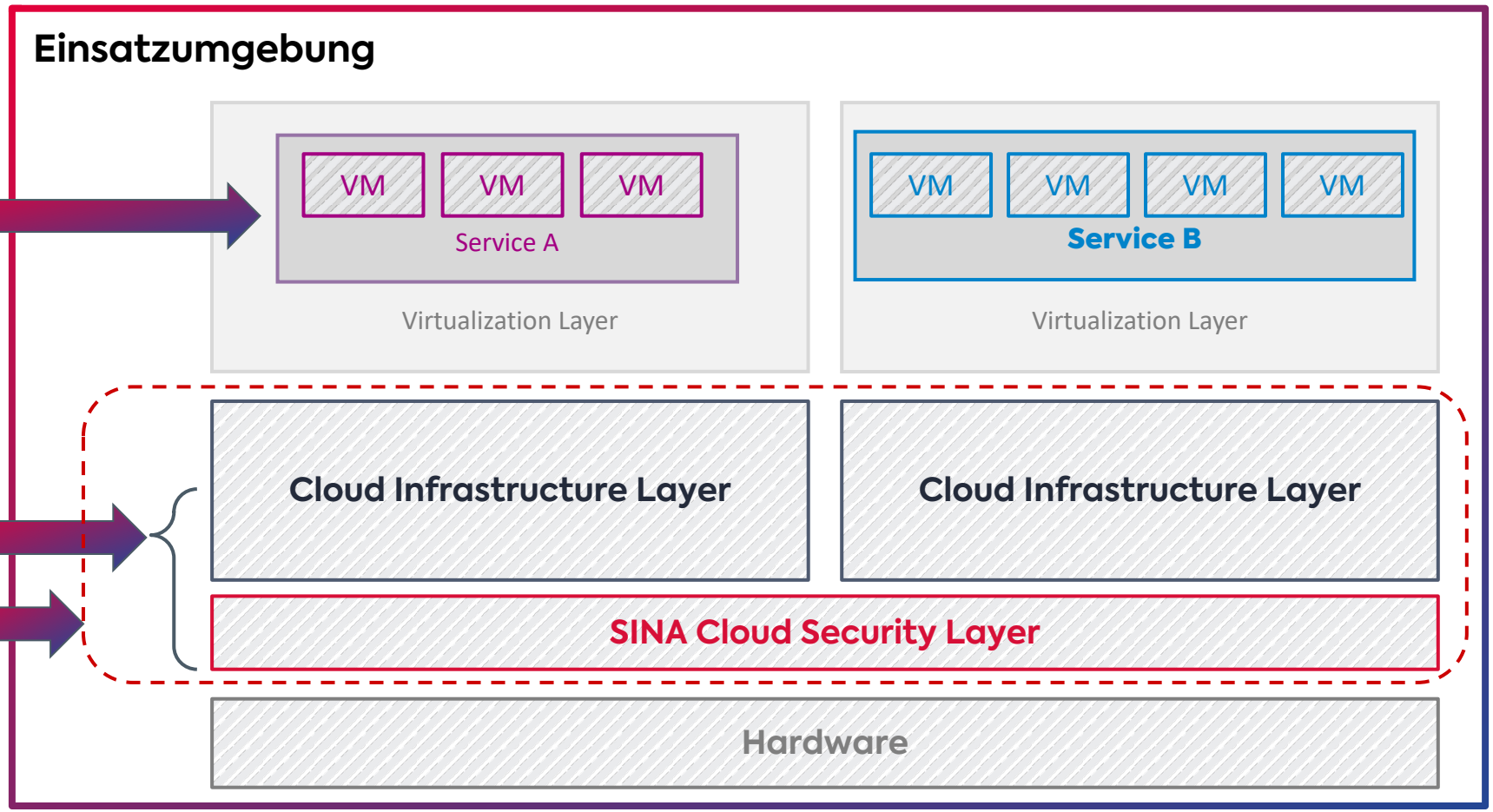
## VS-IT-Systemverbund - Gesamtheitliches IT-Sicherheitskonzept

Die sicherheitskritischen Komponenten der SINA Cloud sind größtenteils vom BSI für VS-NfD und GEHEIM zugelassen.

**Kundenindividuelles IT-Sicherheitskonzept**
Einfach umsetzbar - Leistung der secunet.

**Zulassung nach VSA für Sicherheitskomponenten**
Bestandteil der SINA Cloud.

**IT-Grundschutzprofil für SINA Cloud**
Bestandteil der SINA Cloud.



# SINA Cloud – Die sichere Cloud-Infrastrukturlösung

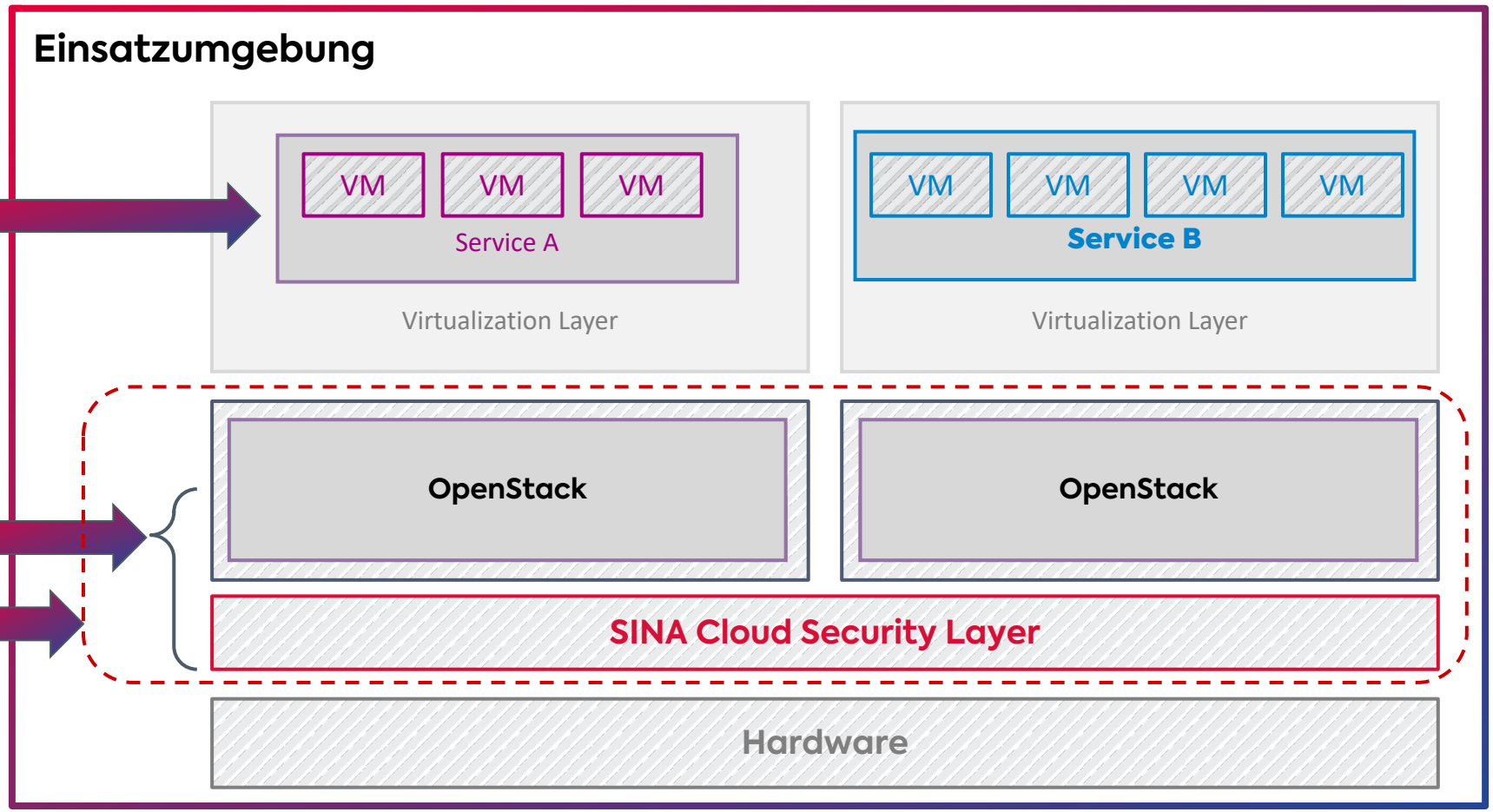
## **VS-IT-Systemverbund** - Gesamtheitliches IT-Sicherheitskonzept

Die sicherheitskritischen Komponenten der SINA Cloud sind größtenteils vom BSI für VS-NfD und GEHEIM zugelassen.

**Kundenindividuelles IT-Sicherheitskonzept**
Einfach umsetzbar - Leistung der secunet.

**Zulassung nach VSA für Sicherheitskomponenten**
Bestandteil der SINA Cloud.

**IT-Grundschutzprofil für SINA Cloud**
Bestandteil der SINA Cloud.



# SINA Cloud – Die sichere Cloud-Infrastrukturlösung

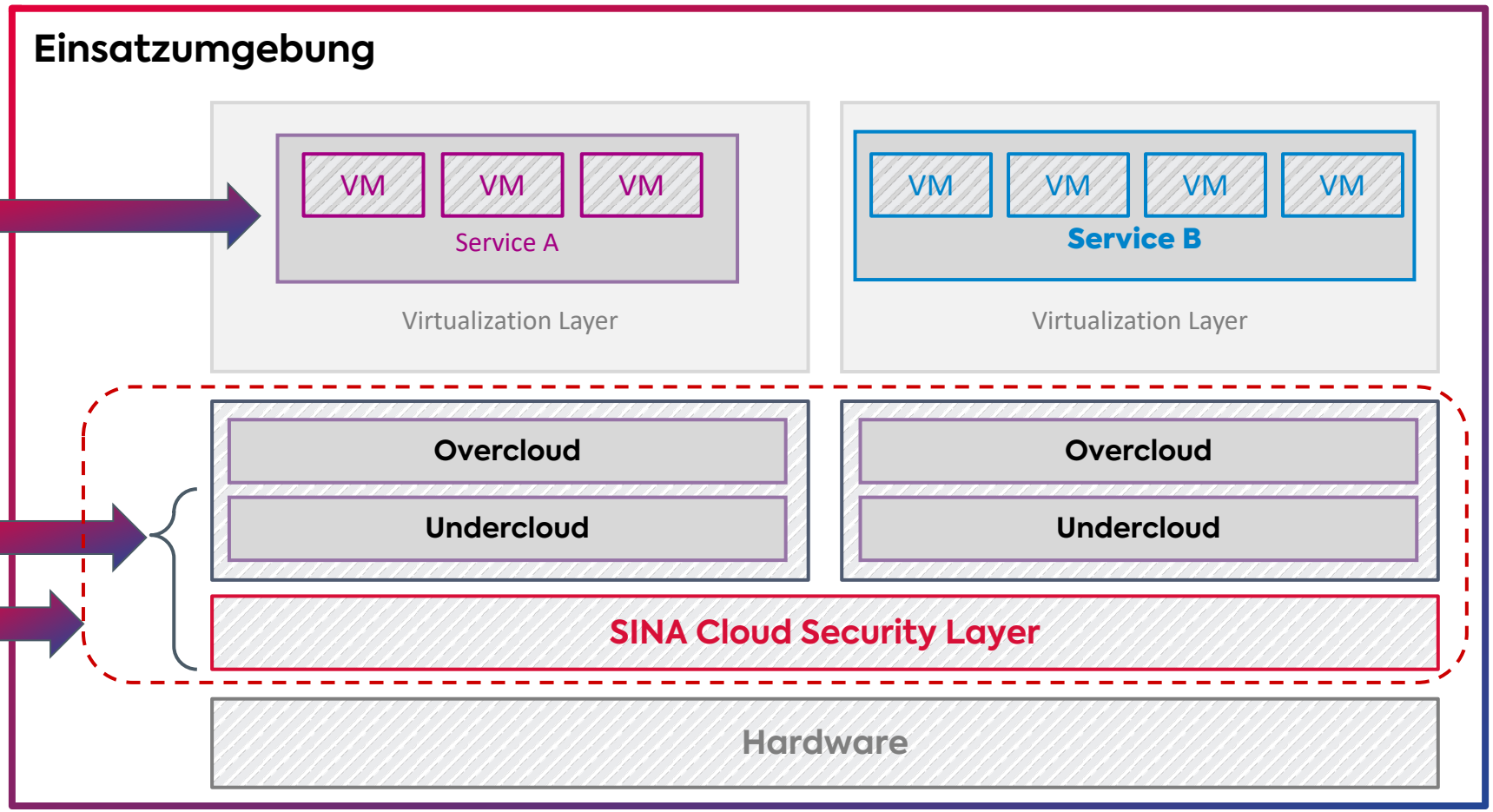
## VS-IT-Systemverbund - Gesamtheitliches IT-Sicherheitskonzept

Die sicherheitskritischen Komponenten der SINA Cloud sind größtenteils vom BSI für VS-NfD und GEHEIM zugelassen.

**Kundenindividuelles IT-Sicherheitskonzept**
Einfach umsetzbar - Leistung der secunet.

**Zulassung nach VSA für Sicherheitskomponenten**
Bestandteil der SINA Cloud.

**IT-Grundschutzprofil für SINA Cloud**
Bestandteil der SINA Cloud.



# SINA Cloud – Die sichere Cloud-Infrastrukturlösung

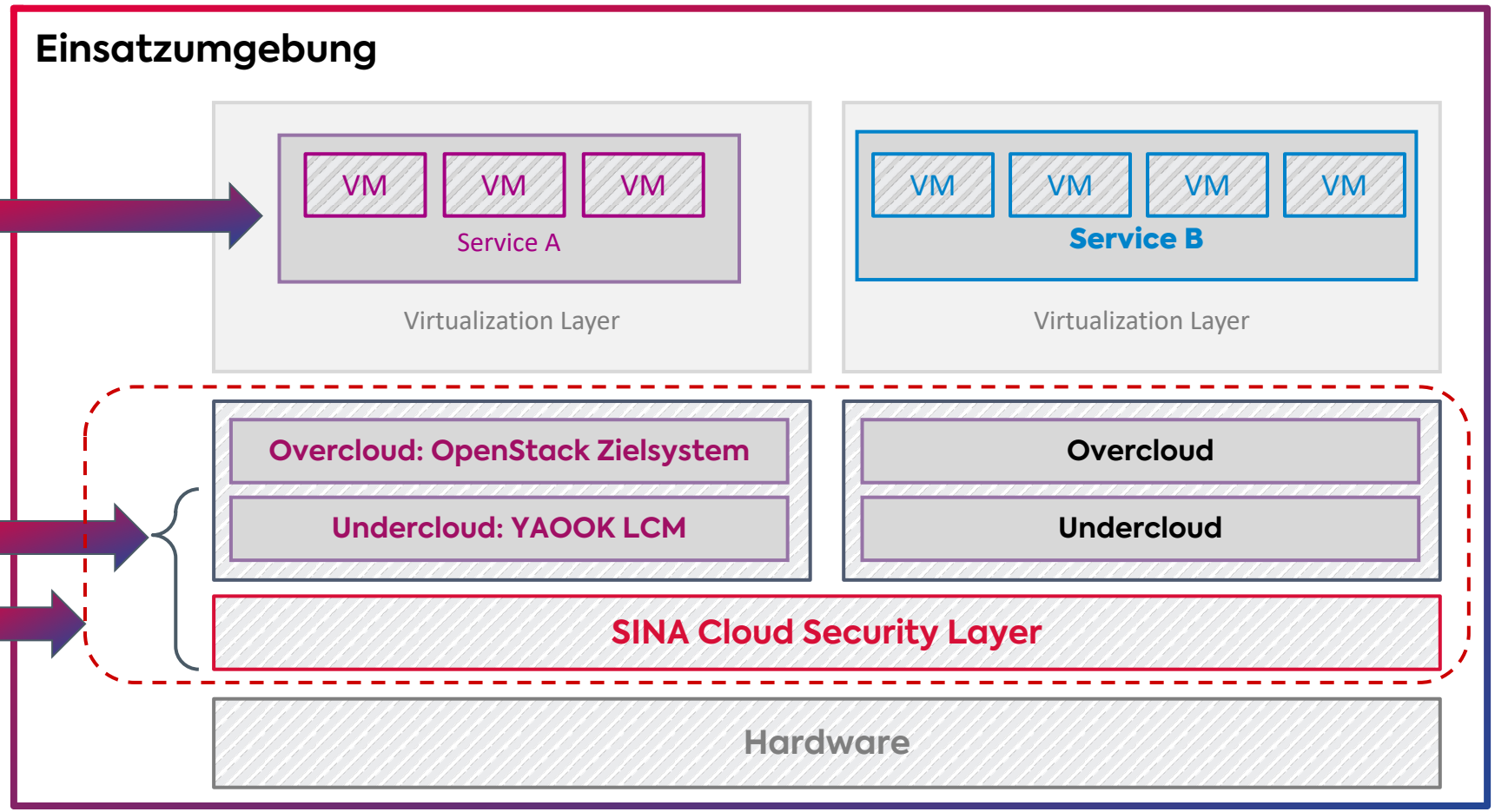
## VS-IT-Systemverbund - Gesamtheitliches IT-Sicherheitskonzept

Die sicherheitskritischen Komponenten der SINA Cloud sind größtenteils vom BSI für VS-NfD und GEHEIM zugelassen.

**Kundenindividuelles IT-Sicherheitskonzept**
Einfach umsetzbar - Leistung der secunet.

**Zulassung nach VSA für Sicherheitskomponenten**
Bestandteil der SINA Cloud.

**IT-Grundschutzprofil für SINA Cloud**
Bestandteil der SINA Cloud.



# SINA Cloud – Die sichere Cloud-Infrastrukturlösung

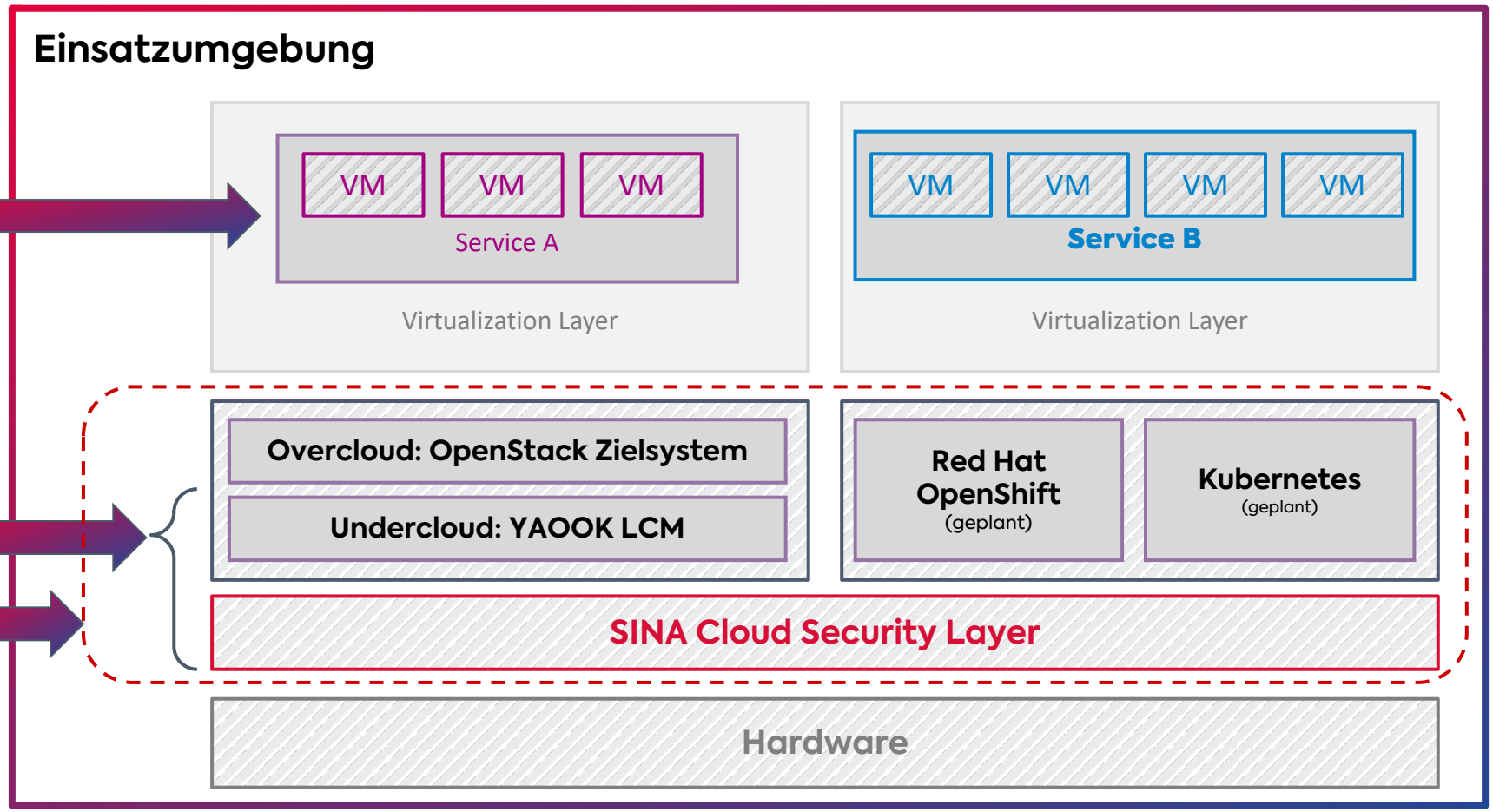
## **VS-IT-Systemverbund** - Gesamtheitliches IT-Sicherheitskonzept

Die sicherheitskritischen Komponenten der SINA Cloud sind größtenteils vom BSI für VS-NfD und GEHEIM zugelassen.

**Kundenindividuelles IT-Sicherheitskonzept**
Einfach umsetzbar - Leistung der secunet.

**Zulassung nach VSA für Sicherheitskomponenten**
Bestandteil der SINA Cloud.

**IT-Grundschutzprofil für SINA Cloud**
Bestandteil der SINA Cloud.



# Unser Angebot

SINA® Cloud


* Zulassung/Einsatzerlaubnis
** im Aufbau

# Wir haben die Anforderungen der VSA für die Cloud umgesetzt

## Verschlusssachen: Verarbeitung nur mit VS-IT zulässig nach §50 (1) VSA

### IT-Sicherheitsprodukte:

- benötigen Zulassung nach §51 (1) VSA
- übernehmen Sicherheitsfunktionen (z.B. Netzwerktrennung) aus §52 (1) VSA

### Einsatzerlaubnis (§51 (5) VSA):

- Sonderfall der Zulassung, falls keine Alternativen existieren oder nicht fristgerecht bereitgestellt werden können
- eingeschränkte Zulassung mit Restrisiken und Hinweisen zu Einsatz- und Betriebsbedingungen
- Einsatz erfordert Risikoanalyse nach § 8a VSA

# Wir haben die Anforderungen der VSA für die Cloud umgesetzt

## Verschlusssachen: Verarbeitung nur mit VS-IT zulässig nach §50 (1) VSA

### IT-Sicherheitsprodukte:

- benötigen Zulassung nach §51 (1) VSA
- übernehmen Sicherheitsfunktionen (z.B. Netzwerktrennung) aus §52 (1) VSA

### Einsatzerlaubnis (§51 (5) VSA):

- Sonderfall der Zulassung, falls keine Alternativen existieren oder nicht fristgerecht bereitgestellt werden können
- eingeschränkte Zulassung mit Restrisiken und Hinweisen zu Einsatz- und Betriebsbedingungen
- Einsatz erfordert Risikoanalyse nach § 8a VSA

**SINA Cloud** enthält alle notwendigen zugelassenen Komponenten

**secunet** unterstützt beim Freigabeprozess für on-premises Deployments

# Ziel: Ein voll umfassendes VS-NfD-Ökosystem

## Querschnittsdienste

- Office-Lösungen
- Collaboration
- Dateiablage/-sharing
- Datenbanken
- etc.

## Fachverfahren

- Spezial-Lösungen

## secunet Lösungen

- SINA Boxen/Workstations
- SINA Mobile
- SINA Workflow
- usw.

05

# Zusammenfassung und Ausblick

# Mehrwerte im VS-Client-Netz-Cloud Ökosystem

## Integrierte Lösungen für VS-Anforderungsprofile

- Erspart äußerst aufwändige Freigabeprozesse für selbst konzipierte Umgebungen und Lösungen
- Beschleunigung durch Einsatz BSI-zugelassener und integrierter Produkte und Komponenten
- Ready-to-use Clients in vielen Formfaktoren
- Resiliente, effizient skalierbare Client-Zugangscluster und WAN-Kryptolösungen
- Unterstützung dezentraler Kommunikation für Clients, Netze und in die Cloud

## Freiheit und Effizienz für Cloud-Betreiber und Nutzer

- Verfügbar für on-premises Einsatz und perspektivisch als Managed Service der secunet
- Open Source als Grundlage – ergänzt um eine zertifizierte Public Cloud
  - C5, IT-Grundschutz und Sovereign Cloud Stack (SCS) Zertifizierung
- Technologie- und Anbieter-Offenheit: Entkoppelung von Sicherheitskomponenten und Cloud-Betriebssoftware
- Kryptographische Mandantentrennung bei optimaler Nutzung vorhandener RZ-Hardware
- Integriertes, automatisiertes Life-Cycle-Management

# SINA Portfolio

**Alles aus einer Hand**

## Wir bieten:

### Hochsichere Endgeräte


SINA Solid

### Hochsichere Transportelemente

### Sichere Backend Infrastruktur



SINA® Cloud

# Zeit für Fragen

Immer gern. Wir sind für Sie da.

Michael Hohensee
SINA Cloud Vertrieb
SysEleven GmbH

Peter Rost
Geschäftsentwicklung
secunet Security Networks AG


secunet

# Security Layer


## SINA Cloud Security Management

- Verwaltet Sicherheitsdomänen
- Sorgt für initialen Start von Sicherheitsdomänen
- Automatisierbare Schnittstelle für Cloud Infrastructure Layer LCM

## Netzwerkverschlüsselung

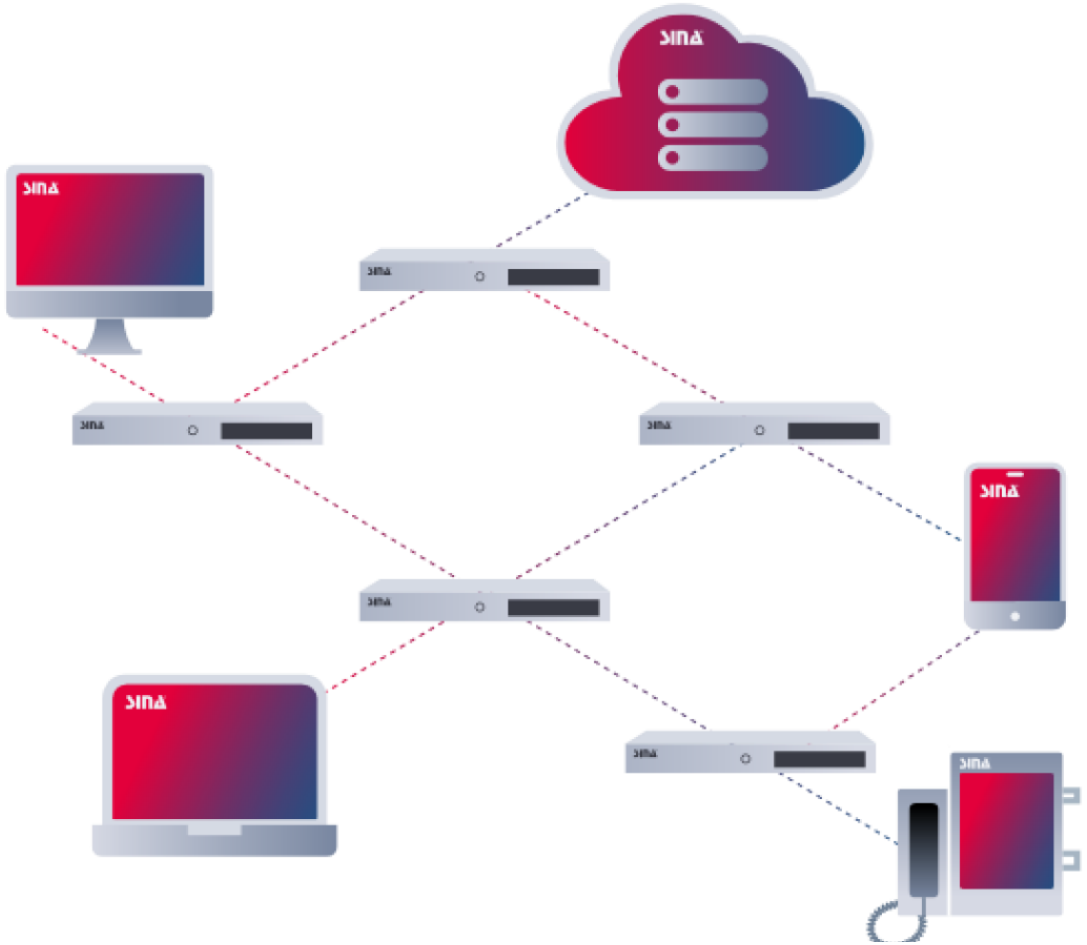
- Netzwerktechnische Trennung von Sicherheitsdomänen
- DPUs verschlüsseln mit dem HEAT Protokoll Netzwerkverkehr

## Speicherverschlüsselung

- Verschlüsselung von Data-at-Rest
  - Volumes
  - Disks
  - Images*
- Zentraler und sicherer Speicher für alle Sicherheitsdomänen

*eingeschränkt

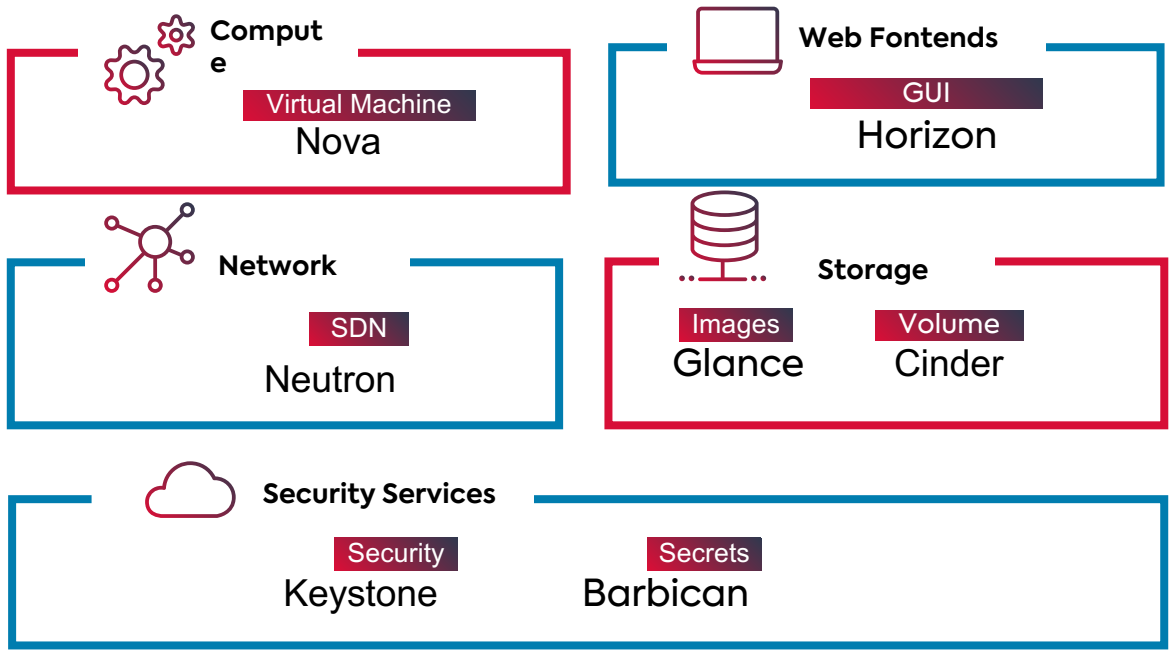
# SINA Cloud –
# Souverän gedacht.
# Sicher gemacht.



# Serviceübersicht von OpenStack

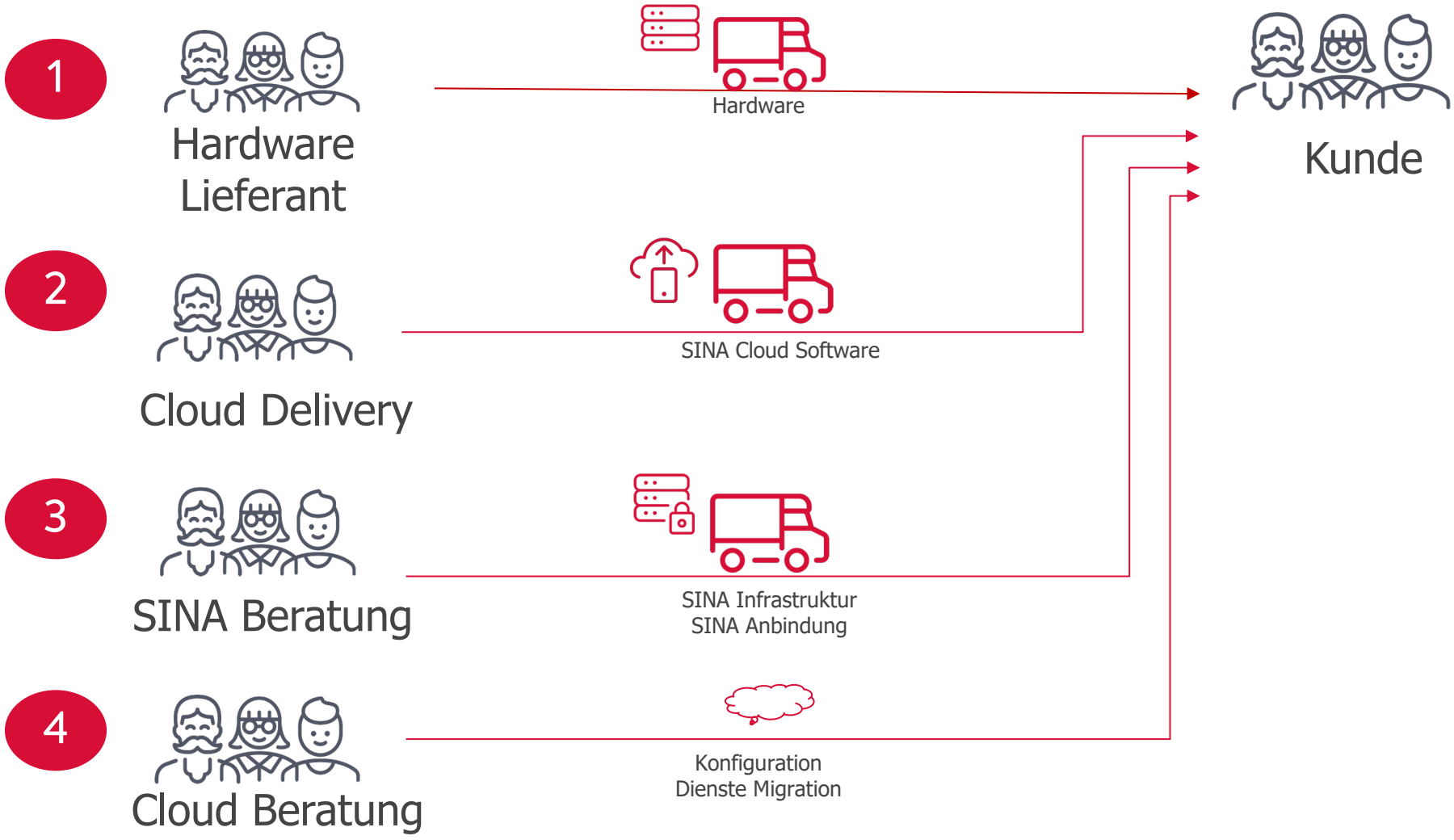
## YAOOK OpenStack Komponenten

- Nova (Compute Service)
- Neutron (Networking)
- Cinder (Block Storage)
- Keystone (Identity Service)
- Glance (Image Service)
- Barbican (Key Management Service)
- Horizon (Web Frontend)



# Rollen bei der Inbetriebnahme

## SINA Cloud OnPrem






secunet SysEleven

# Aufgaben bei der Software-Inbetriebnahme

Cloud Delivery

**Software-Inbetriebnahme (einmalig)**

- Netzwerk hochziehen
- Storage bereitstellen
- Installation der SINA Cloud Images
- Enrollment von VS-Komponenten
- Security Layer hochziehen
- ggf. erste Security Domain bereitstellen

Kunde
Beratung (unterstützend)

**Software-Inbetriebnahme (einmalig)**

- Anbindung in Einsatzumgebung*

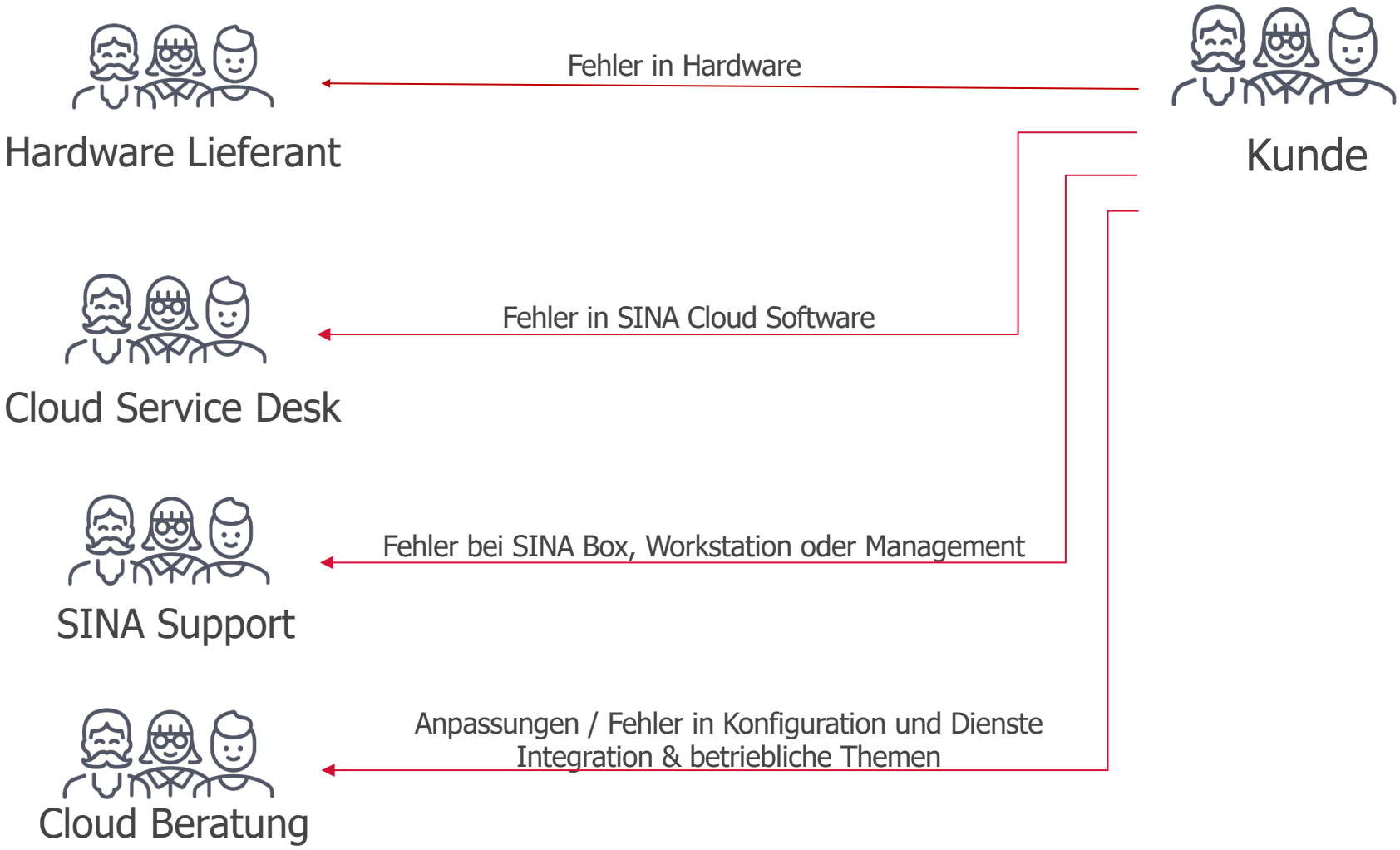
**Software-Inbetriebnahme (wiederkehrend)**

- Enrollment von DPU/Cloud Encrypter
- Security Domain bereitstellen und konfigurieren
- Dienste integrieren und konfigurieren
- Updates der SINA Cloud Images durchführen

* Bei SINA Box durch SINA Beratung

# Rollen im Support

## SINA Cloud OnPrem






secunet SysEleven