
genua.

# Battle of the Nerds

## IT meets OT

**Paul Schulz**, genua GmbH, Presales Consultant

**Stefan Blancke**, Controlware GmbH,
Senior System Engineer Information Security

*16.09.2025, Congress Park Hanau*

Security
Safety
Availability

Security
C – Confidentiality
I – Integrity
A – Availability

Compliance

Monitoring

Zero Trust

Patch
Tuesday

Altanlagen

Safety

Availability

„Never touch a
running system“

Betriebskontinuität

Wartungsfenster

Physische Prozesse

Echtzeitsteuerung

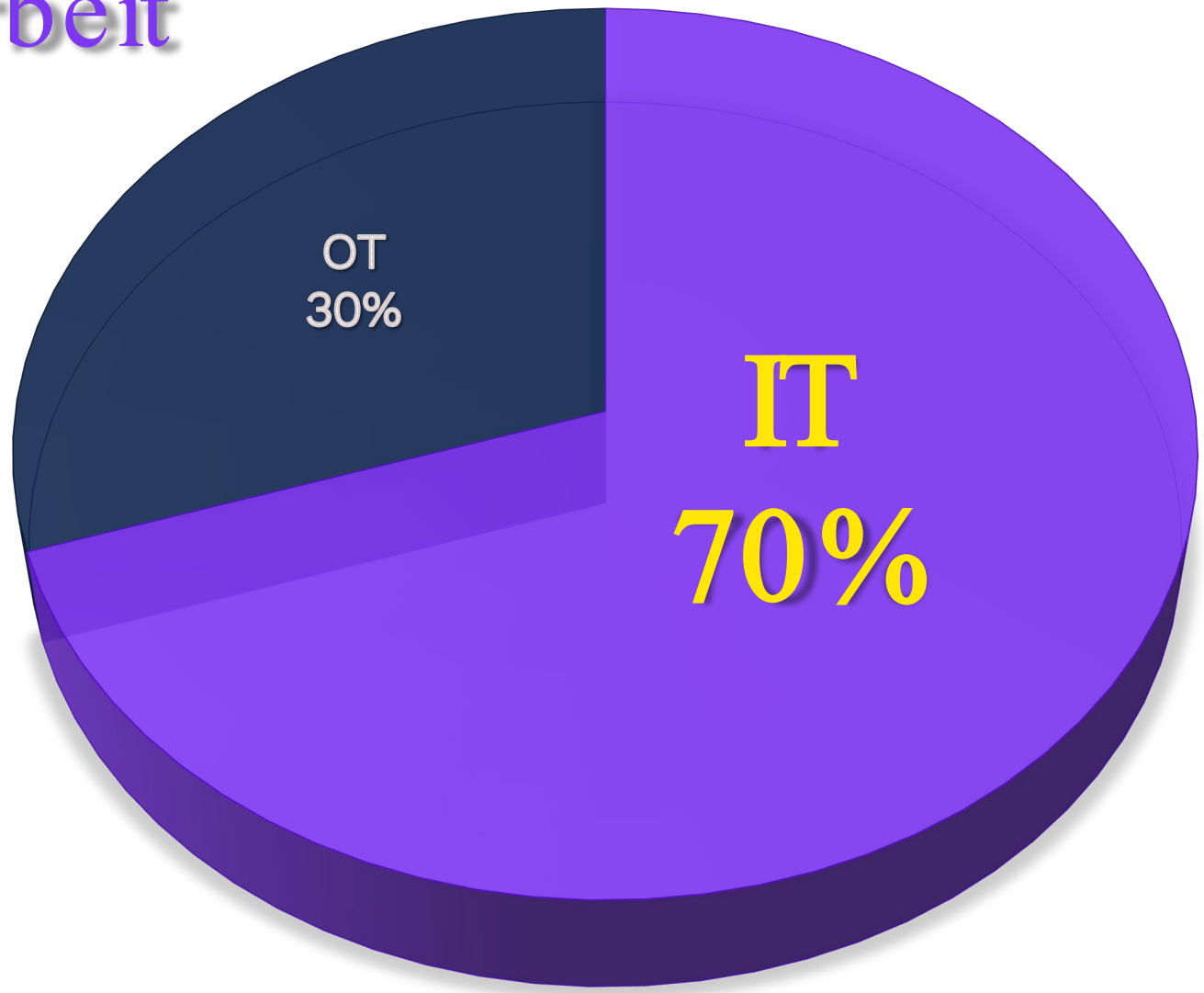
# Warum Zusammenarbeit unvermeidbar ist

Laut einer aktuellen Dragos-Studie starten

**70 % aller OT-Sicherheitsvorfälle im IT-Netz.**

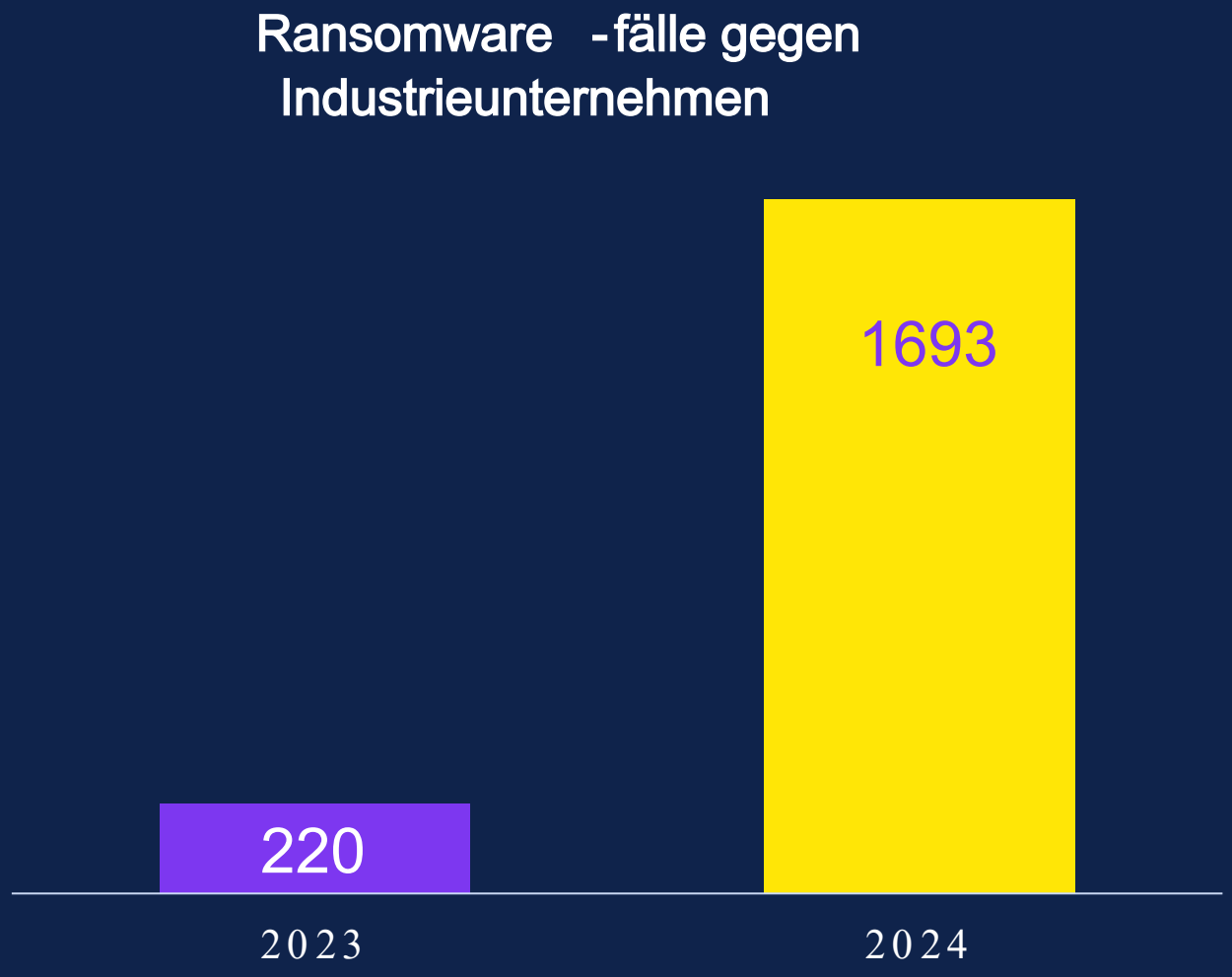
Das bedeutet:

Auch wenn eine Anlage isoliert wirkt Schwachstellen in der IT reißen die OT mit hinein




*Quelle: Dragos, Year in Review 2024

# Die Angriffe nehmen rasant zu




Im Jahr 2024 verzeichnete Dragos weltweit **1.693 Ransomware-Fälle gegen Industrieunternehmen**

Das ist ein **Anstieg um 87 % gegenüber 2023** .

Der Trend zeigt klar:

Angreifer konzentrieren sich immer stärker auf den Produktionssektor.

*Quelle: Dragos, Year in Review 2024

# Fast jedes vierte System ist betroffen

Im vierten Quartal 2024 blockte Kaspersky auf **21,9 % aller ICS-Rechner** Schadaktivität.

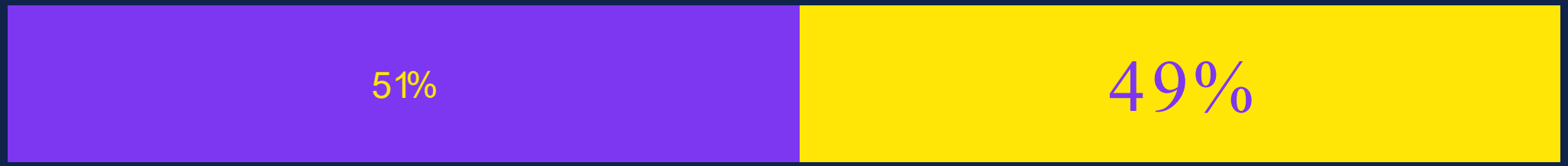
Mit anderen Worten: jedes vierte System war Angriffen ausgesetzt.


Quelle: Kaspersky ICS-CERT Q4 2024

# Wenn es kracht, wird es **teuer**

Laut einer CPS-Studie erlitten
**49 % der betroffenen Industrieunternehmen**
über 12 Stunden Produktionsausfall nach einem Cybervorfall.

Solche Stillstände verursachen schnell
**Millionenschäden .**




Quelle: Kaspersky ICS-CERT Q4 2024

Sicherheitskonzepte
müssen beide Welten
verbinden

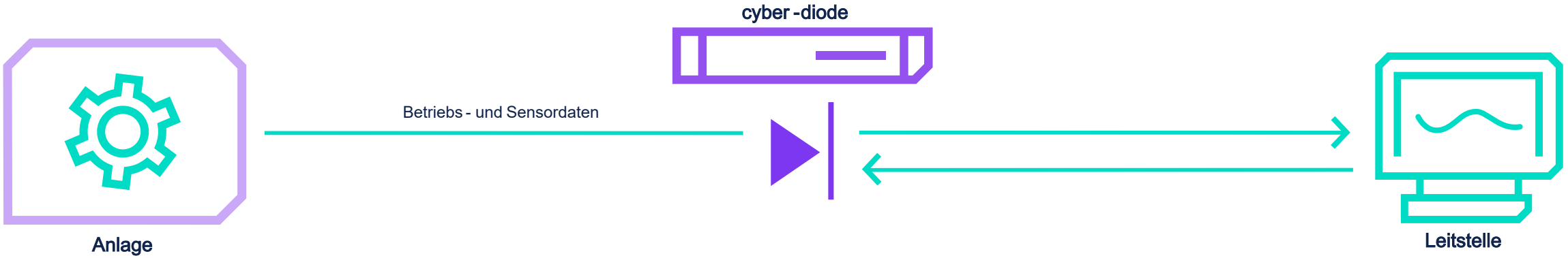
–

sonst bleibt die
Produktion verwundbar.

# Use Case 1

## Sensordaten sicher aus alten Anlagen ausleiten

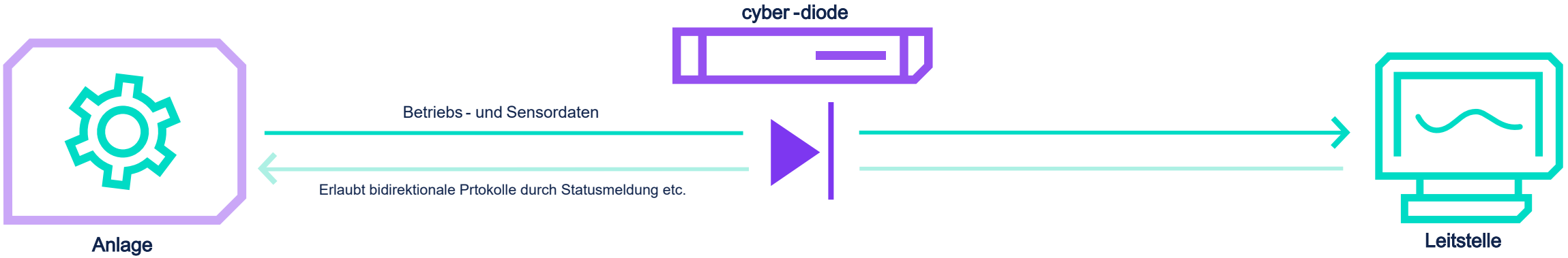
*Wie lassen sich Produktions - und Sensordaten aus Legacy-Systemen in Monitoring - und Analysesysteme übertragen – ohne das Risiko, einen Rückkanal für Angriffe zu öffnen?*



# Use Case 1

## Sensordaten sicher aus alten Anlagen ausleiten

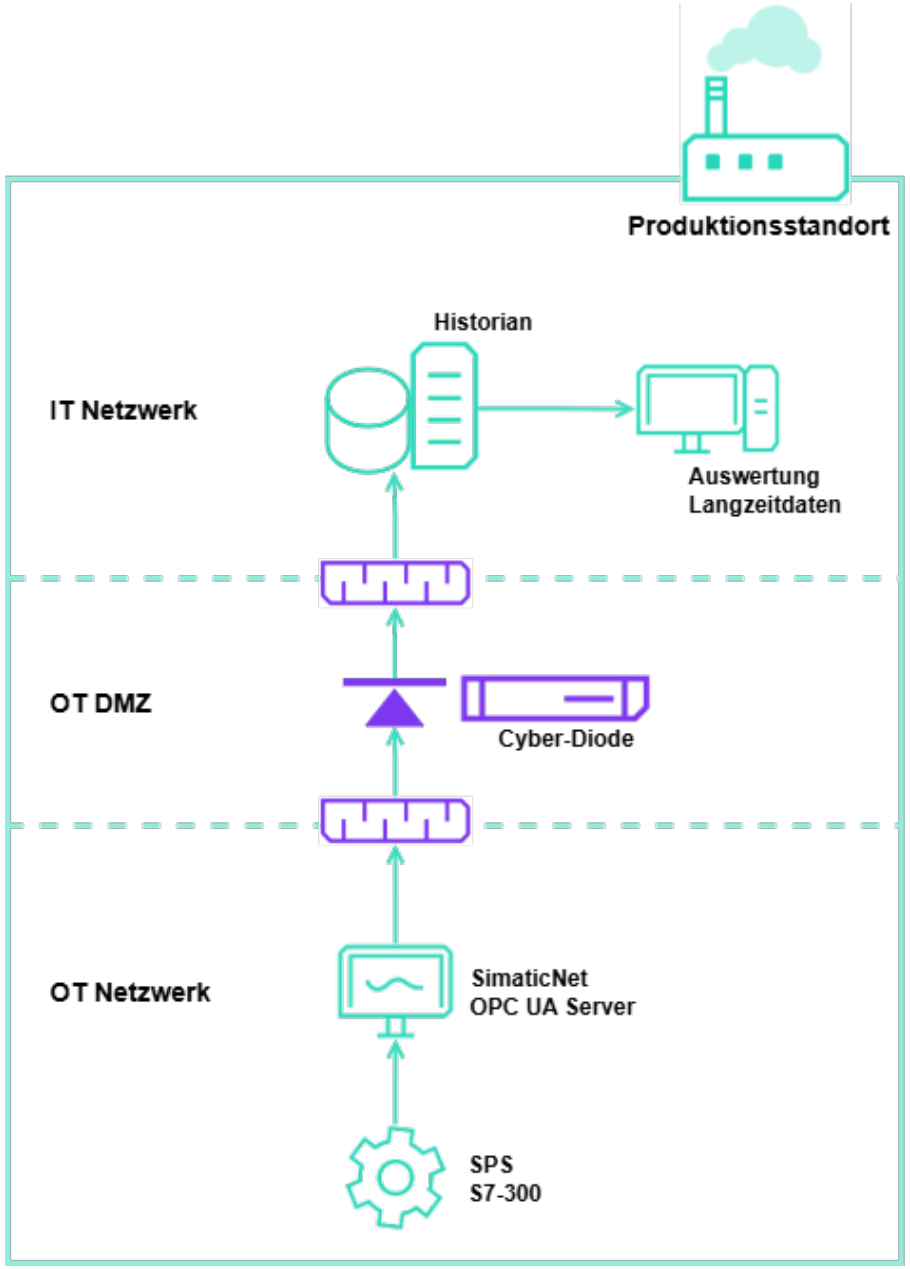
*Wie lassen sich Produktions - und Sensordaten aus Legacy-Systemen in Monitoring - und Analysesysteme übertragen – ohne das Risiko, einen Rückkanal für Angriffe zu öffnen?*



# In Praxis

## Sensordaten sicher aus alten Anlagen ausleiten

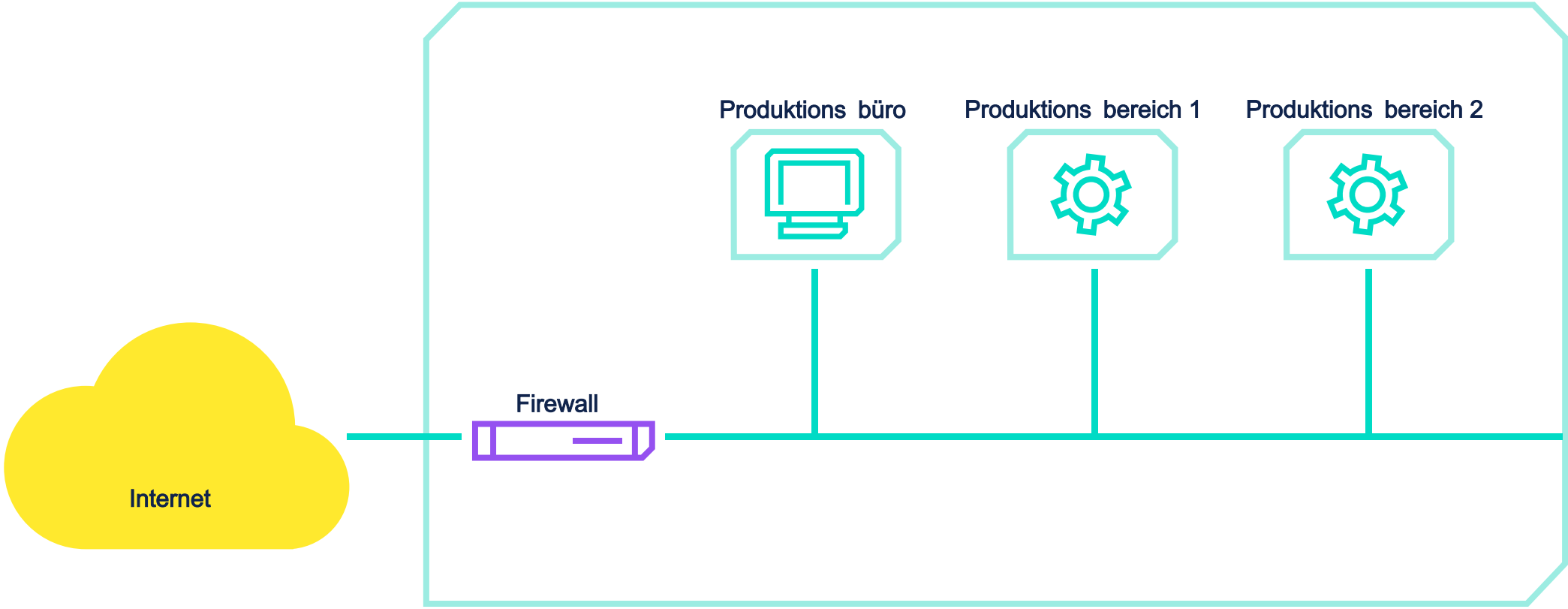
- *Mitarbeiter wollten Langzeittrends & Meldungen in eigenen Tools auswerten.*
- *Früher: nur RDP-Zugriff auf Produktionsdaten, keine flexible Nutzung.*
- *Lösung: Historian in IT-Umgebung, gespeist per OPC UA.*
- *Diode überträgt Daten sicher aus SPS durch DMZ→ Historian.*



# Use Case 2

## Produktionsnetz sauber segmentieren

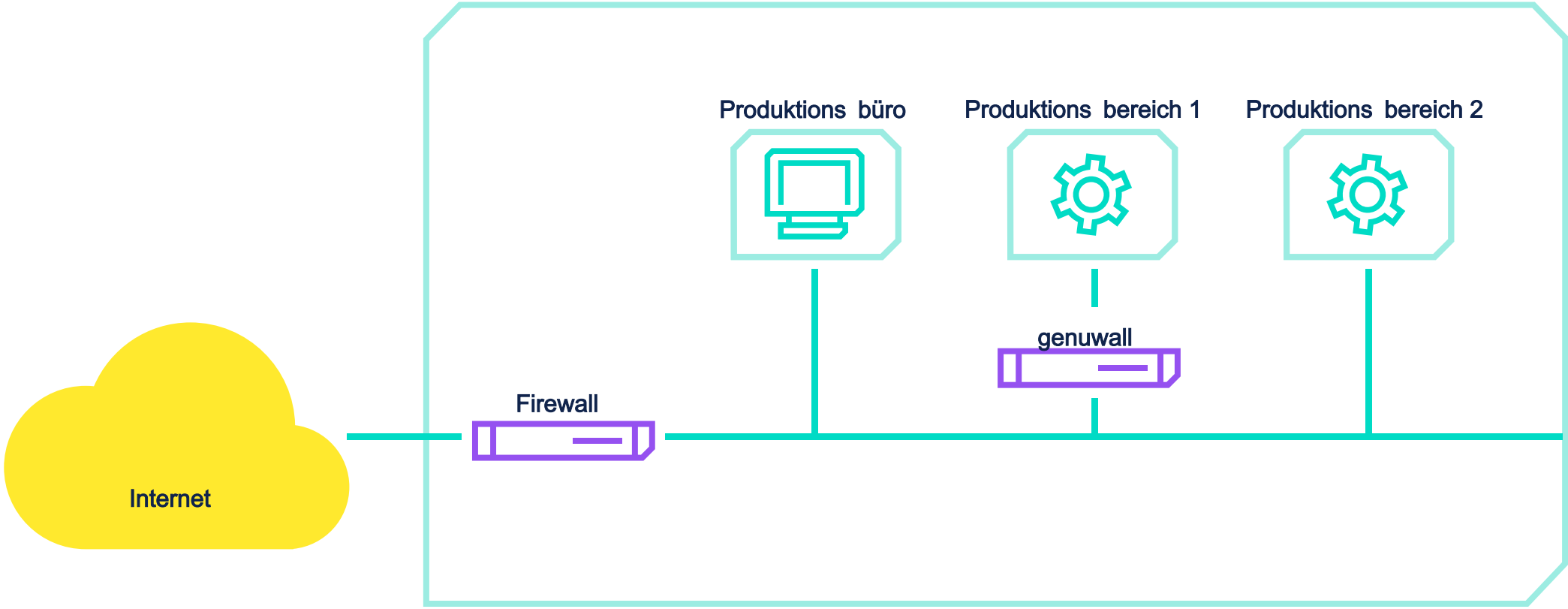
*Wie trennen wir Linien, Zellen und Übergänge so, dass Malware nicht das ganze Werk lahmlegt – ohne Adresspläne umzubauen und ohne die Produktion zu stören?*



# Use Case 2

## Produktionsnetz sauber segmentieren

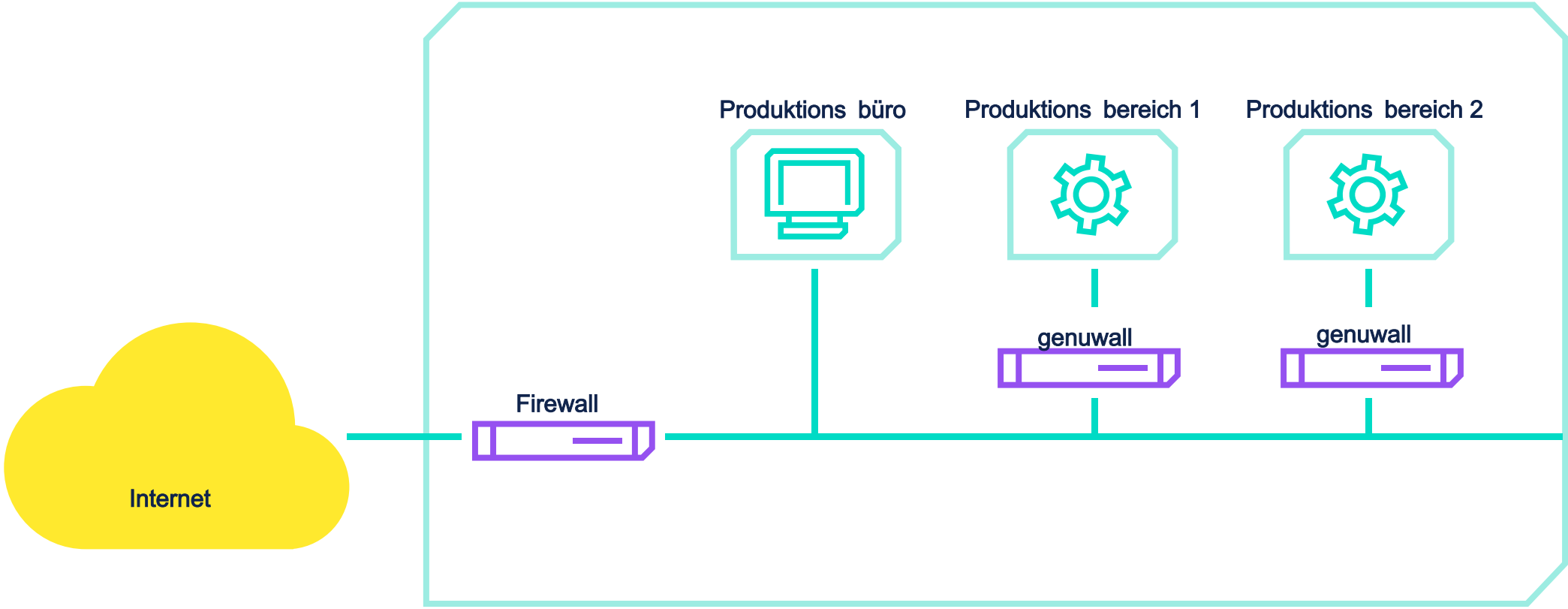
*Wie trennen wir Linien, Zellen und Übergänge so, dass Malware nicht das ganze Werk lahmlegt – ohne Adresspläne umzubauen und ohne die Produktion zu stören?*



# Use Case 2

## Produktionsnetz sauber segmentieren

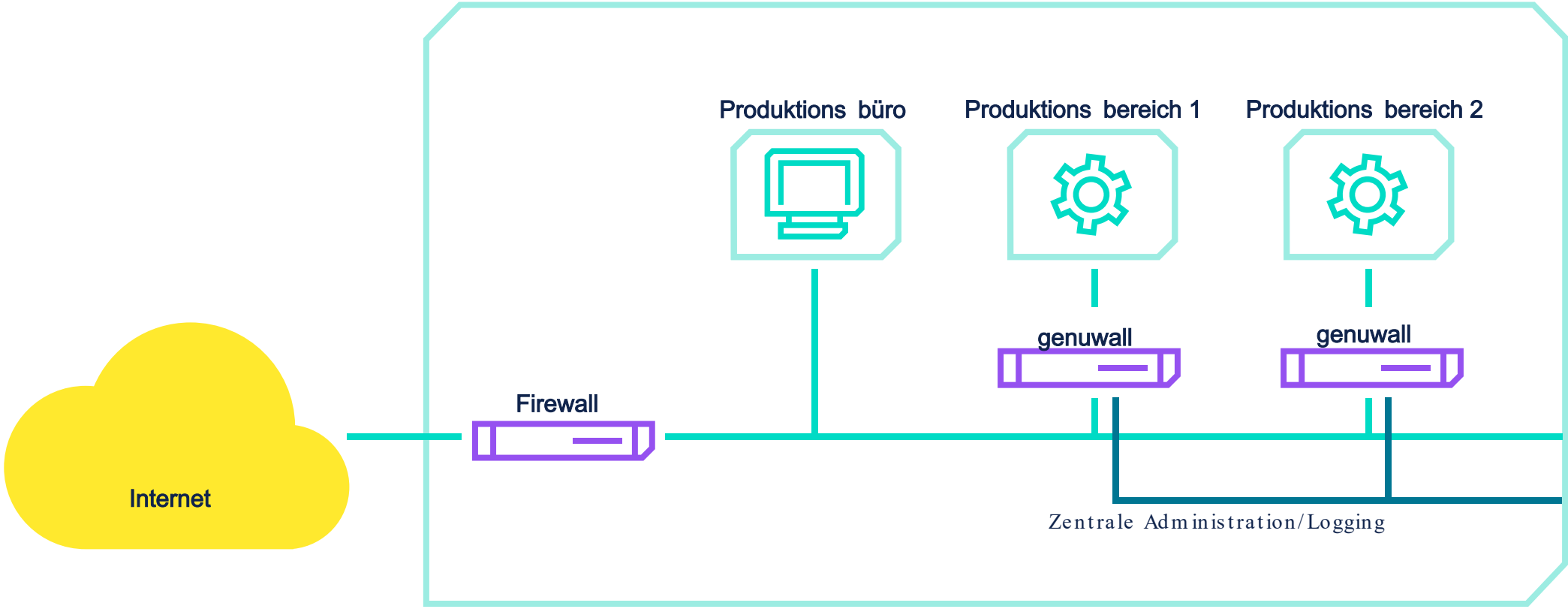
*Wie trennen wir Linien, Zellen und Übergänge so, dass Malware nicht das ganze Werk lahmlegt – ohne Adresspläne umzubauen und ohne die Produktion zu stören?*



# Use Case 2

## Produktionsnetz sauber segmentieren

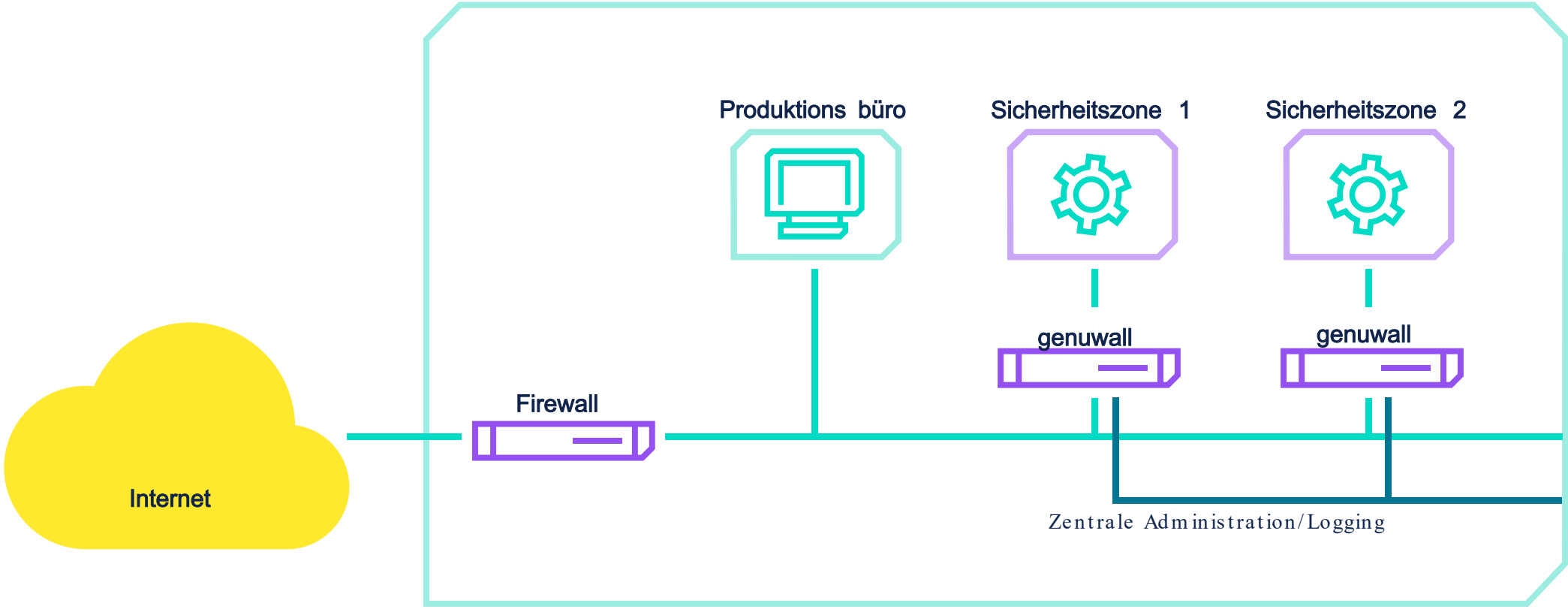
*Wie trennen wir Linien, Zellen und Übergänge so, dass Malware nicht das ganze Werk lahmlegt – ohne Adresspläne umzubauen und ohne die Produktion zu stören?*



# Use Case 2

## Produktionsnetz sauber segmentieren

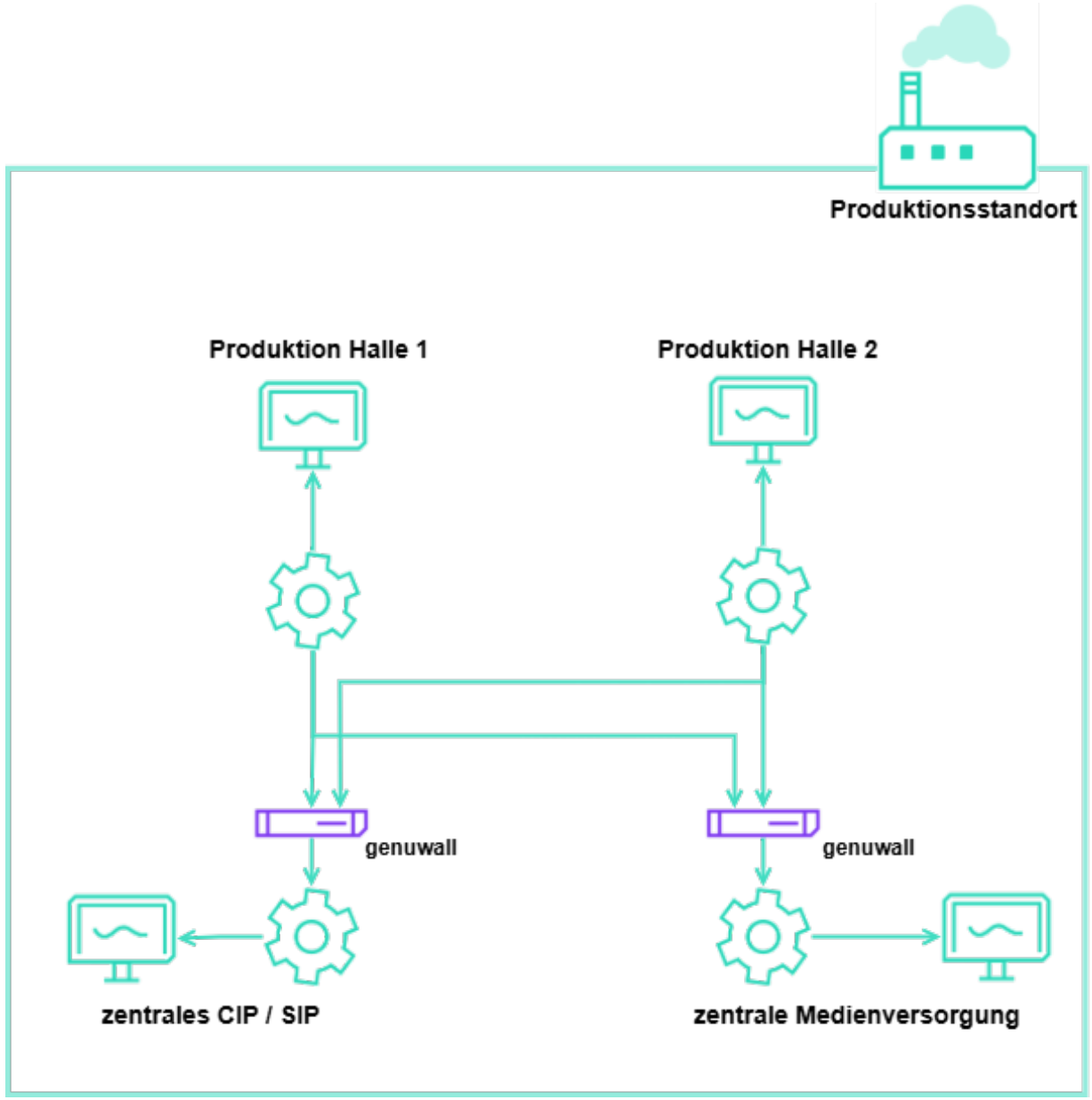
*Wie trennen wir Linien, Zellen und Übergänge so, dass Malware nicht das ganze Werk lahmlegt – ohne Adresspläne umzubauen und ohne die Produktion zu stören?*



# In Praxis

## Produktionsnetz sauber segmentieren

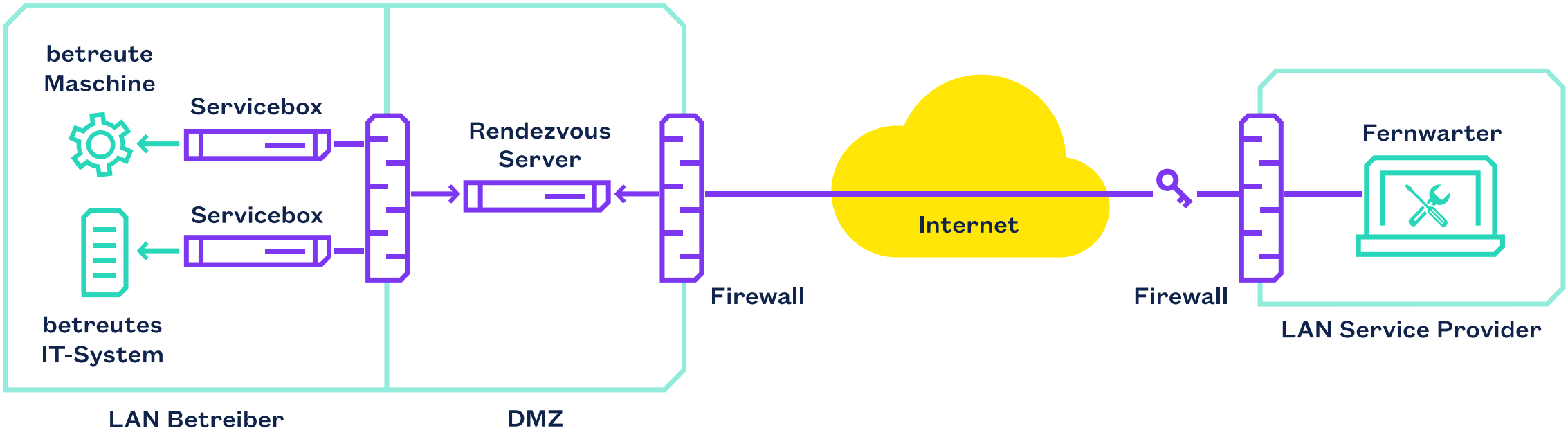
- *Mehrere Linien brauchten Zugriff auf zentrale Medienanlagen (Dampf, Wasser, CIP/SIP).*
- *Netze der Linien zwar getrennt, aber über zentrale Anlagen wieder verbunden → Störungen & Risiken.*
- *Mit genuwall als Layer-2-Bridge:*
  - *Netze sauber getrennt,*
  - *keine Rekonfiguration nötig,*
  - *Störungen minimiert.*



# Use Case 3:

## Fernwartung ohne offene Hintertüren

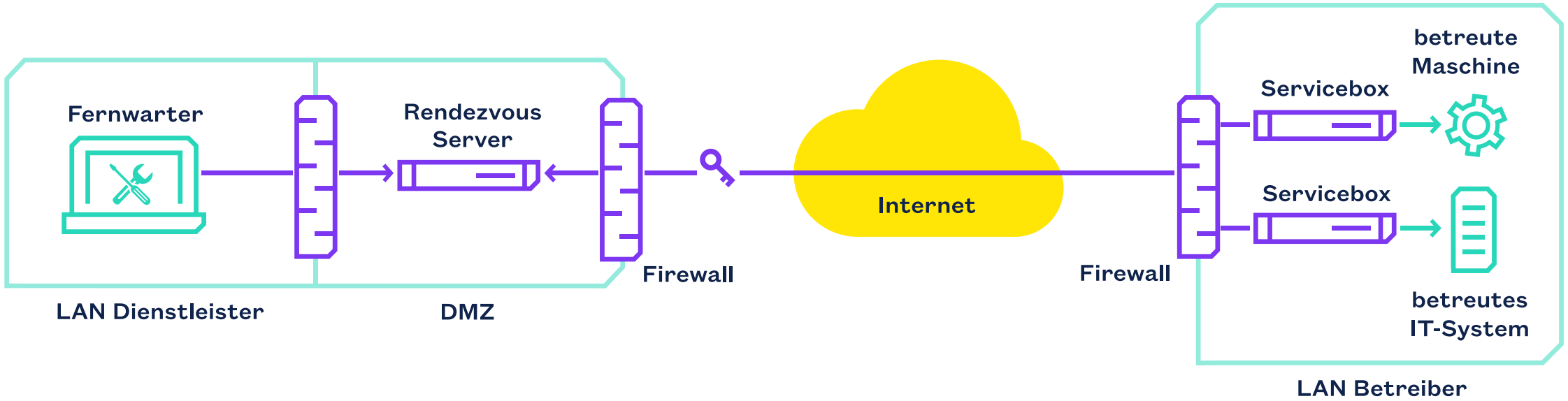
*Wie ermöglichen wir Maschinenbauern und Servicepartnern sicheren Fernzugriff – ohne Dauer-VPNs, offene Firewalls oder unkontrollierbare Schatten-IT?*



# Use Case 3:

## Fernwartung ohne offene Hintertüren

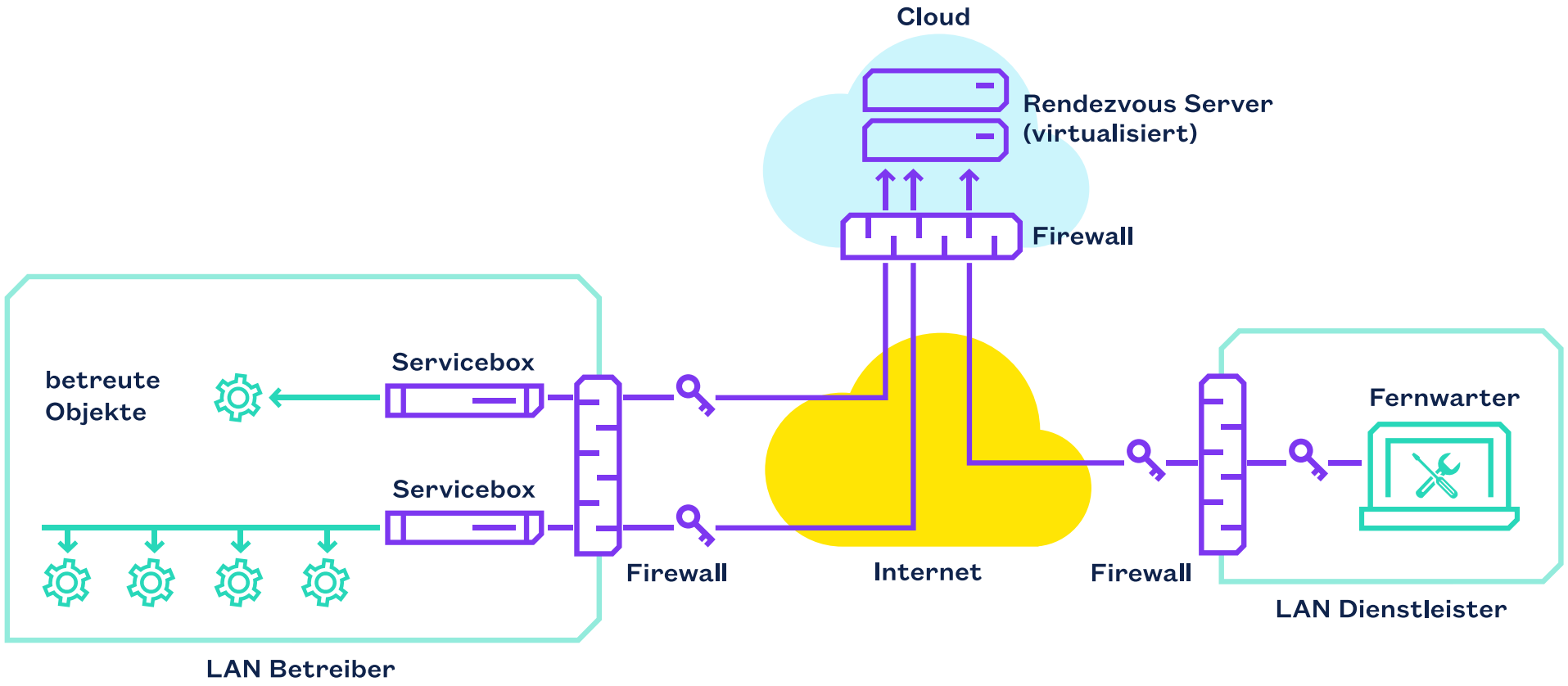
*Wie ermöglichen wir Maschinenbauern und Servicepartnern sicheren Fernzugriff – ohne Dauer-VPNs, offene Firewalls oder unkontrollierbare Schatten-IT?*



# Use Case 3:

## Fernwartung ohne offene Hintertüren

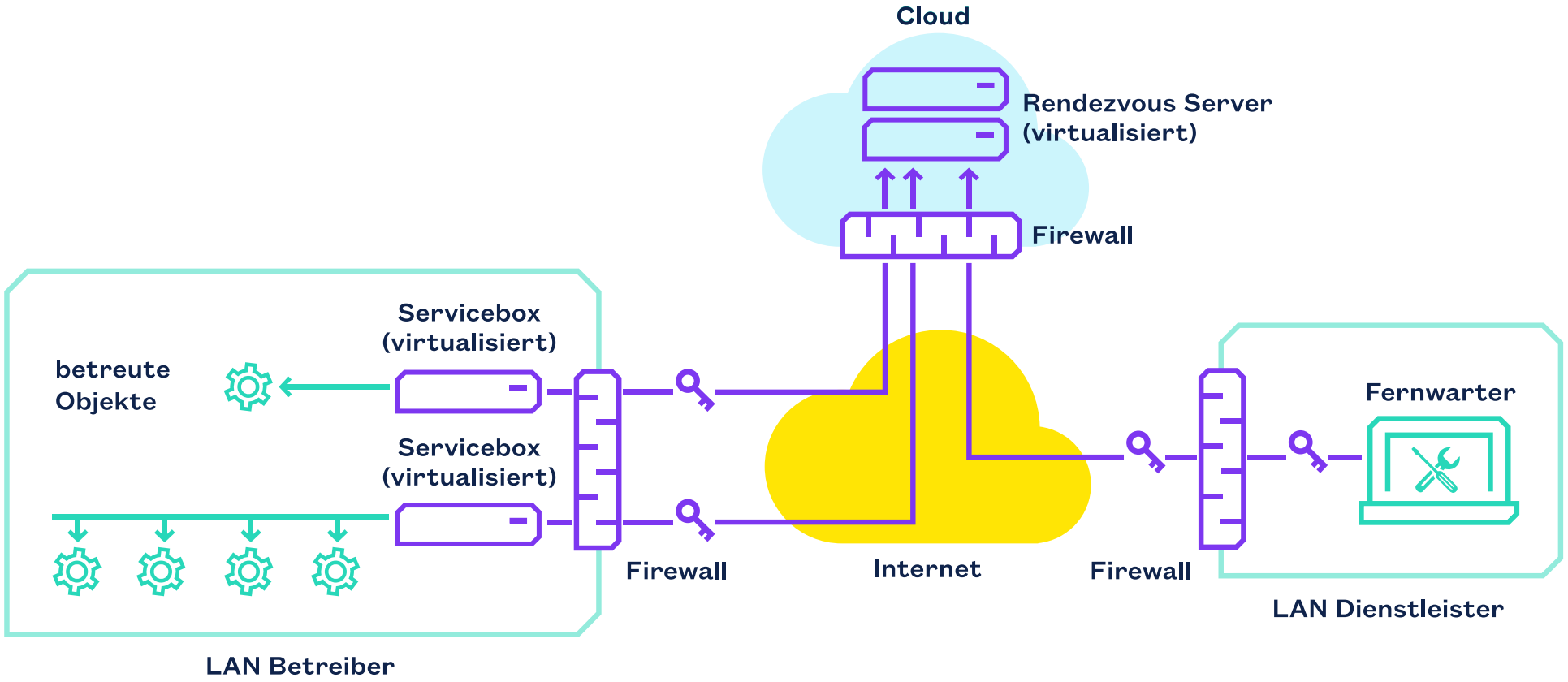
*Wie ermöglichen wir Maschinenbauern und Servicepartnern sicheren Fernzugriff – ohne Dauer-VPNs, offene Firewalls oder unkontrollierbare Schatten-IT?*



# Use Case 3:

## Fernwartung ohne offene Hintertüren

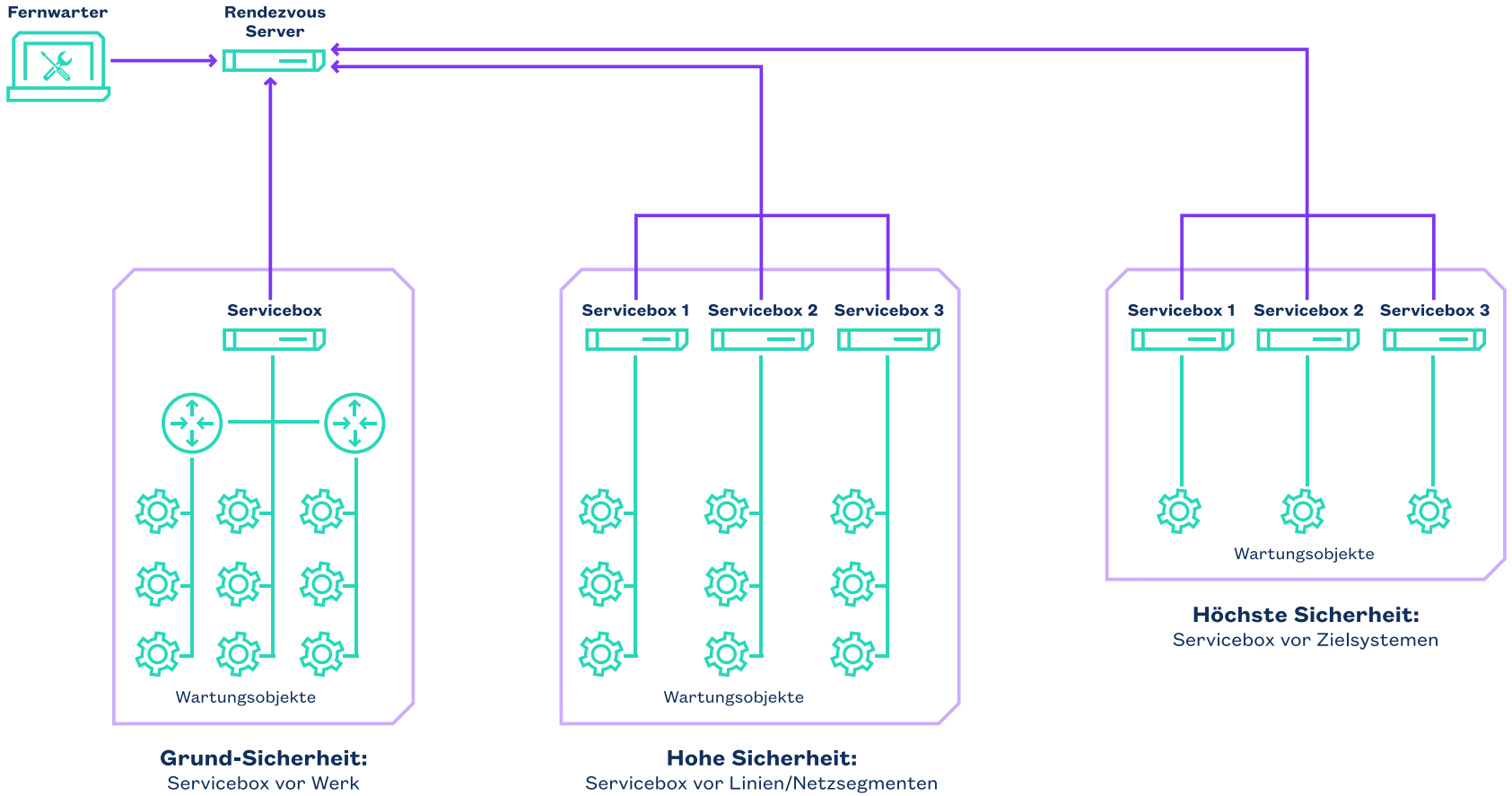
*Wie ermöglichen wir Maschinenbauern und Servicepartnern sicheren Fernzugriff – ohne Dauer-VPNs, offene Firewalls oder unkontrollierbare Schatten-IT?*



# Use Case 3:

## Fernwartung ohne offene Hintertüren

*Wie ermöglichen wir Maschinenbauern und Servicepartnern sicheren Fernzugriff – ohne Dauer-VPNs, offene Firewalls oder unkontrollierbare Schatten-IT?*



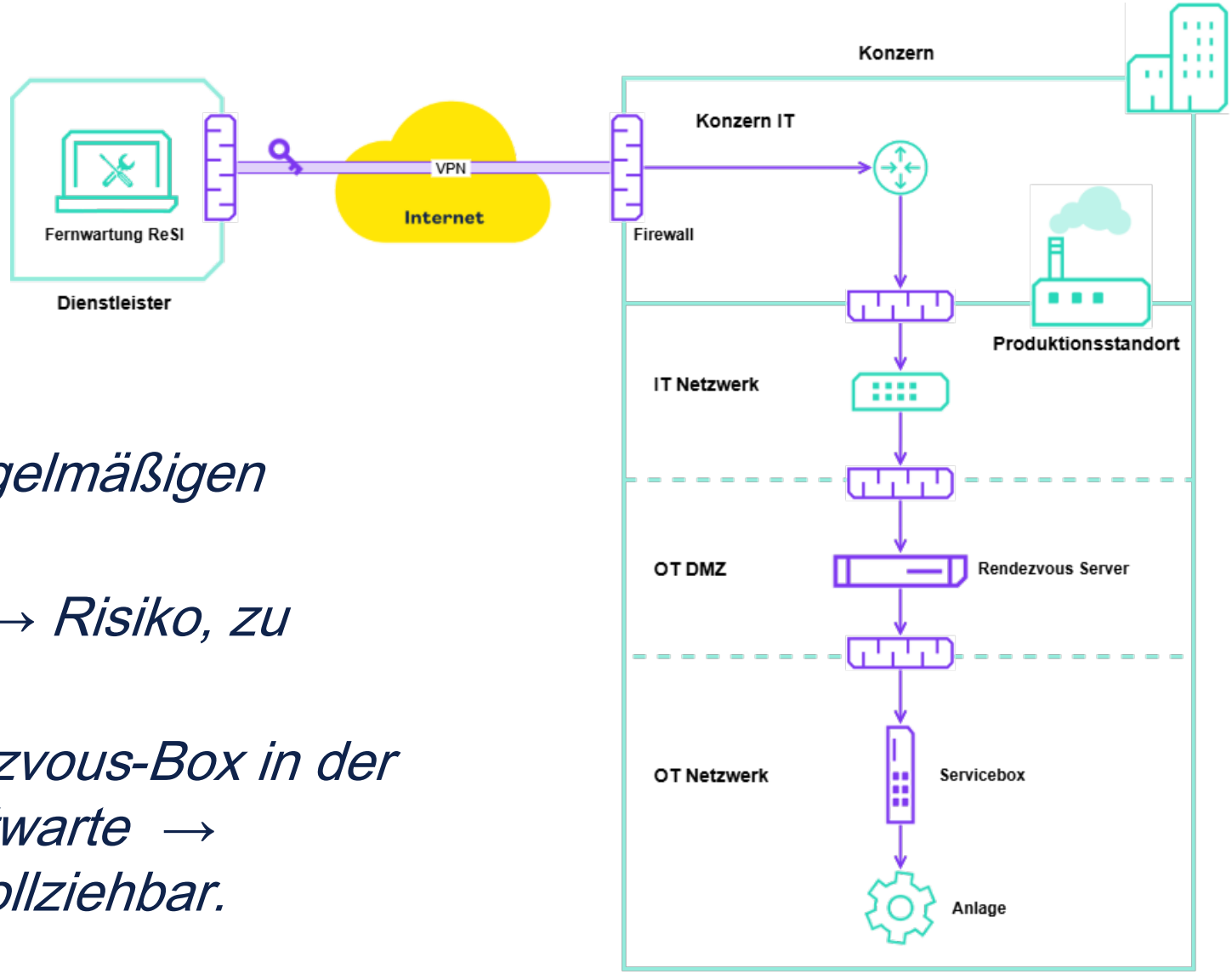

**Grund-Sicherheit:**
Servicebox vor Werk

**Hohe Sicherheit:**
Servicebox vor Linien/Netzsegmenten

**Höchste Sicherheit:**
Servicebox vor Zielsystemen

# In Praxis:

## Fernwartung ohne offene Hintertüren




- *Externe OEMs brauchten regelmäßigen Zugriff auf eine Anlage.*
- *Früher: VPN ins Konzern-IT → Risiko, zu weitreichender Zugang.*
- *Heute: Zugriff nur bis Rendezvous-Box in der OT-DMZ.Freigabe durch Leitwarte → temporär, kontrolliert, nachvollziehbar.*

# Security Safety Availability

Controlware
Security Day

# Danke für Ihre Aufmerksamkeit.
# Wir freuen uns über Ihr Feedback!

**Bitte geben Sie den ausgefüllten Bogen am Empfang ab und erhalten Sie als Dankeschön ein kleines Präsent.**

© 2025 Controlware GmbH