

# SCION INTERNET



SICHER, ZUVERLÄSSIG, FLEXIBEL UND DANK UNSEREM MANAGED SERVICE AUCH EXTREM WIRTSCHAFTLICH.

Stefan Pfiffner, Head of Security Prevention Solutions, InfoGuard AG

# INTRODUCTION | *PROBLEMSTELLUNG*

## SCION (SCALABILITY, CONTROL, AND ISOLATION ON NEXT-GENERATION NETWORKS)

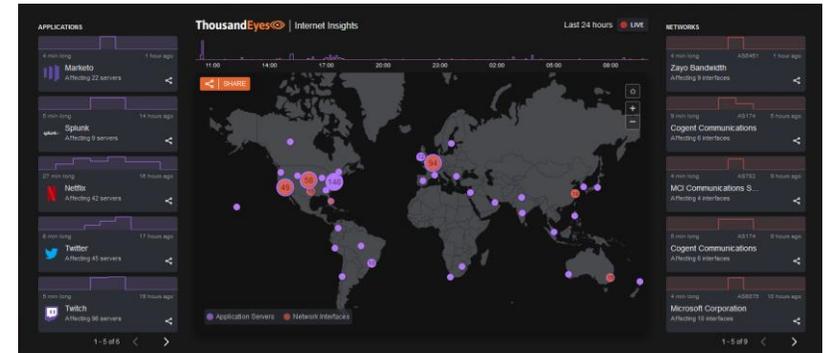
### ➤ Das Internet wurde nicht als sicheres Netzwerk konzipiert

- BGP Hijacking
- BGP Leaking
- DDoS
- Spoofing
- ...

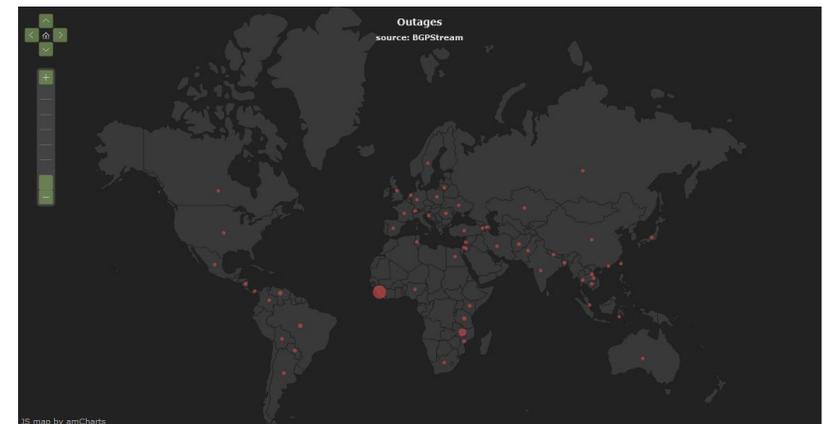
### ➤ Limitierte Transparenz

### ➤ Limitierte Kontrolle

### ➤ Schlechte Skalierbarkeit



Quelle: <https://www.thousandeyes.com/outages/> | 02.06.2023



Quelle: <https://bgpstream.crosswork.cisco.com/> | 02.06.2023 | ~6500 Ausfälle

# INTRODUCTION | WAS IST SCION?

## SCION

SCiON wurde in mehr als 10 Jahren Forschungsarbeit an der ETH Zürich entwickelt und kombiniert die Sicherheit und Zuverlässigkeit privater Netzwerke mit der Flexibilität des Internets. Die SCION-Architektur überwindet die Einschränkungen des derzeitigen BGP-basierten Internets, wodurch es volle Kontrolle, Sicherheit, Verfügbarkeit und Leistung bietet.

### ➤ Path Control

- Der Sender entscheidet über den Pfad



### ➤ Multipathing

- Zuverlässigkeit und Performance



### ➤ Security by Design

- Verifizierte Netzwerk Informationen



Quelle: <https://www.anapaya.net/hubfs/diagram-scion-network-%5Bv2.0%5D-1.svg>

## ➤ Isolation Domains (ISDs)

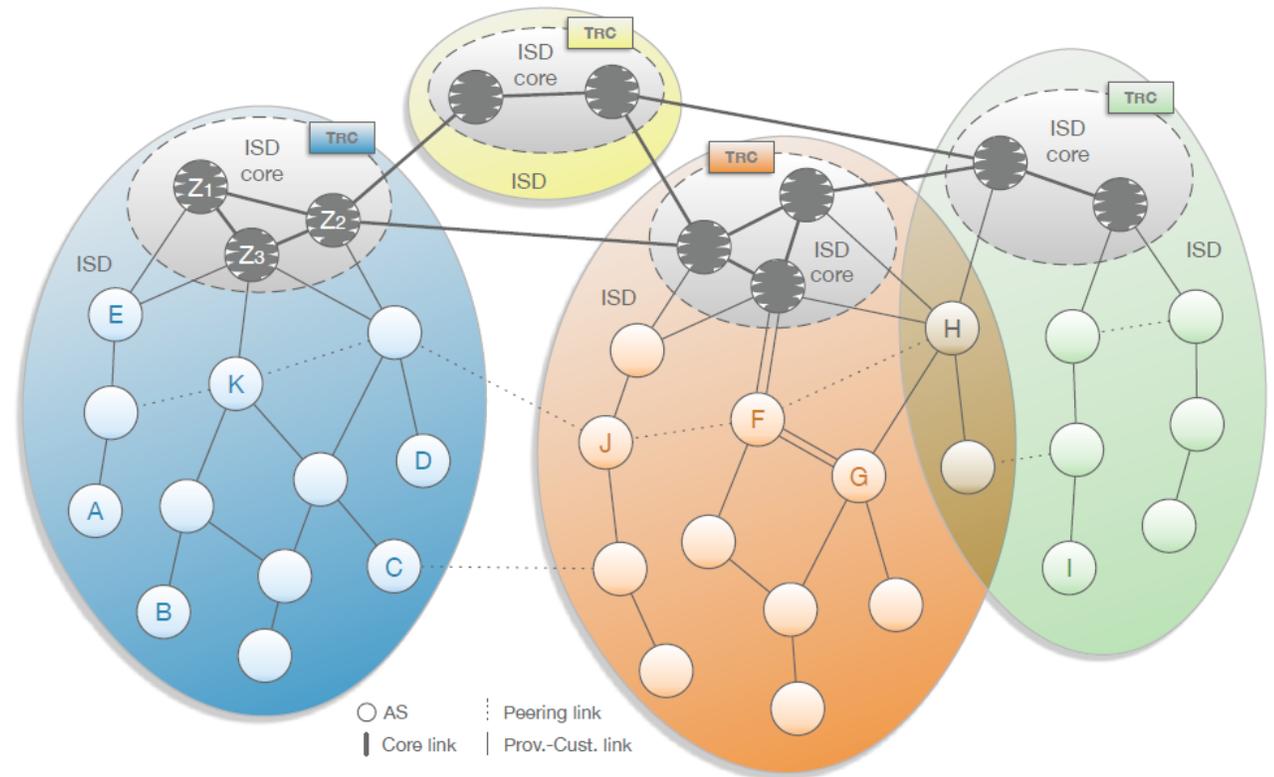
- Logische Gruppierung von ASes
- Isoliert die Routing Plane
- Definiert die TRC

## ➤ Control Plane

- Erstellt und verwaltet Pfad Segmente
- Kryptografische Absicherung des Routings

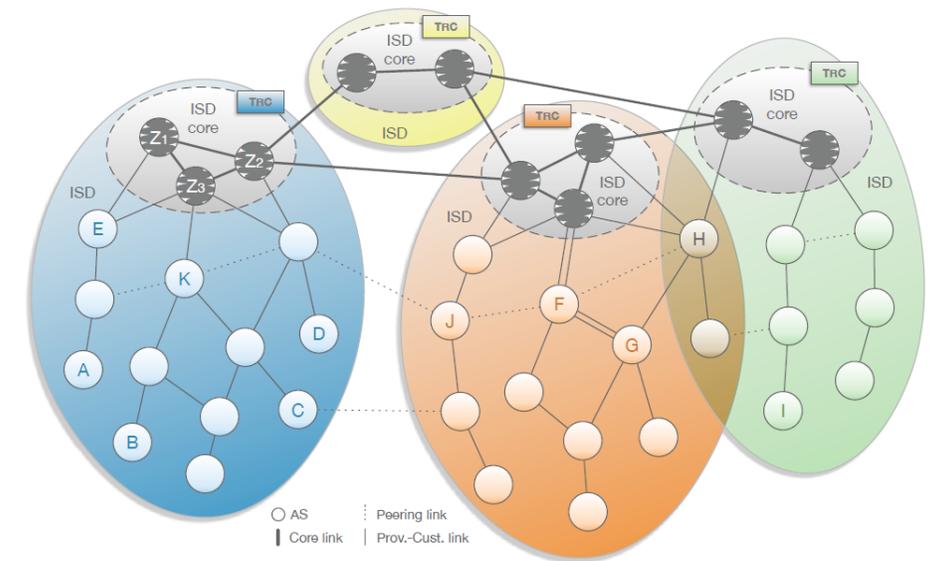
## ➤ Data Plane

- Paket Forwarding



Quelle: <https://scion-architecture.net/pdf/SCION-book.pdf>

- Das SCiON Netzwerk besteht aus untereinander verbundenen ISDs
- Eine ISD besteht aus untereinander verbundenen AS
- Jede ISD definiert eine TRC
- Jedes AS benötigt ein Zertifikat um Mitglied einer ISD zu werden



Quelle: <https://scion-architecture.net/pdf/SCION-book.pdf>

## ➤ Control Services

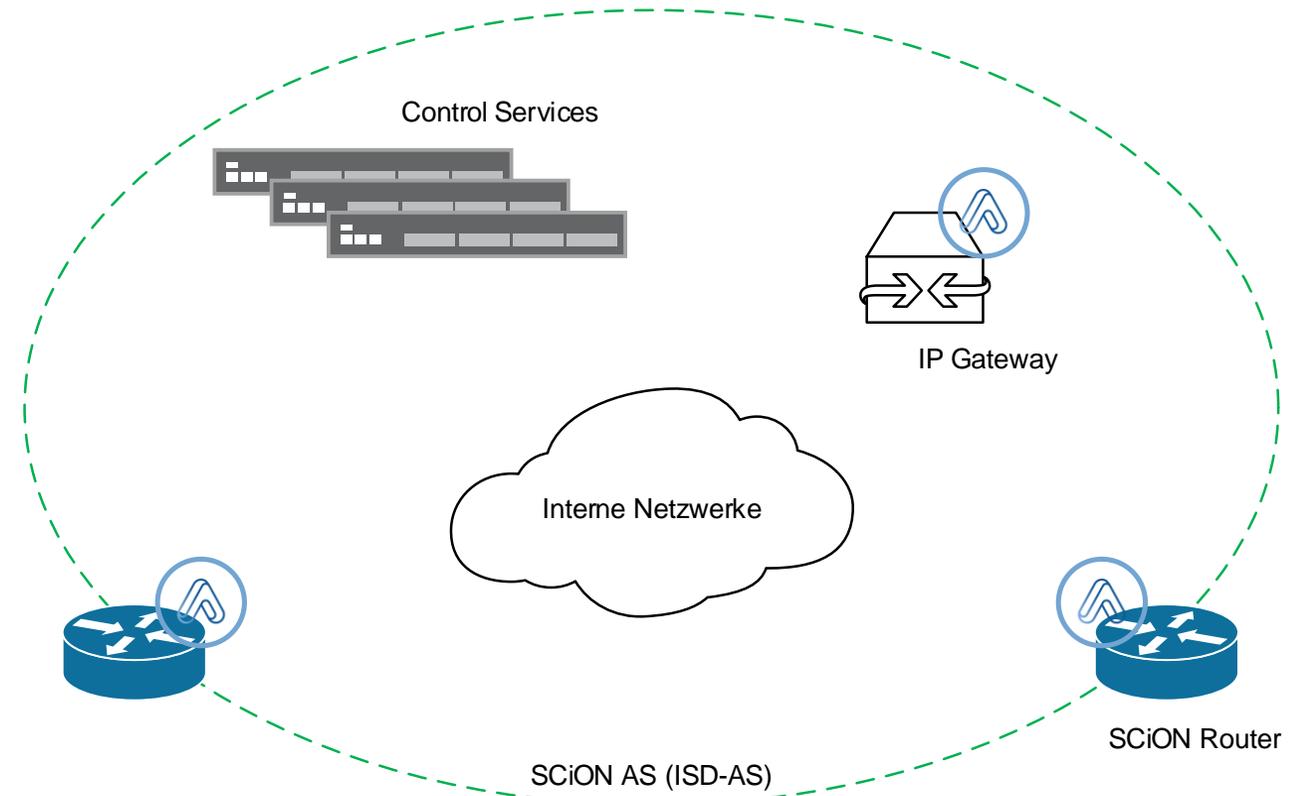
- Control Plane

## ➤ SCiON Routers

- Data Plane

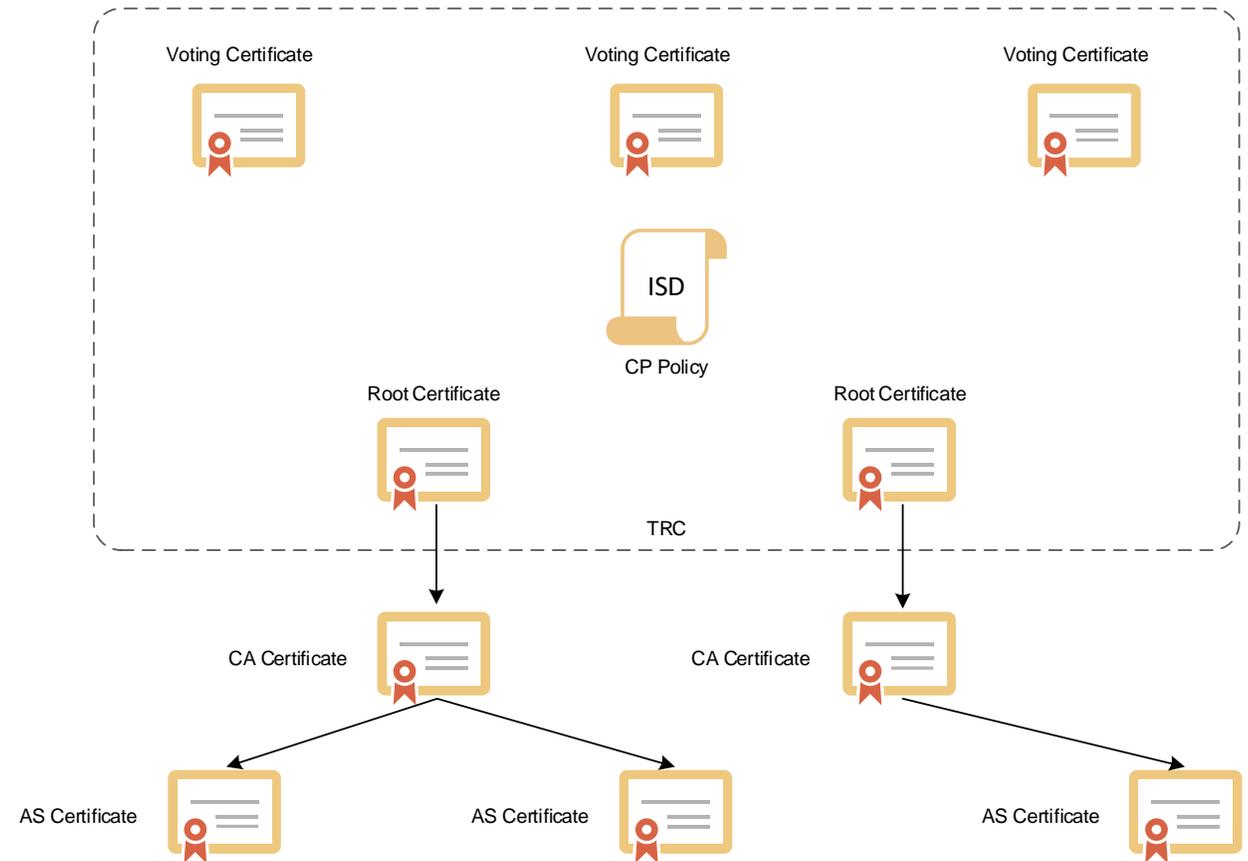
## ➤ SCiON IP Gateways

## ➤ Interne Netzwerke



# INTRODUCTION | TRUST ROOT CONFIGURATION SCION

- **Spezifiziert die primären ASes für die ISD**
- **Root of Trust für die ISD**
- **Enthält die Root Zertifikate für die ISD**
- **Enthält die ISD Control Plane Policy**
  - Voting Quorum
  - Core ASes





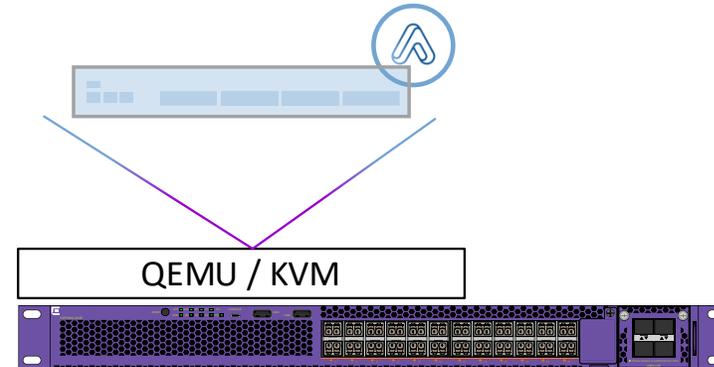
**INFOGUARD  
SCION EDGE  
DEVICE SERVICE**

# SERVICE | ÜBERSICHT

## INFOGUARD SCION EDGE DEVICE

### ➤ Powered by Extreme Networks

- Integrated Application Hosting (IAH)
- QEMU / KVM Hypervisor
- Benötigt keinen komplexen Server Setup



### ➤ In Zusammenarbeit mit

- Anapaya
- Extreme Networks
- InfoGuard AG



# SERVICE | DESIGN

## SCION EDGE DEVICE

### ➤ Single Access

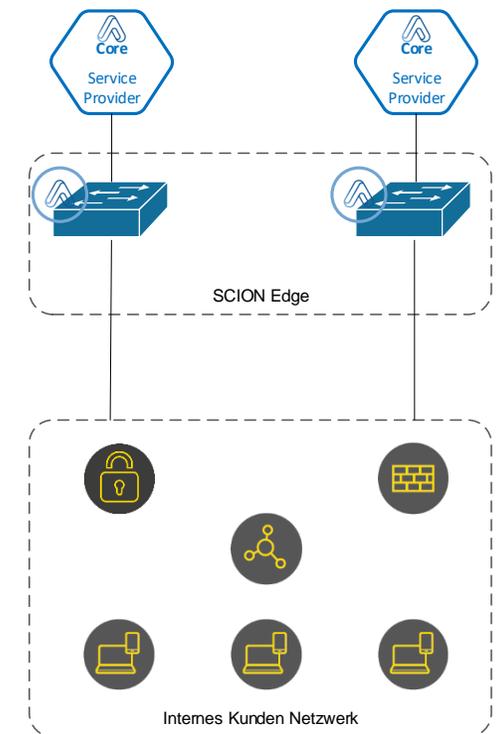
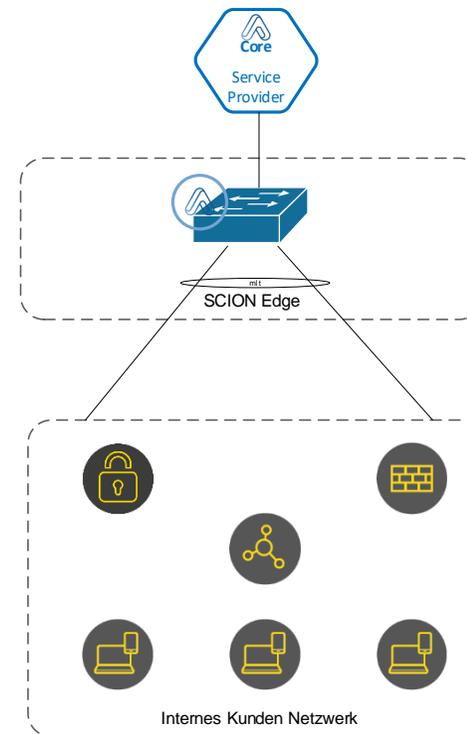
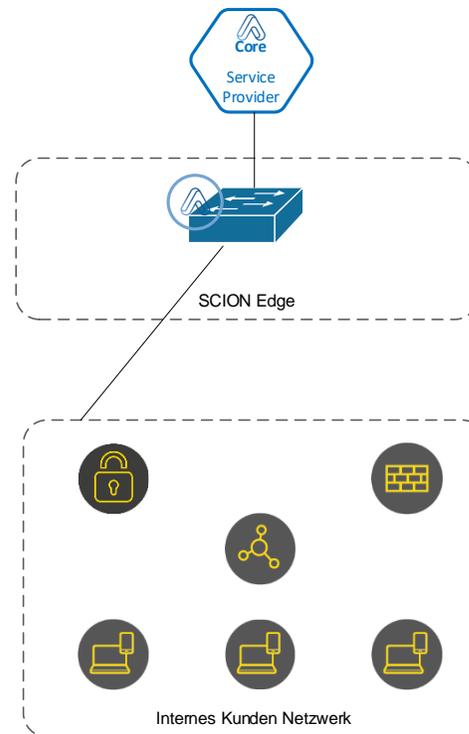
- Single LAN Anbindung
- Single ISP
- Single Edge Device

### ➤ Single+ Access

- Redundante LAN Anbindung
- Single ISP
- Single Edge Device

### ➤ Redundant Access

- Redundante Anbindung
- Mehrere ISPs
- Redundante Edge Devices



# SERVICE | DESIGN

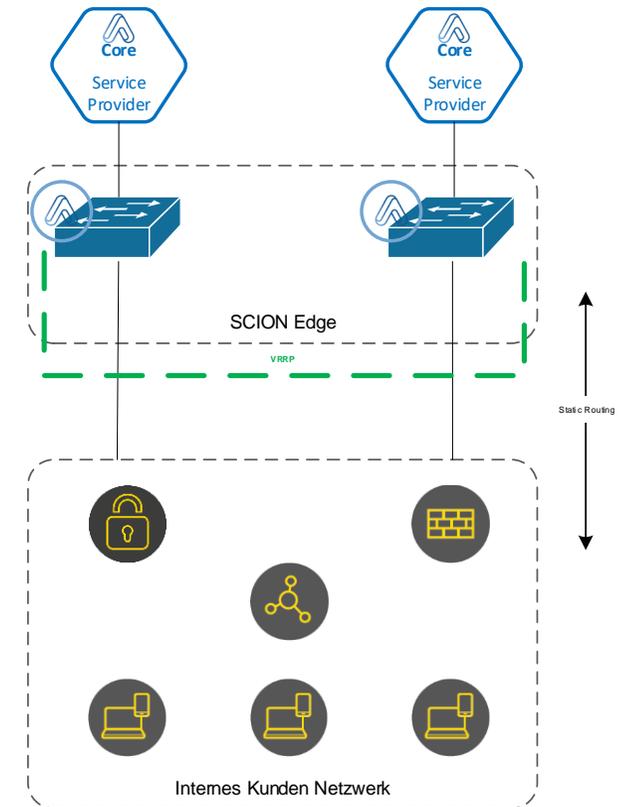
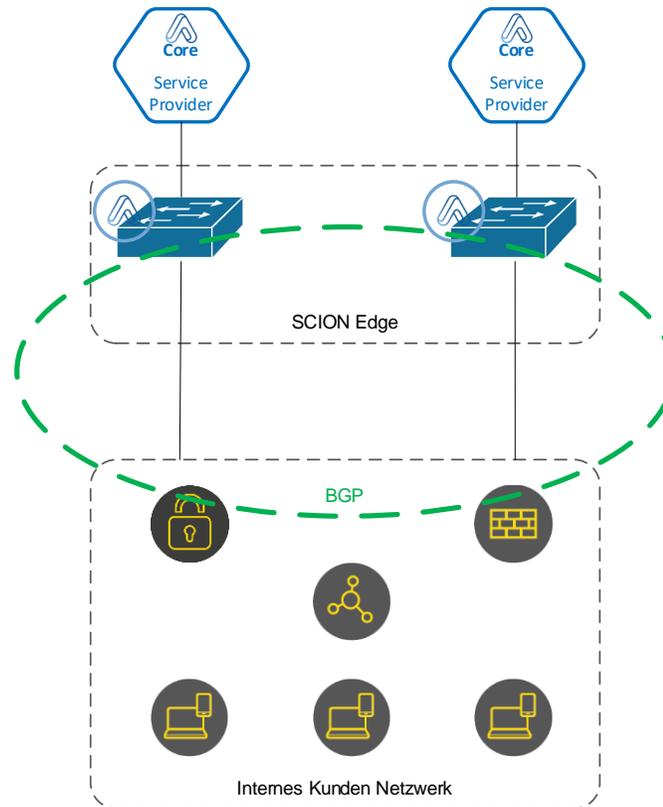
## SCION EDGE DEVICE

### ➤ Statisches Routing

- VRRP

### ➤ Dynamisches Routing

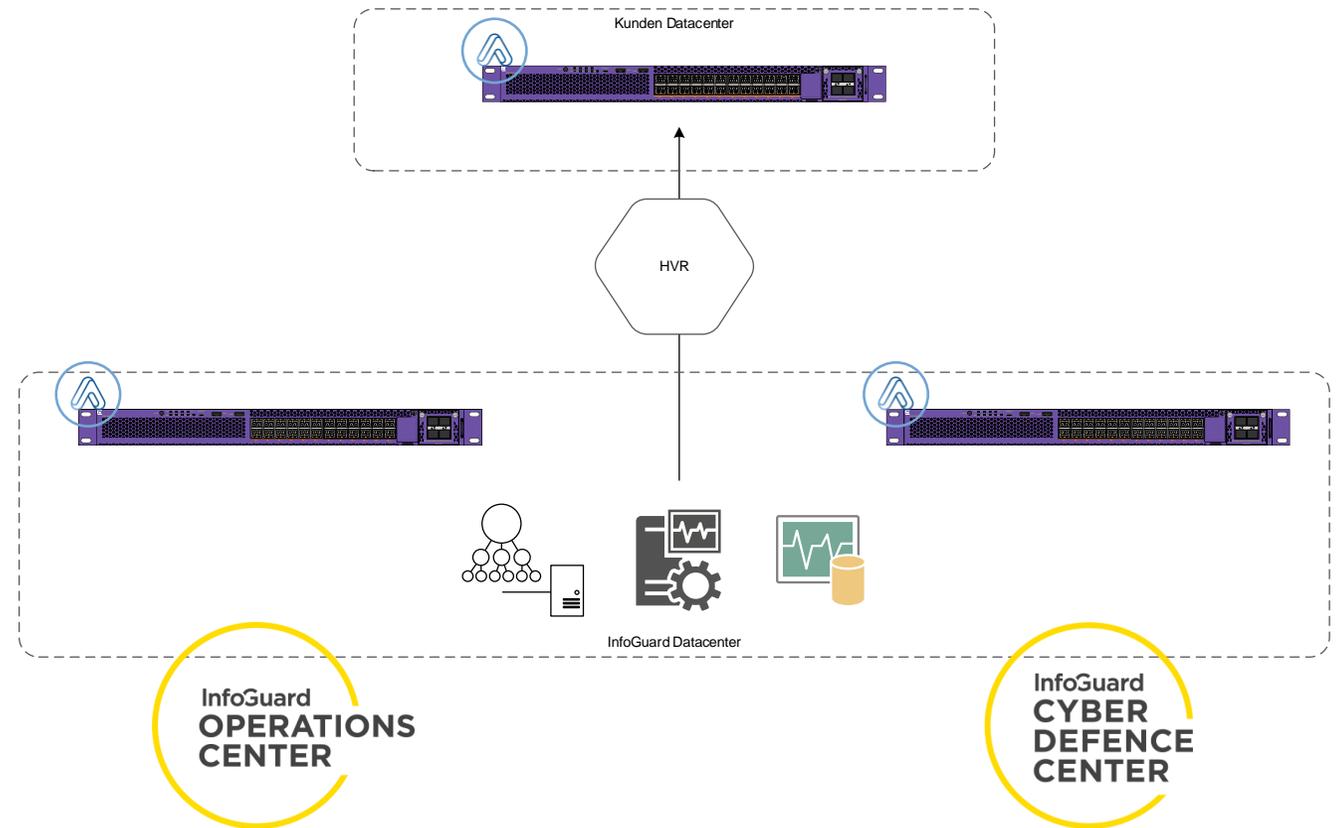
- BGP



# SERVICE | VORTEILE SCION EDGE DEVICE

## ➤ Full Managed 7x24

- Incident / Problem / Change Management
- Proaktive Serviceinformationen
- Proaktives Systemmanagement
- Inkl. Health Monitoring
- Inkl. Security Monitoring



# WEITERE INFORMATIONEN ZUM SERVICE



Stefan Pfiffner

[stefan.pfiffner@infoguard.ch](mailto:stefan.pfiffner@infoguard.ch)

Wie und wo erhalten Sie weitere Informationen zu diesem Thema?



<https://www.infoguard.ch/de/hvr-managed-scion-edge>



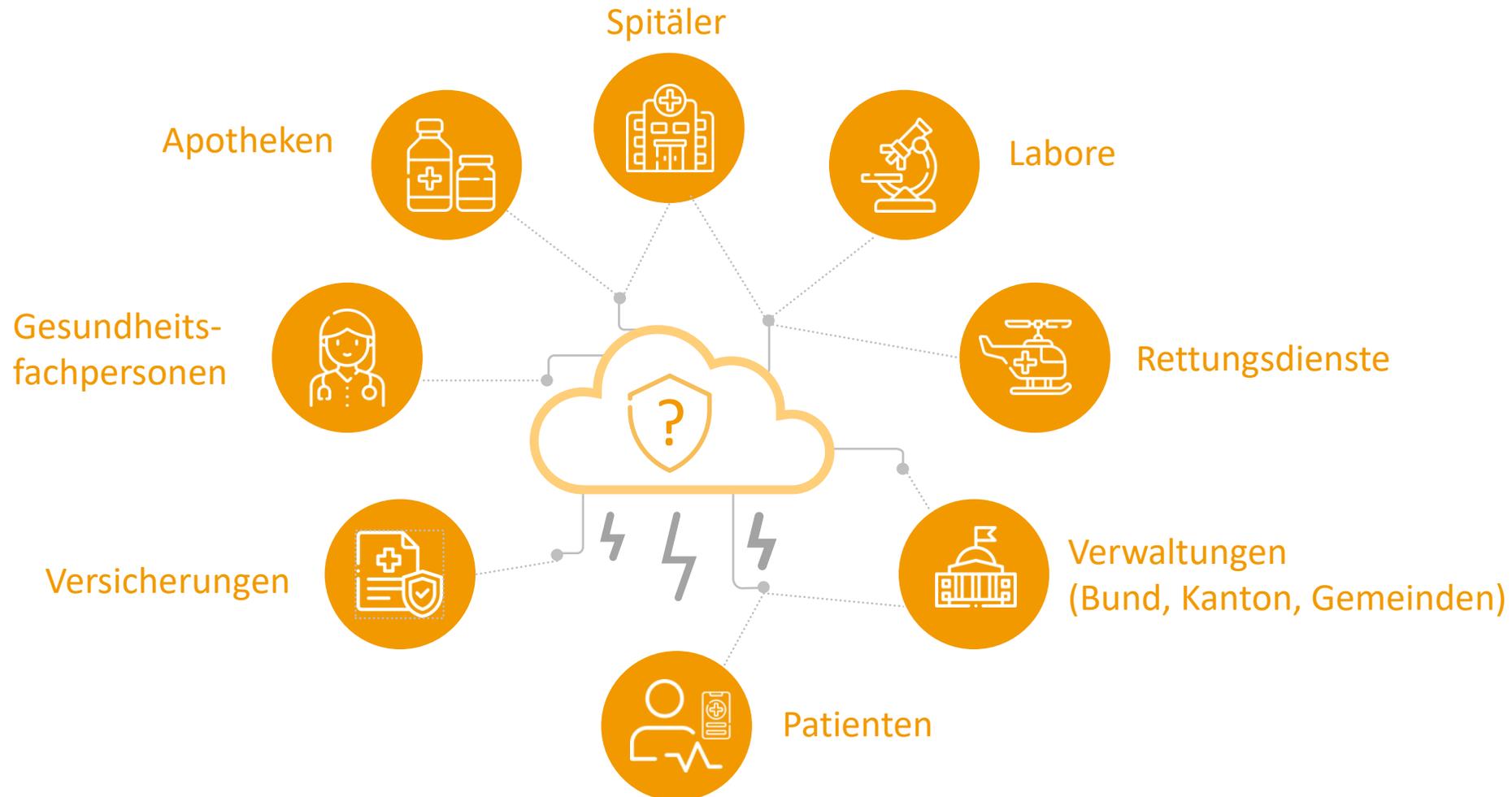


# HIN Vertrauensraum

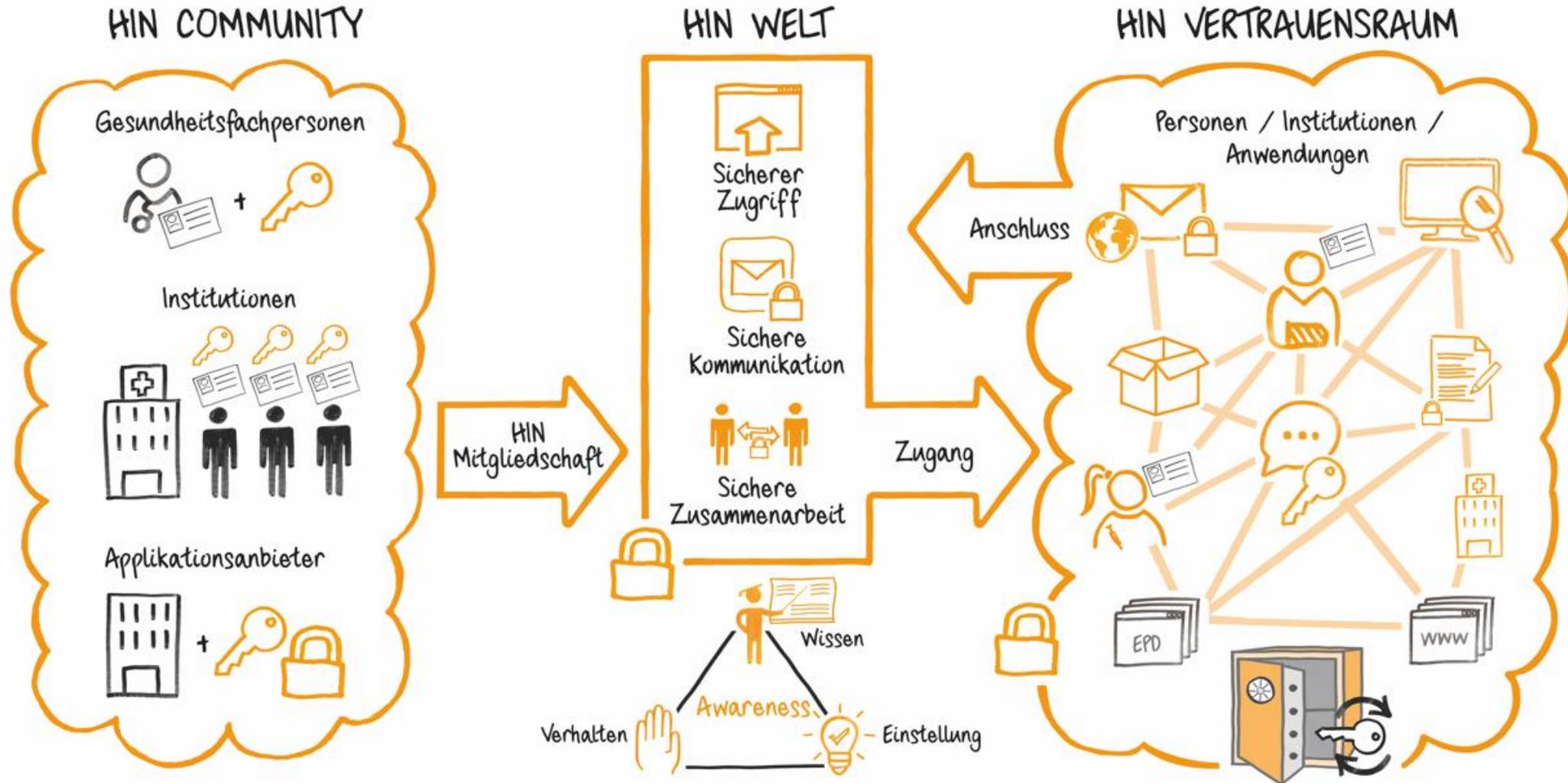
14.06.2023 / Urs Fischer @ .ch

# Sichere und zuverlässige Vernetzung eine Herausforderung für das reguläre Internet

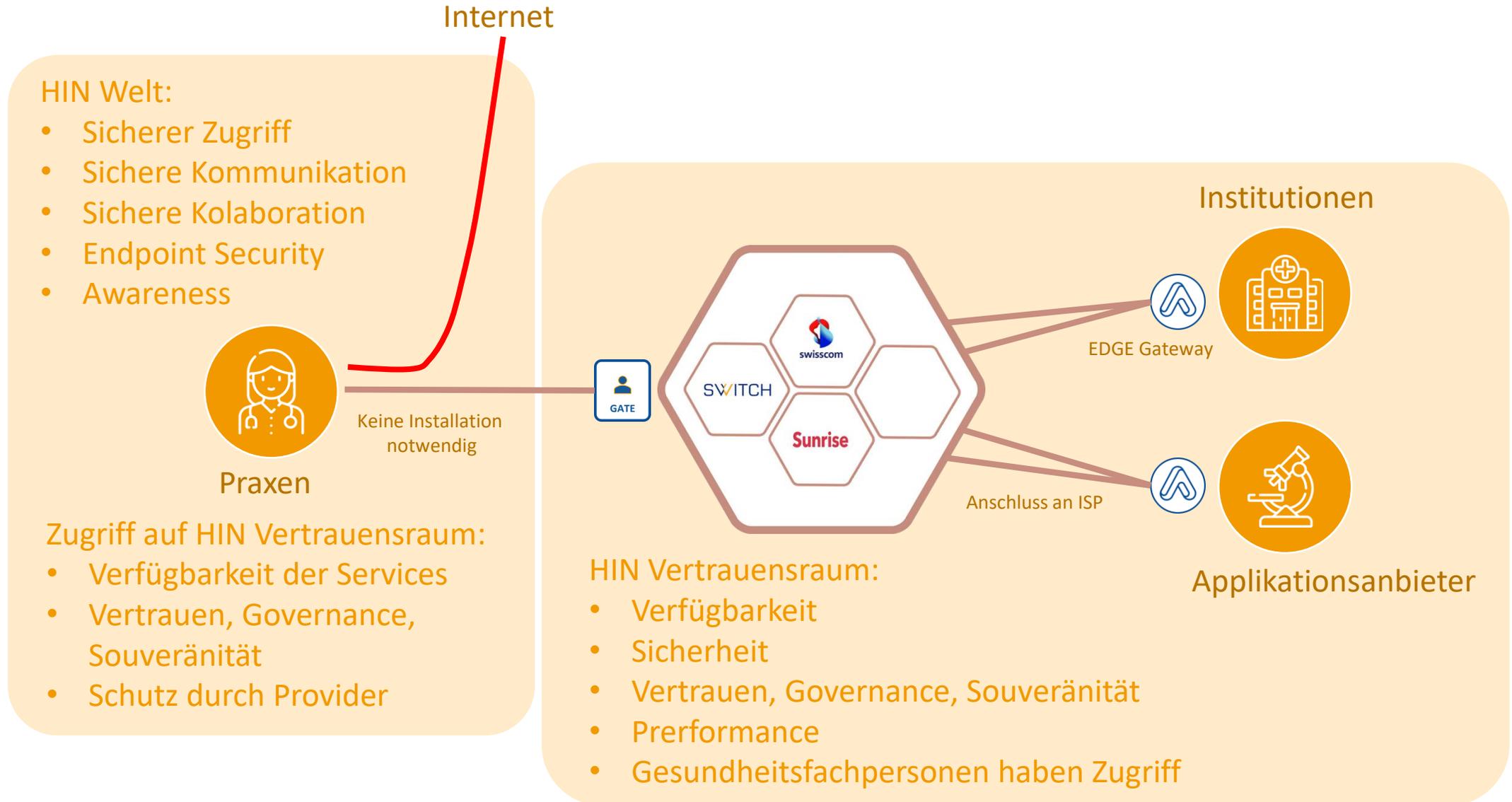
Das Gesundheitswesen ist in hohem Masse von der Kommunikation zwischen mehreren Parteien abhängig:



# HIN Vertrauensraum

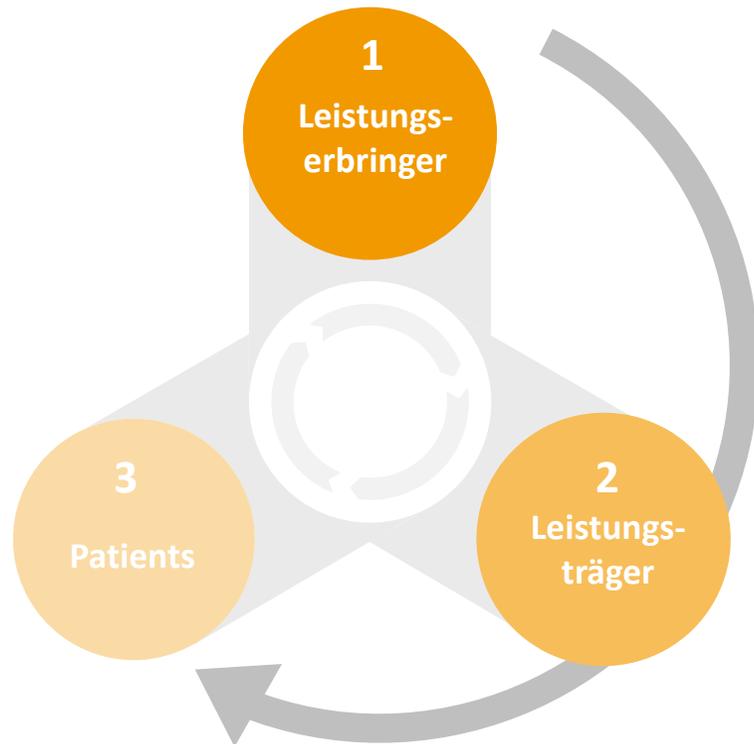


# HIN Vertrauensraum Anschlüsse



# Erschliessung des Ökosystems in mehreren Phasen

Sicherheit und Verfügbarkeit für das Gesundheits-Ökosystem



- 1** Leistungserbringer verbinden:
  - Gesundheitsfachpersonen Anschliessen (HIN stellt Anschluss zur Verfügung)
  - Sicherheit, Verfügbarkeit und Souveränität in das Ökosystem bringen
  - Serviceplattformen: HIN, KIS, PIS, EPD
  - Krankenhäuser, Kliniken, Großpraxen, Apotheken und Labore
  - Leistungsgarantien bieten, um Innovationen wie die Telechirurgie zu erleichtern
- 2** Die Leistungsträger in das Ökosystem einbinden
  - Versicherungen <-> Leistungsplattformen
- 3** Schützen der gesundheitsbezogenen Kommunikation der Patienten:
  - Patienten <-> Telemedizinische Zentren
  - Patienten <-> EPD
  - Patienten <-> Versicherungsportale

