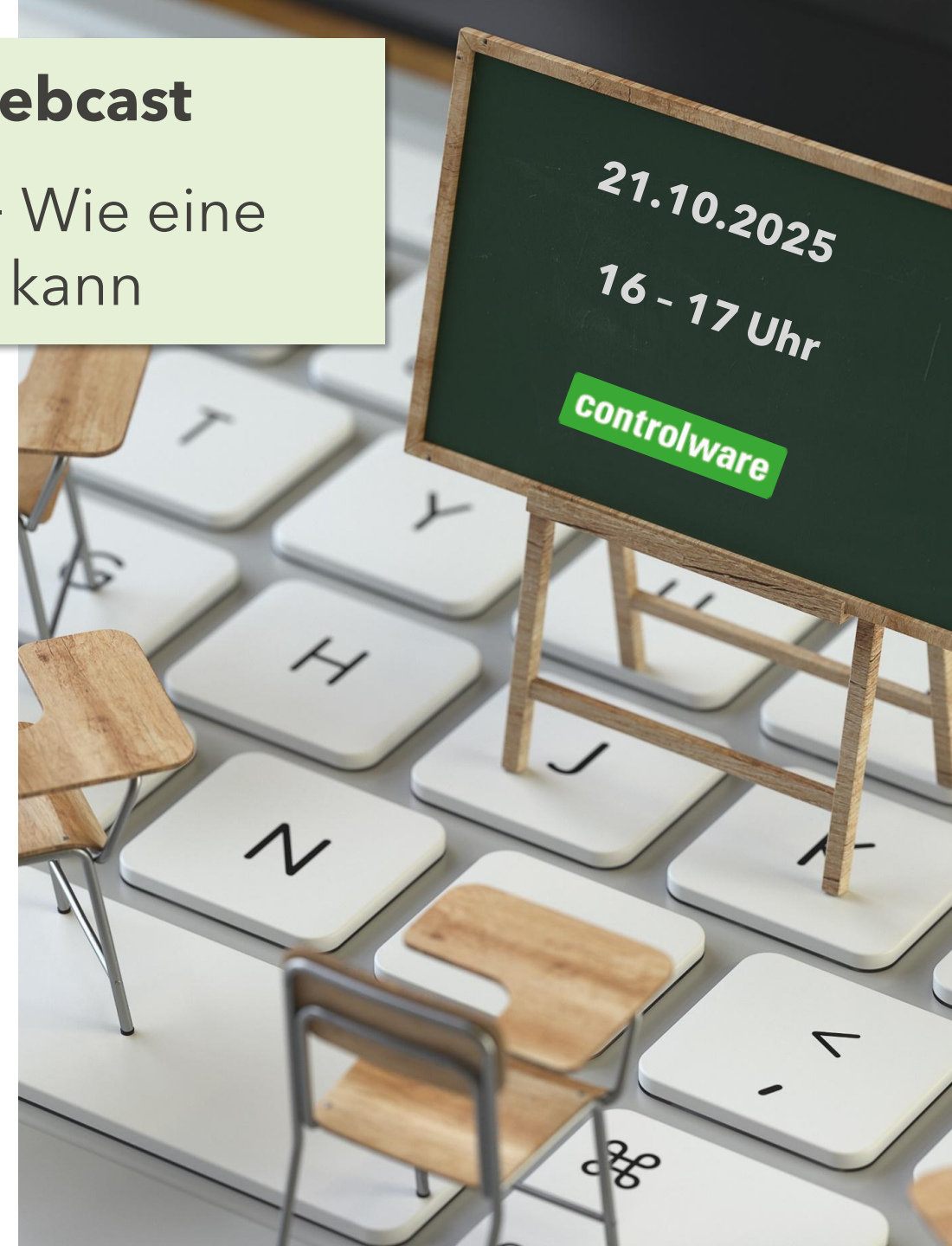


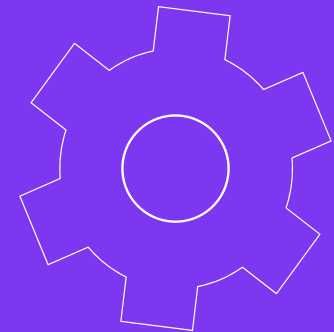
Willkommen zum Competence Webcast

IT/OT-Sicherheit "Made in Germany" – Wie eine erfolgreiche Umsetzung gelingen kann

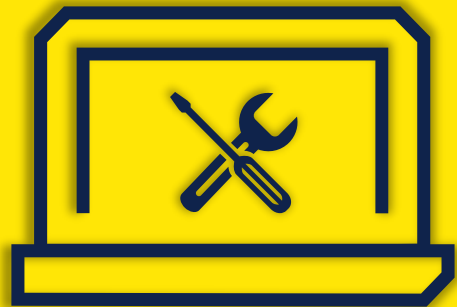
Housekeeping

- Alle Teilnehmer sind stummgeschaltet
- Diese Session wird aufgezeichnet und Ihnen im Nachgang zusammen mit der Präsentation zur Verfügung gestellt
- Unter Fragen und Antworten gestellte Fragen werden am Ende des Webcast mündlich beantwortet
- Bitte nehmen Sie sich nach dem Webcast kurz für eine Bewertung unseres Webcasts Zeit





Security
C – Confidentiality
I – Integrity
A – Availability



Compliance

Monitoring

Zero Trust

Patch
Tuesday

Security
Safety
Availability

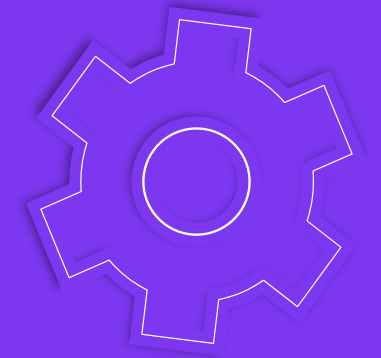


Altanlagen
Safety

Availability

„Never touch a
running system“

Betriebskontinuität



Wartungsfenster

Physische Prozesse

Echtzeitsteuerung

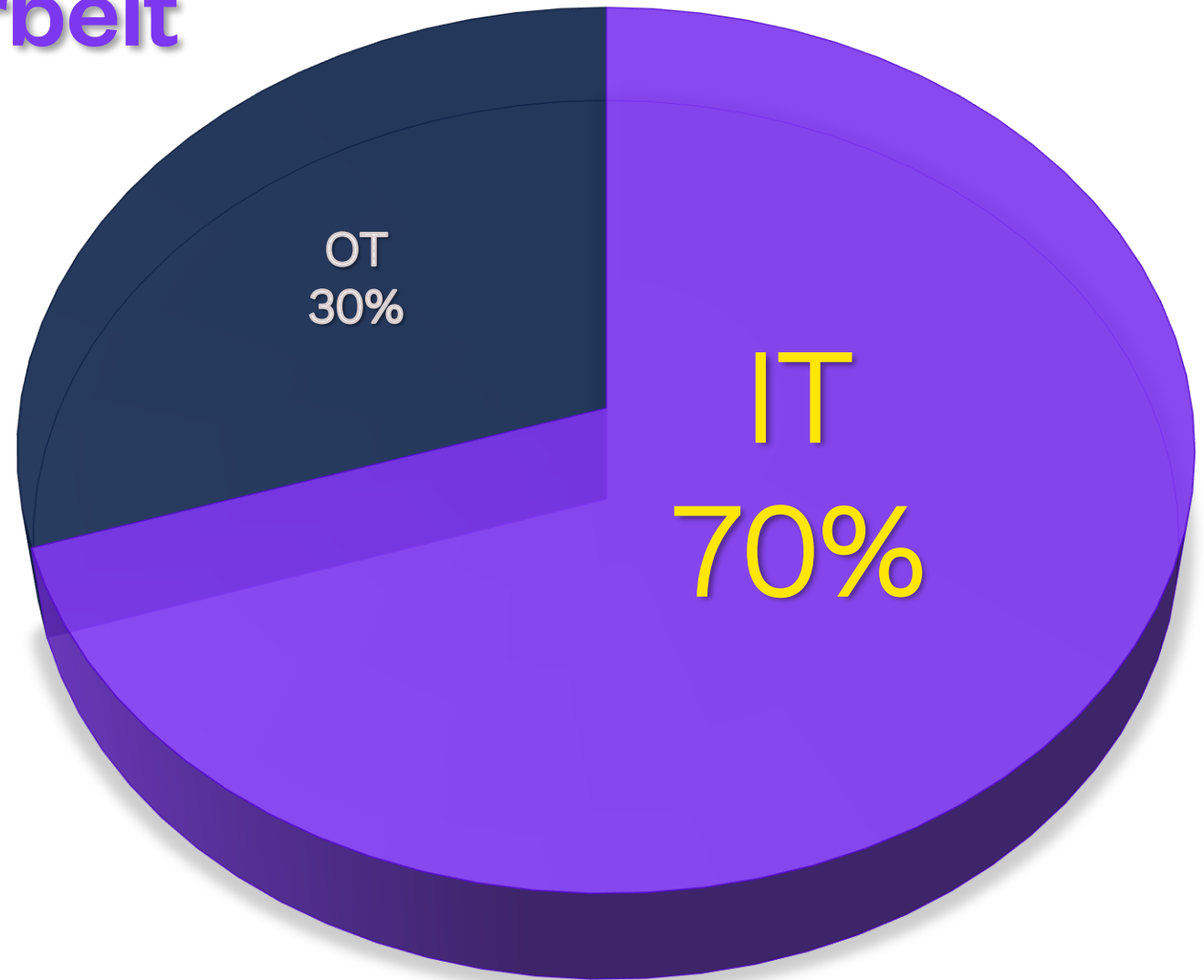
Warum Zusammenarbeit unvermeidbar ist

Laut einer aktuellen Dragos-Studie starten

70 % aller OT-Sicherheitsvorfälle im IT-Netz.

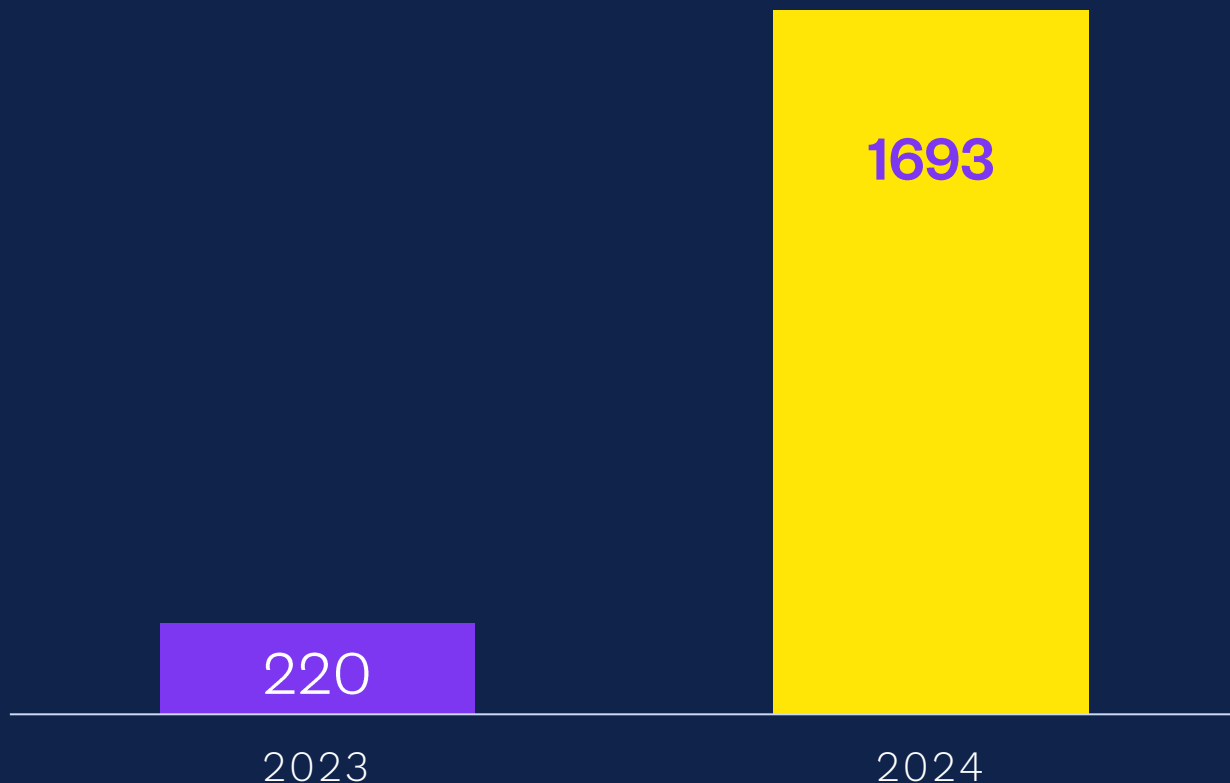
Das bedeutet:

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



Die Angriffe nehmen rasant zu

Ransomware-fälle gegen
Industrieunternehmen



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.

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.

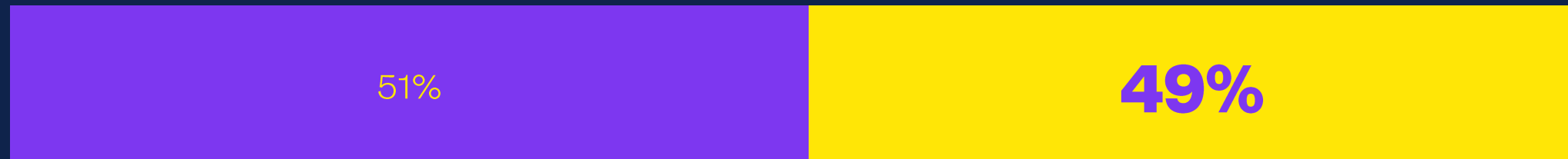


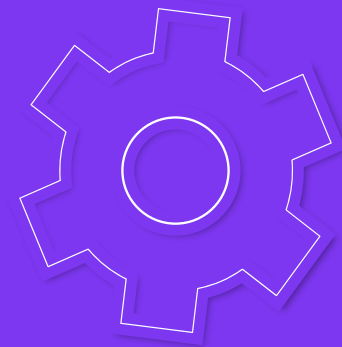
Wenn es kracht, wird es **teuer**

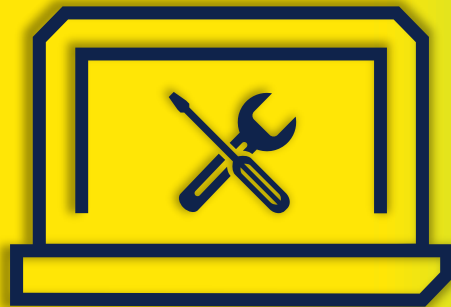


Laut einer CPS-Studie erlitten
49 % der betroffenen Industrieunternehmen
über 12 Stunden Produktionsausfall nach einem
Cybervorfall.

Solche Stillstände verursachen schnell
Millionenschäden.



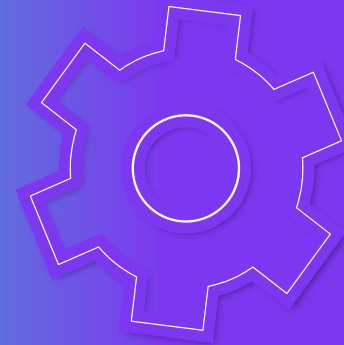


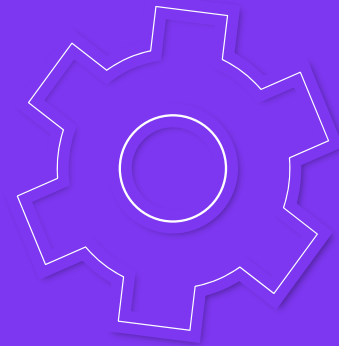
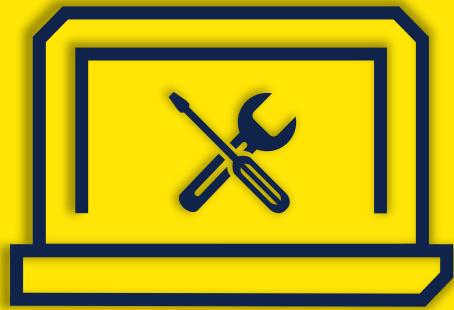


Sicherheitskonzepte
müssen beide Welten
verbinden

–

sonst bleibt die
Produktion verwundbar.

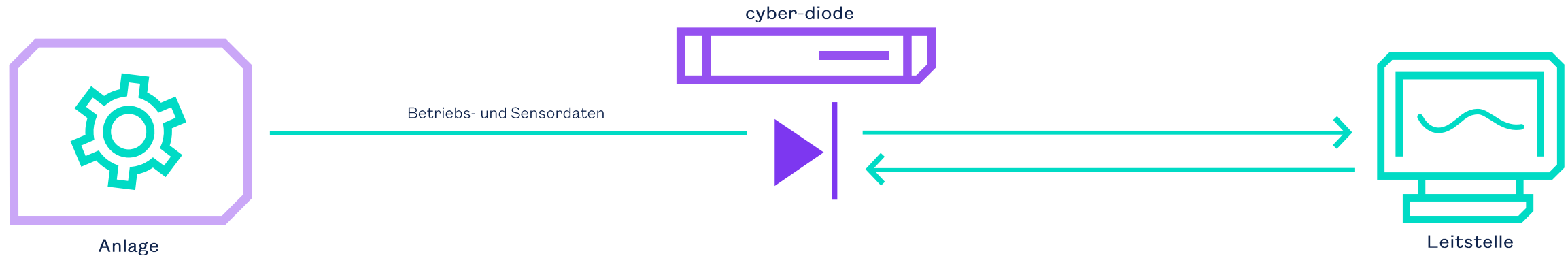




Use Case 1

Sensordaten sicher aus alten Anlagen ausleiten

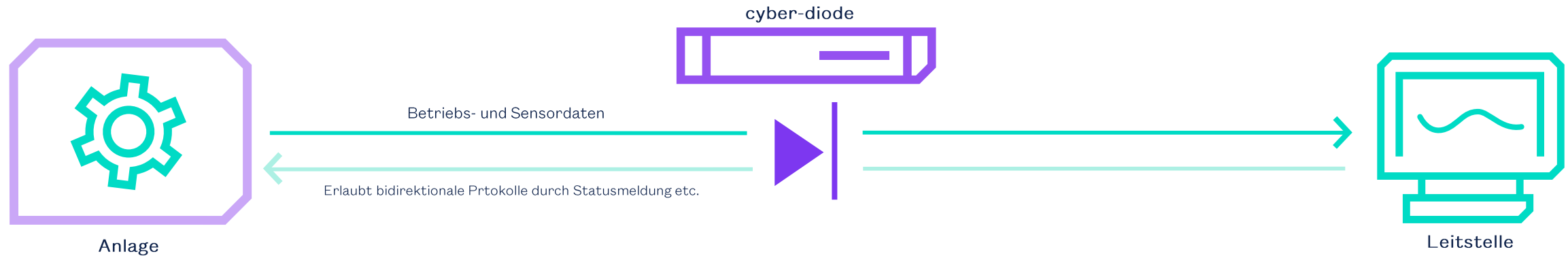
Wie lassen sich Produktions- und Sensordaten aus Legacy-Systemen in Monitoring- und Analysesysteme übertragen – ohne das Risiko, einen Rückkanal für Angriffe zu öffnen?



Use Case 1

Sensordaten sicher aus alten Anlagen ausleiten

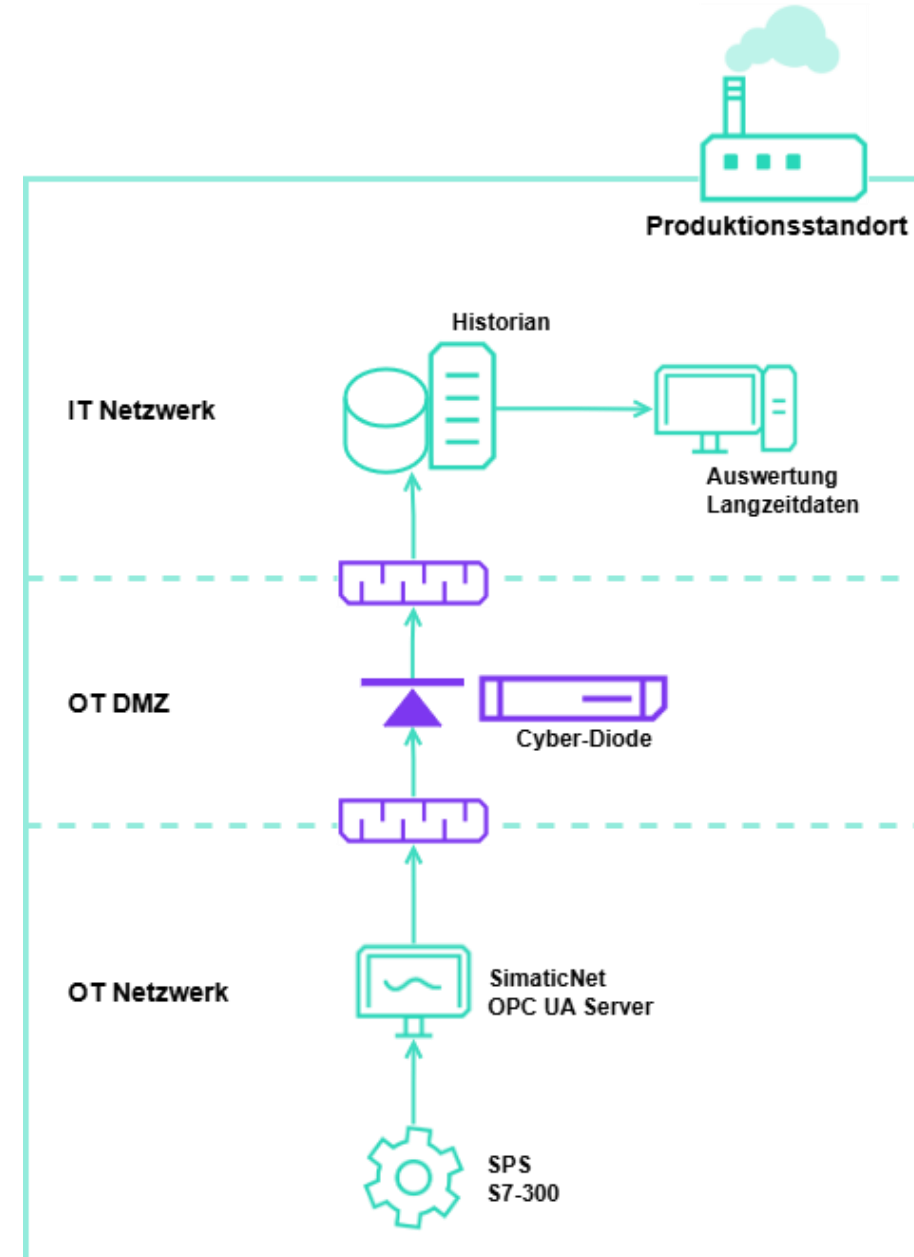
Wie lassen sich Produktions- und Sensordaten aus Legacy-Systemen in Monitoring- und Analysesysteme übertragen – ohne das Risiko, einen Rückkanal für Angriffe zu öffnen?



In Praxis

Sensordaten sicher aus alten Anlagen ausleiten

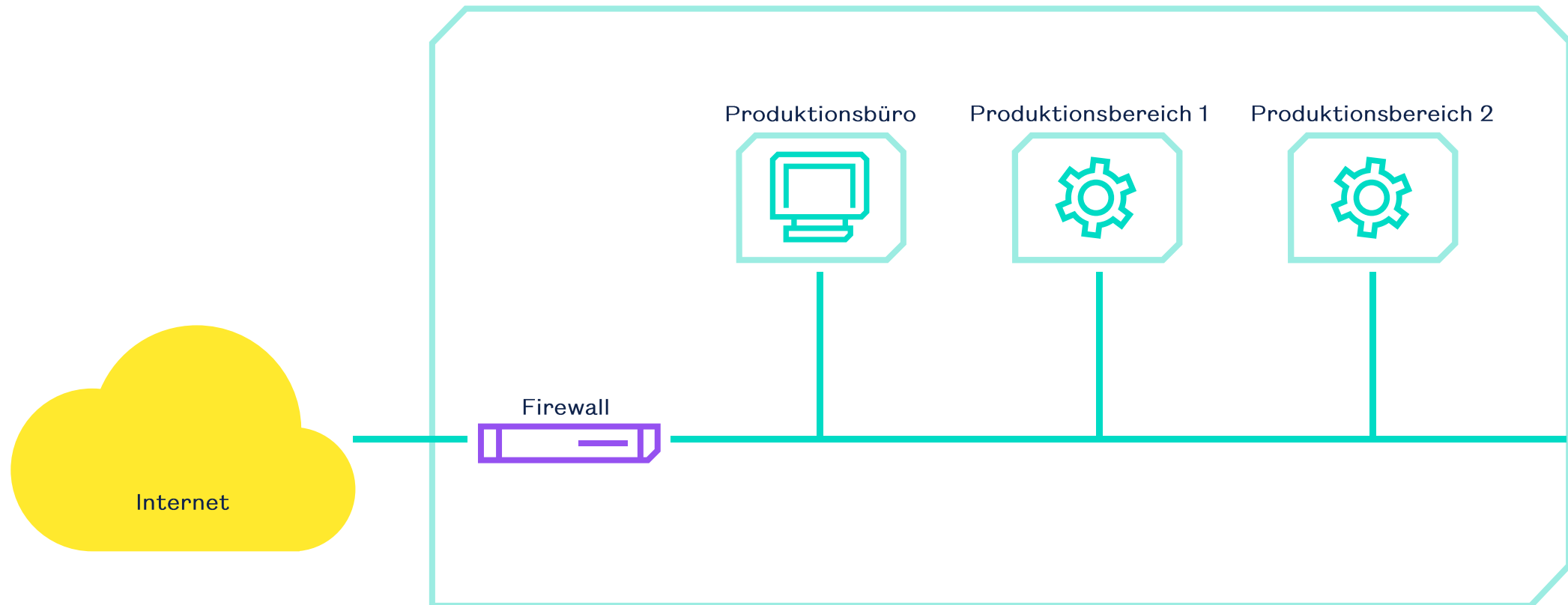
- *Mitarbeiter wollten Langzeittrends & Meldungen in eigenen Tools auswerten.*
- *Früher: nur RDP-Zugriff auf Produktionsdaten, keine flexible Nutzung.*
- *Lösung: Historian in IT-Umgebung, gespeist per OPC UA.*
- *Diode überträgt Daten sicher aus SPS durch DMZ → Historian.*



Use Case 2

Produktionsnetz sauber segmentieren

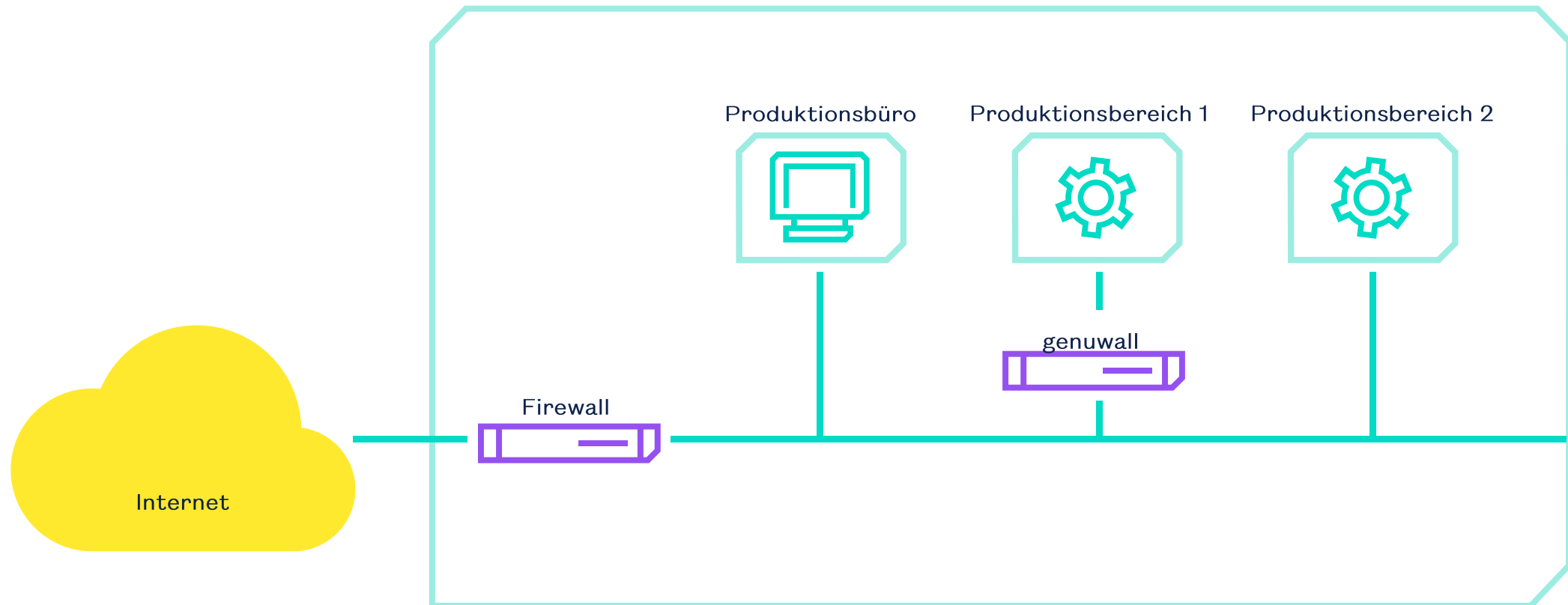
Wie trennen wir Linien, Zellen und Übergänge so, dass Malware nicht das ganze Werk lahmlegt – ohne Adresspläne umzubauen und ohne die Produktion zu stören?



Use Case 2

Produktionsnetz sauber segmentieren

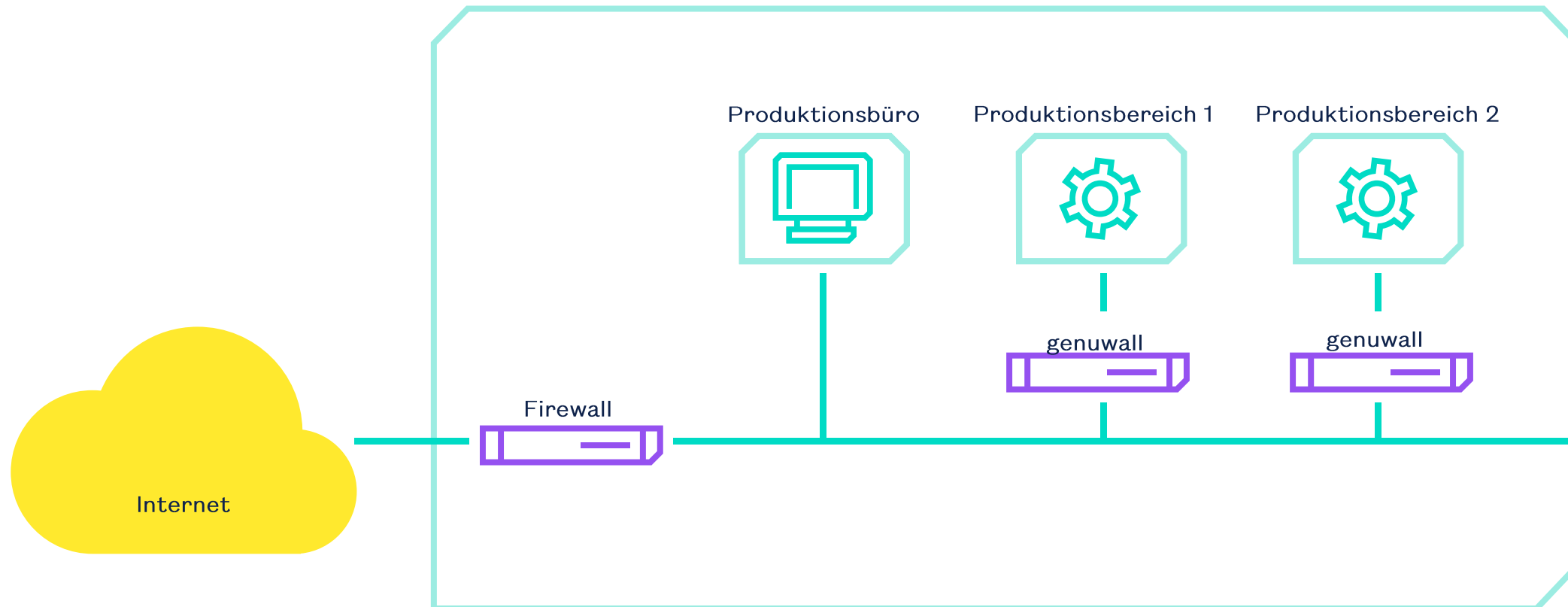
Wie trennen wir Linien, Zellen und Übergänge so, dass Malware nicht das ganze Werk lahmlegt – ohne Adresspläne umzubauen und ohne die Produktion zu stören?



Use Case 2

Produktionsnetz sauber segmentieren

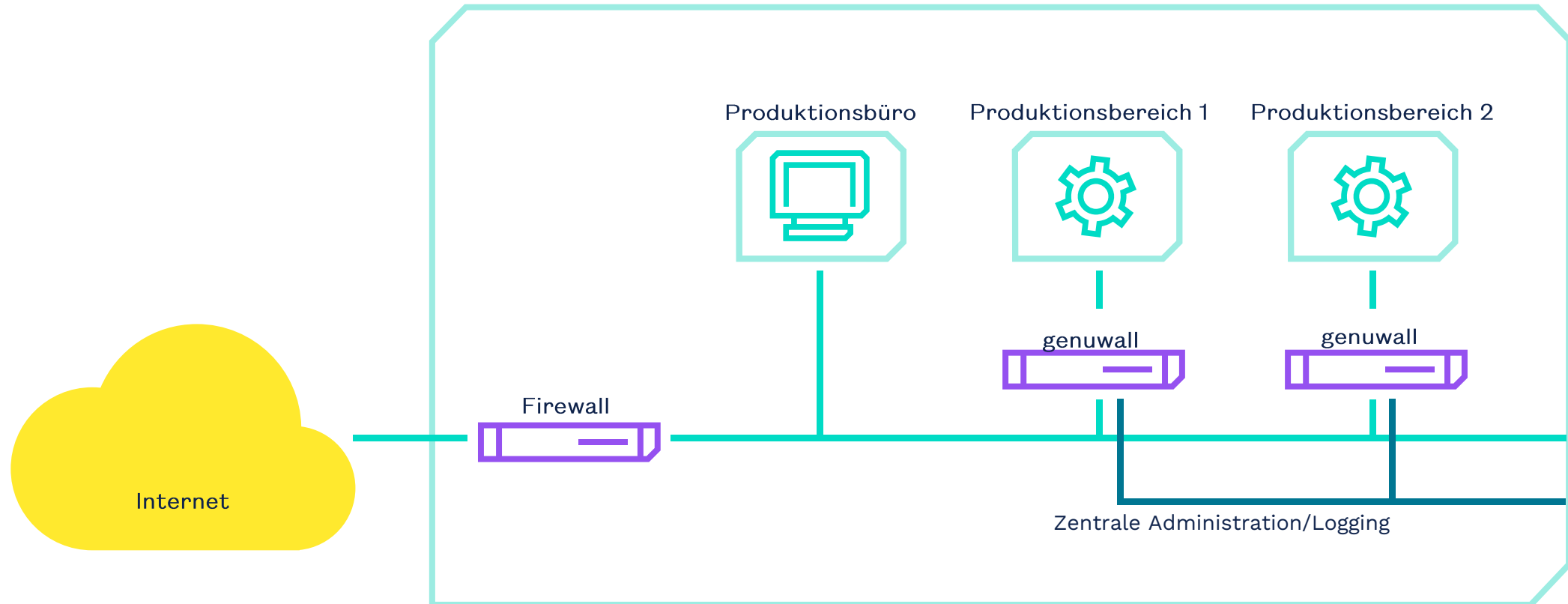
Wie trennen wir Linien, Zellen und Übergänge so, dass Malware nicht das ganze Werk lahmlegt – ohne Adresspläne umzubauen und ohne die Produktion zu stören?



Use Case 2

Produktionsnetz sauber segmentieren

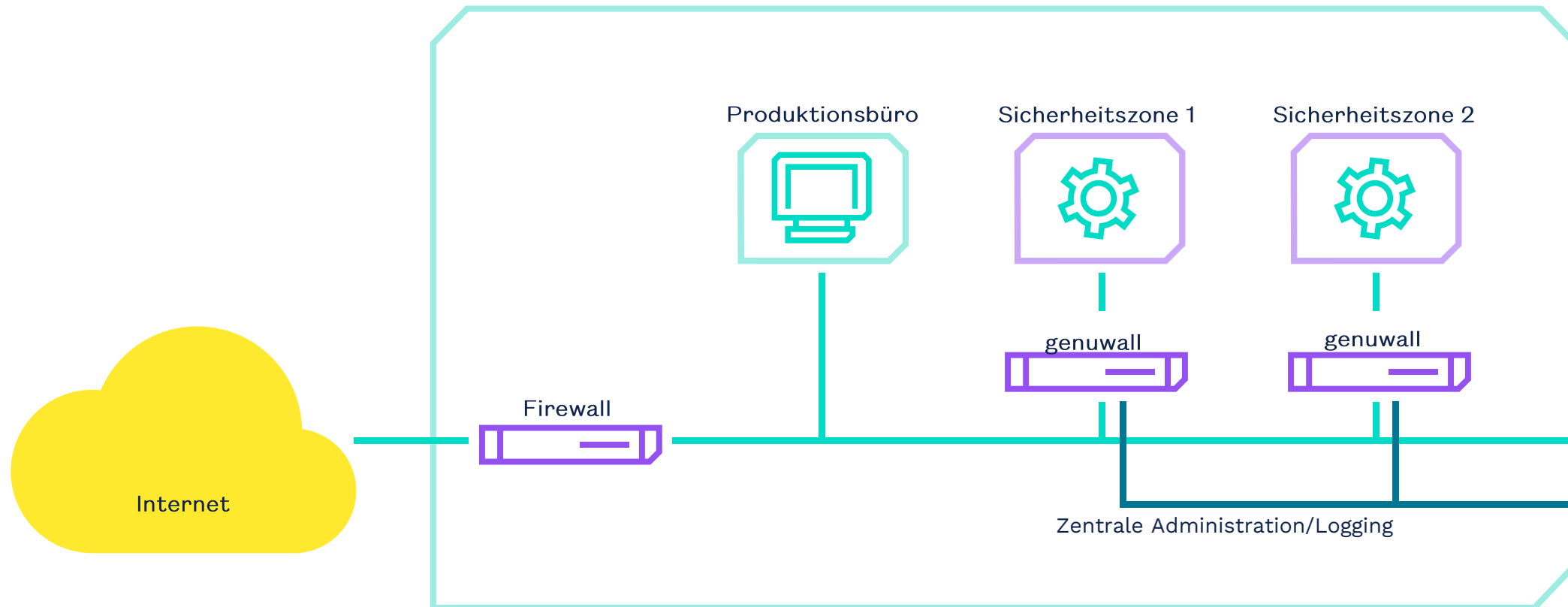
Wie trennen wir Linien, Zellen und Übergänge so, dass Malware nicht das ganze Werk lahmlegt – ohne Adresspläne umzubauen und ohne die Produktion zu stören?



Use Case 2

Produktionsnetz sauber segmentieren

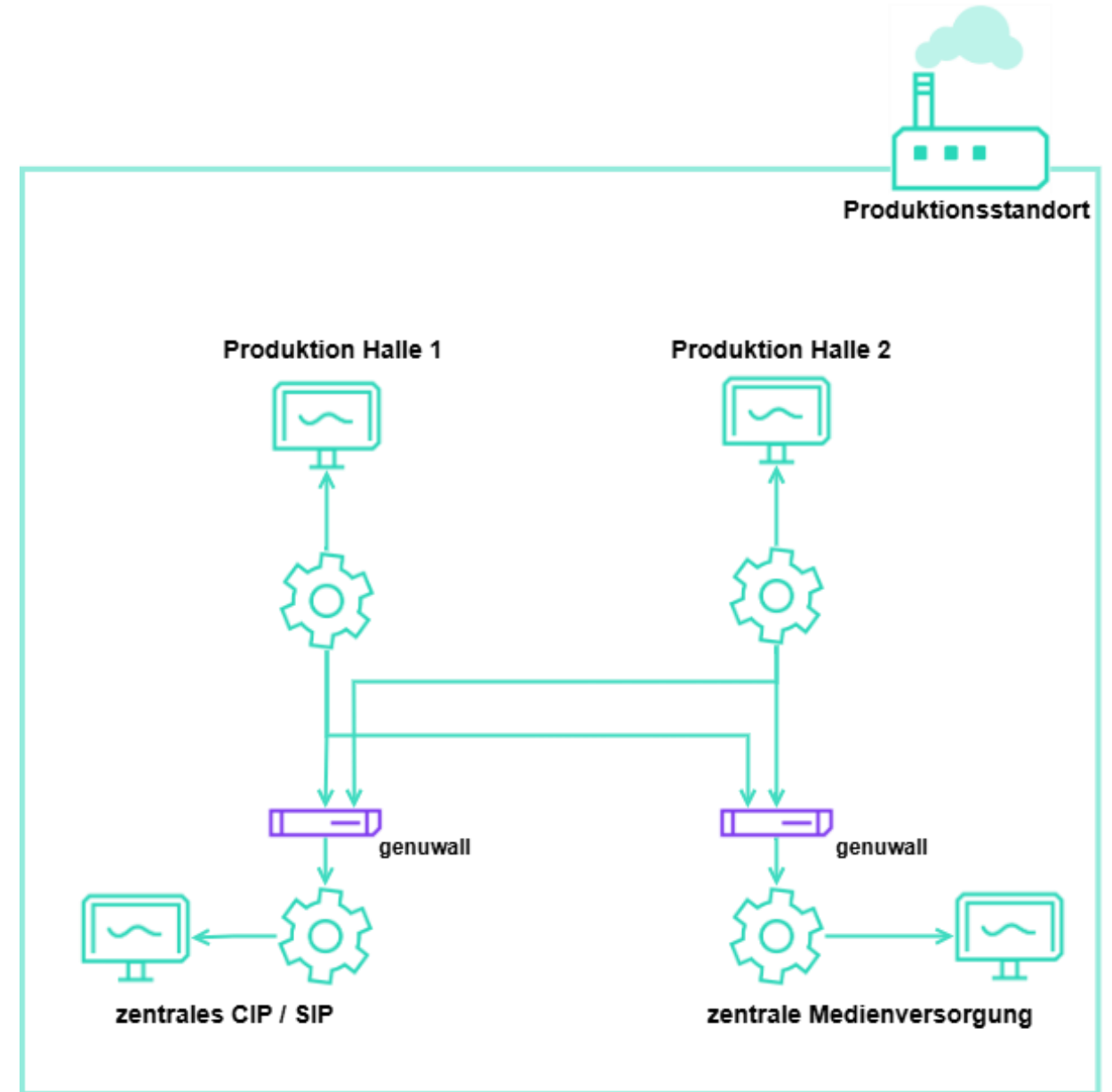
Wie trennen wir Linien, Zellen und Übergänge so, dass Malware nicht das ganze Werk lahmlegt – ohne Adresspläne umzubauen und ohne die Produktion zu stören?



In Praxis

Produktionsnetz sauber segmentieren

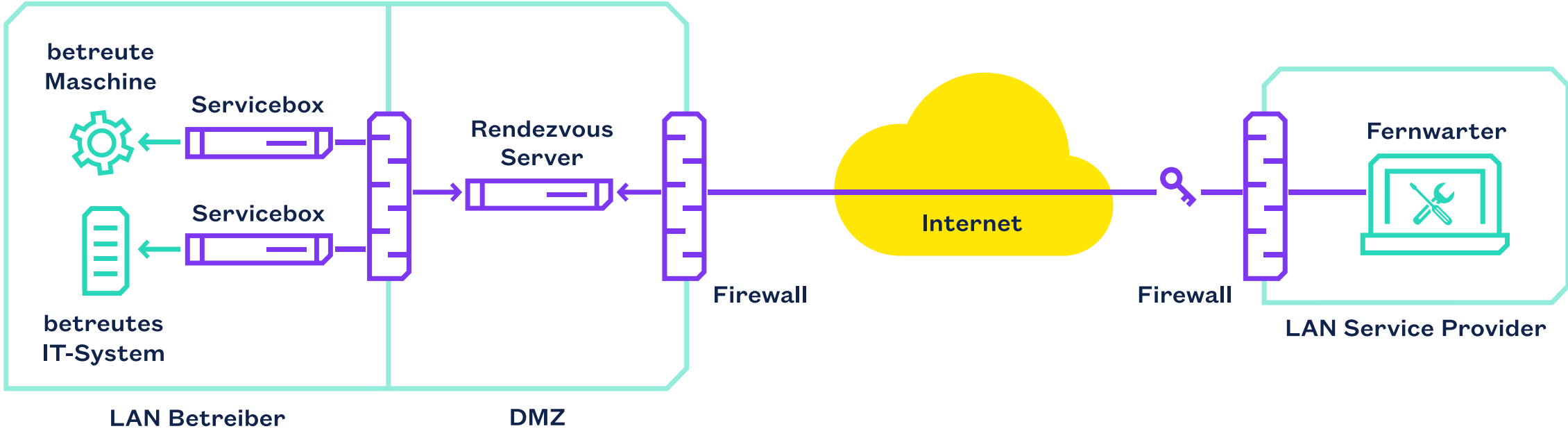
- *Mehrere Linien brauchten Zugriff auf zentrale Medienanlagen (Dampf, Wasser, CIP/SIP).*
- *Netze der Linien zwar getrennt, aber über zentrale Anlagen wieder verbunden → Störungen & Risiken.*
- *Mit genuwall als Layer-2-Bridge:*
 - *Netze sauber getrennt,*
 - *keine Rekonfiguration nötig,*
 - *Störungen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



Use Case 3:

Fernwartung ohne offene Hintertüren

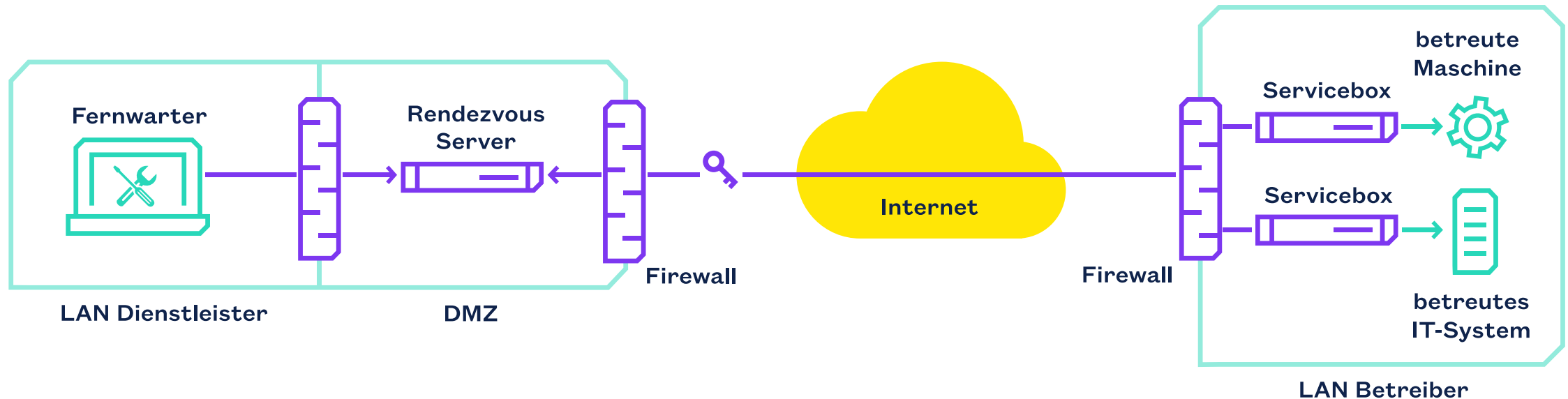
Wie ermöglichen wir Maschinenbauern und Servicepartnern sicheren Fernzugriff – ohne Dauer-VPNs, offene Firewalls oder unkontrollierbare Schatten-IT?



Use Case 3:

Fernwartung ohne offene Hintertüren

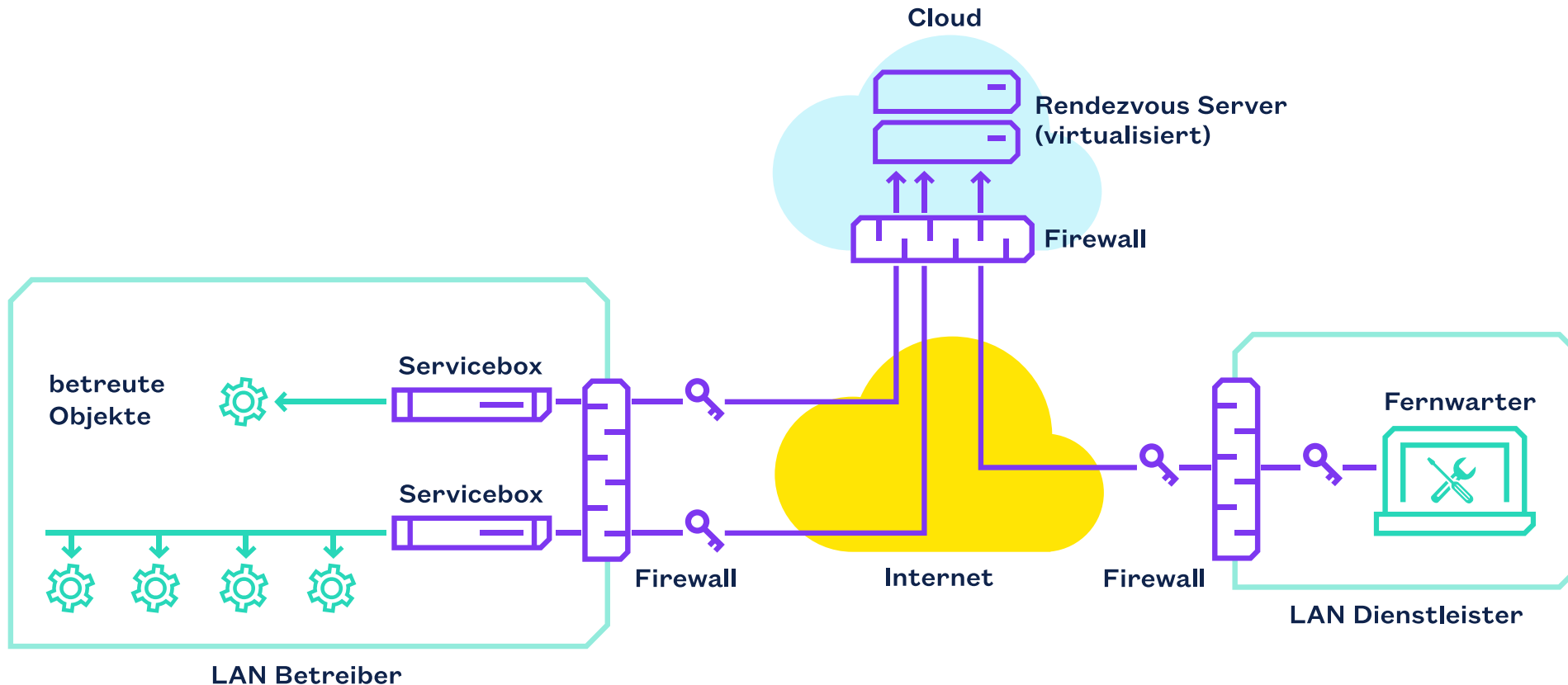
Wie ermöglichen wir Maschinenbauern und Servicepartnern sicheren Fernzugriff – ohne Dauer-VPNs, offene Firewalls oder unkontrollierbare Schatten-IT?



Use Case 3:

Fernwartung ohne offene Hintertüren

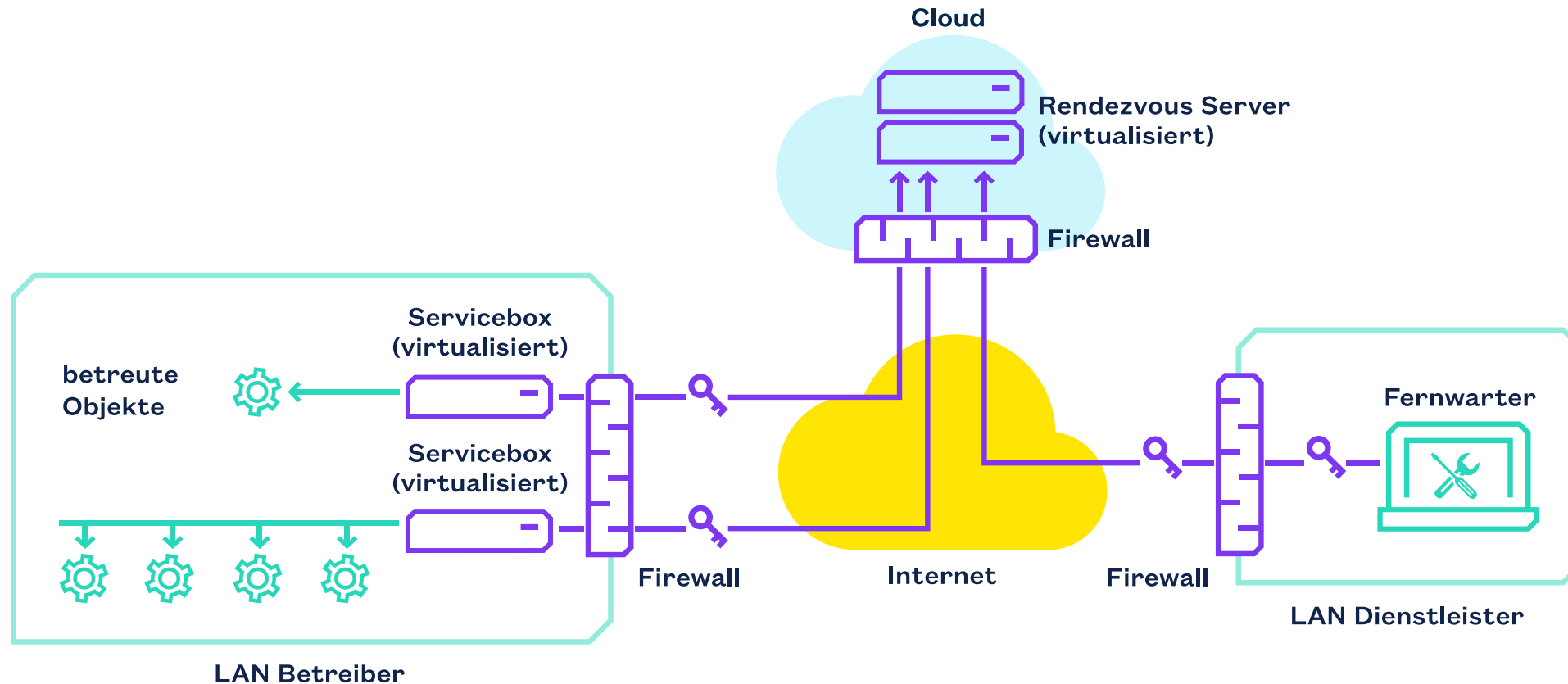
Wie ermöglichen wir Maschinenbauern und Servicepartnern sicheren Fernzugriff – ohne Dauer-VPNs, offene Firewalls oder unkontrollierbare Schatten-IT?



Use Case 3:

Fernwartung ohne offene Hintertüren

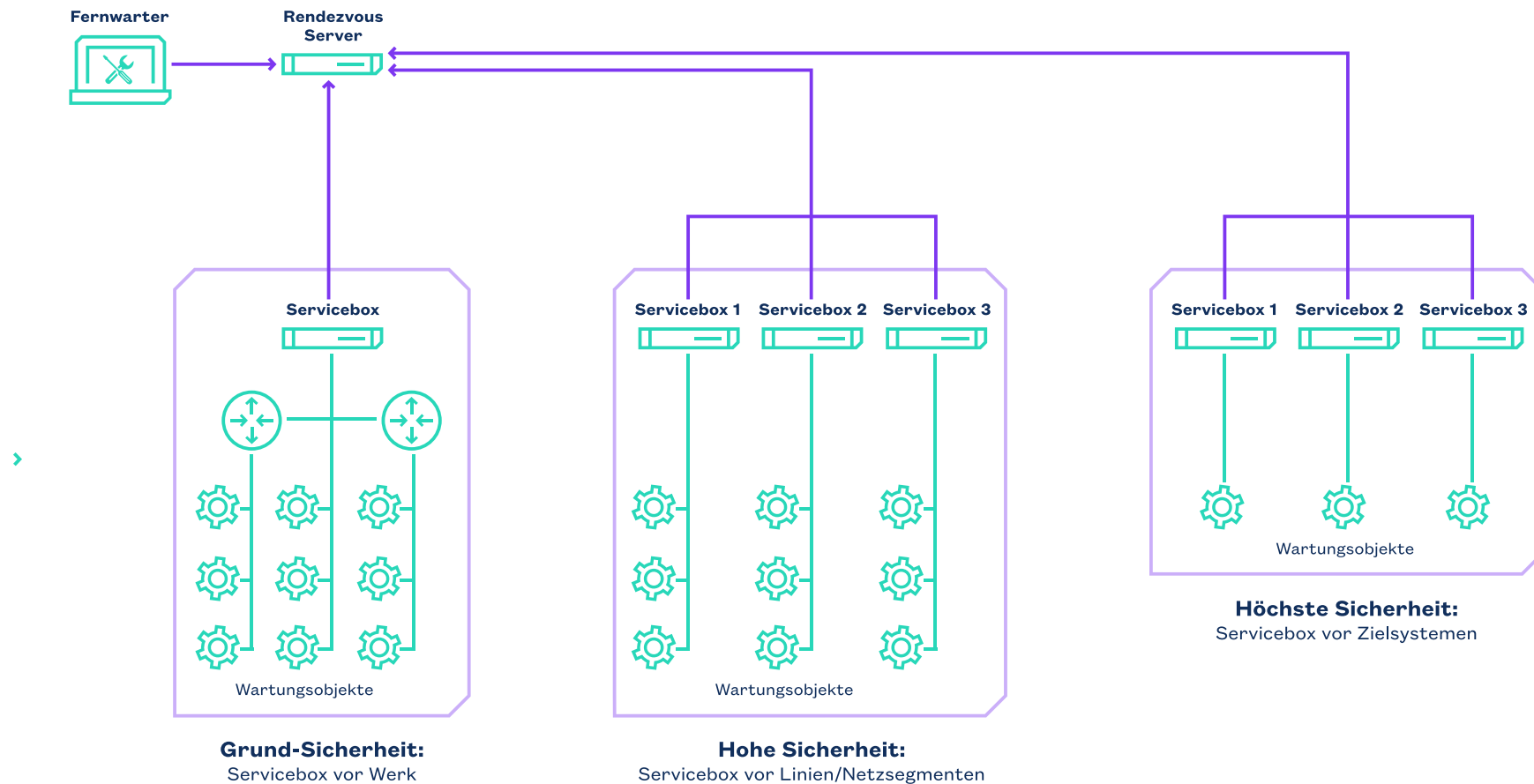
Wie ermöglichen wir Maschinenbauern und Servicepartnern sicheren Fernzugriff – ohne Dauer-VPNs, offene Firewalls oder unkontrollierbare Schatten-IT?



Use Case 3:

Fernwartung ohne offene Hintertüren

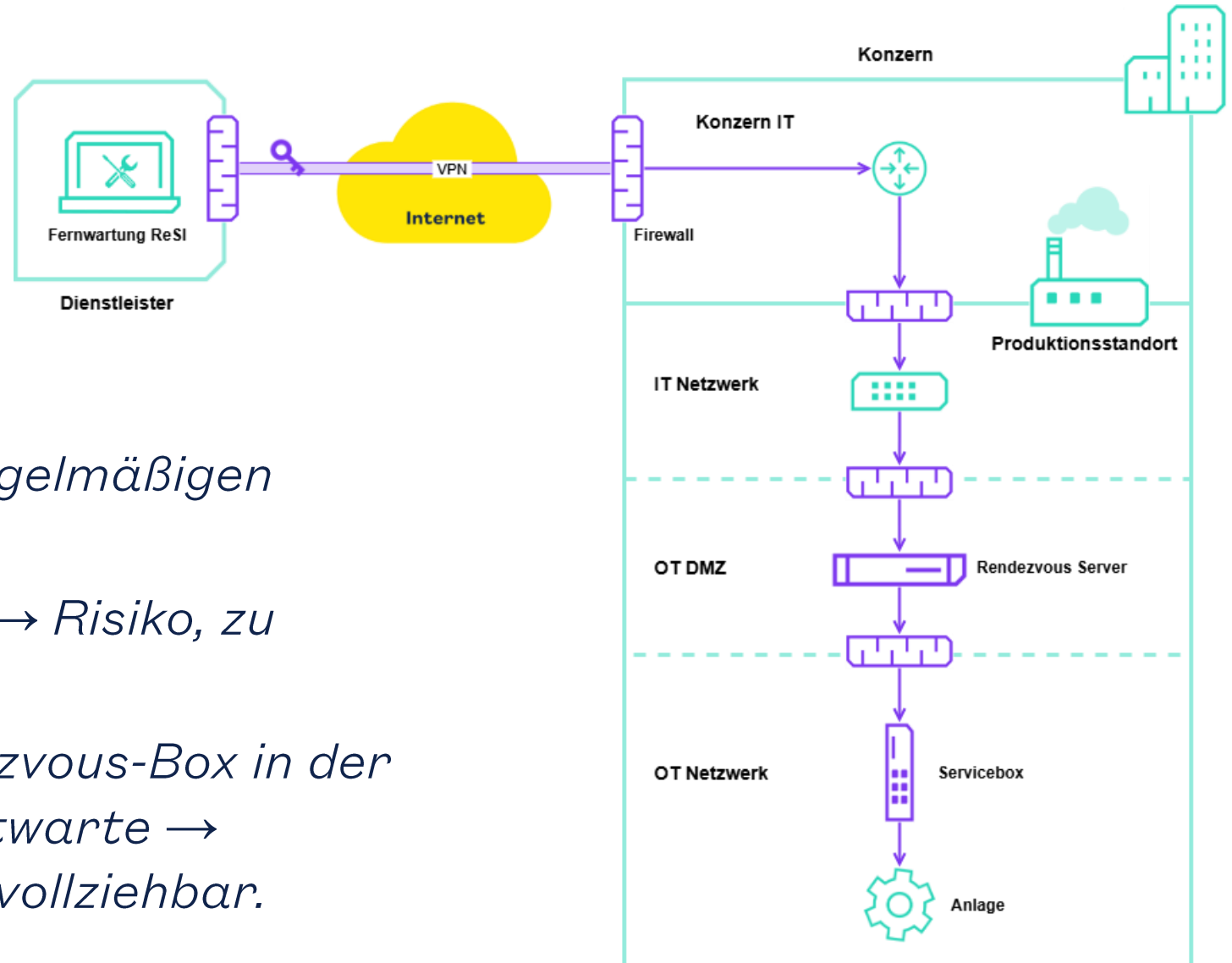
Wie ermöglichen wir Maschinenbauern und Servicepartnern sicheren Fernzugriff – ohne Dauer-VPNs, offene Firewalls oder unkontrollierbare Schatten-IT?

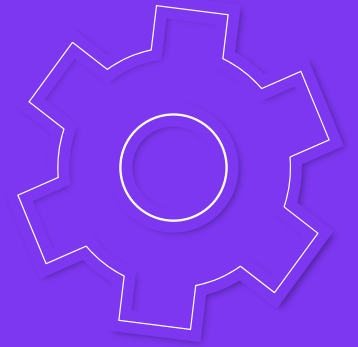
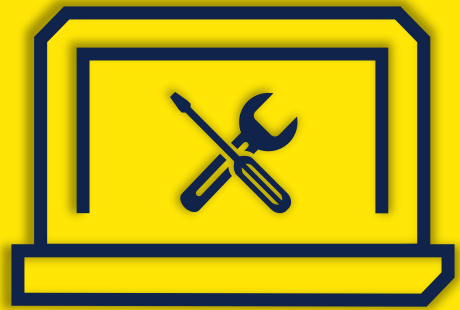


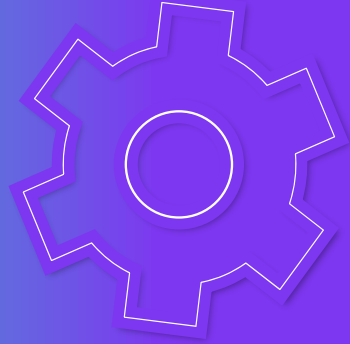
In Praxis:

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



...wie geht es weiter?

Controlware Veranstaltungen: IT – Aktuell & Informativ

Roadshow

11.11.25 Oberhausen
13.11.25 Frankfurt
18.11.25 München
20.11.25 Stuttgart
25.11.25 Berlin

Network Day on Tour 2025

Sie erfahren, wie Sie Ihr Netzwerk effizienter, sicherer und transparenter betreiben können – von der Edge bis zur Cloud. Wir zeigen Ihnen reale Anwendungsfälle aus der Praxis auf sowie neue Ansätze zur Automatisierung und ganzheitlichen Steuerung komplexer Netzwerke.

Webcast

18.11.25 16:00 – 17:00 Uhr

Cybersecurity trifft GenAI – KI denkt schnell, wir denken sicher. Kontrolle statt Chaos!

Sichere Nutzung von GenAI: Erfahren Sie im Webcast, wie moderne Lösungen für Transparenz, Echtzeit-Risikobewertung und Data Loss Prevention sorgen – für Compliance, Schutz sensibler Daten und volle Kontrolle über KI-gestützte Anwendungen.

Anmeldung & weitere Informationen unter: www.controlware.de/termine