

TeleTrust-interner Workshop

Berlin, 25.06.2026

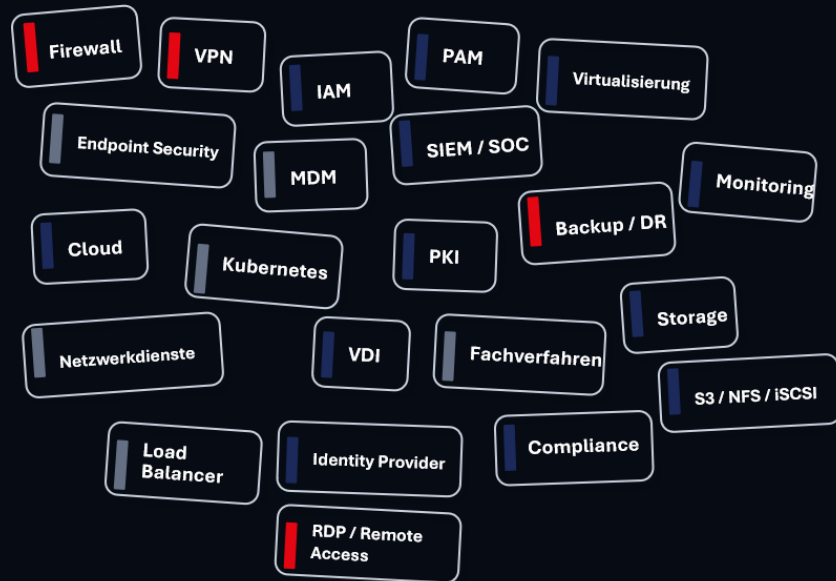
Schnittstellen aktiver Zusammenarbeit statt Silos in der IT-Branche

Yakup Saygin, SAYTEC

Die fragmentierte IT-Realität

Viele Bausteine — aber keine durchgängige Sicherheits- und Betriebsarchitektur

Einzellösungen wachsen schneller als die Architektur, die sie verbinden soll.



Fleckenteppich



RISIKO 1

Angriffsflächen wachsen

KI-gestützte Angriffe, Remote Work und Supply-Chain-Risiken.

RISIKO 2

Regulatorischer Druck steigt

NIS2, BSI-Anforderungen und DSGVO erhöhen den Nachweisdruck.

RISIKO 3

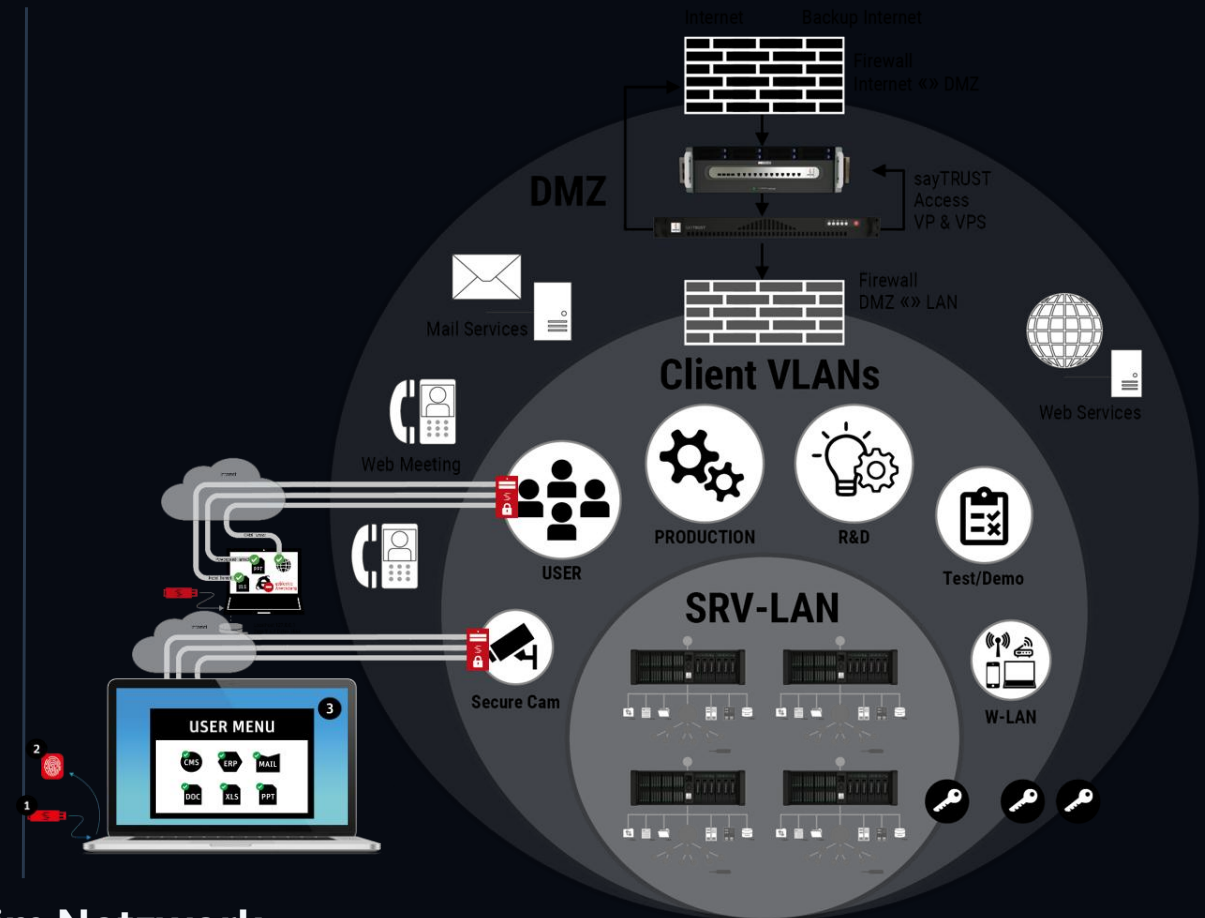
Souveränität wird kritisch

Insellösungen und Abhängigkeiten schwächen Betriebskontinuität.

Das Problem ist nicht der fehlende einzelne Security-Baustein, sondern die fehlende verbindende Sicherheits- und Resilienz-Architektur.

Zwei Ebenen, ein Zielbild

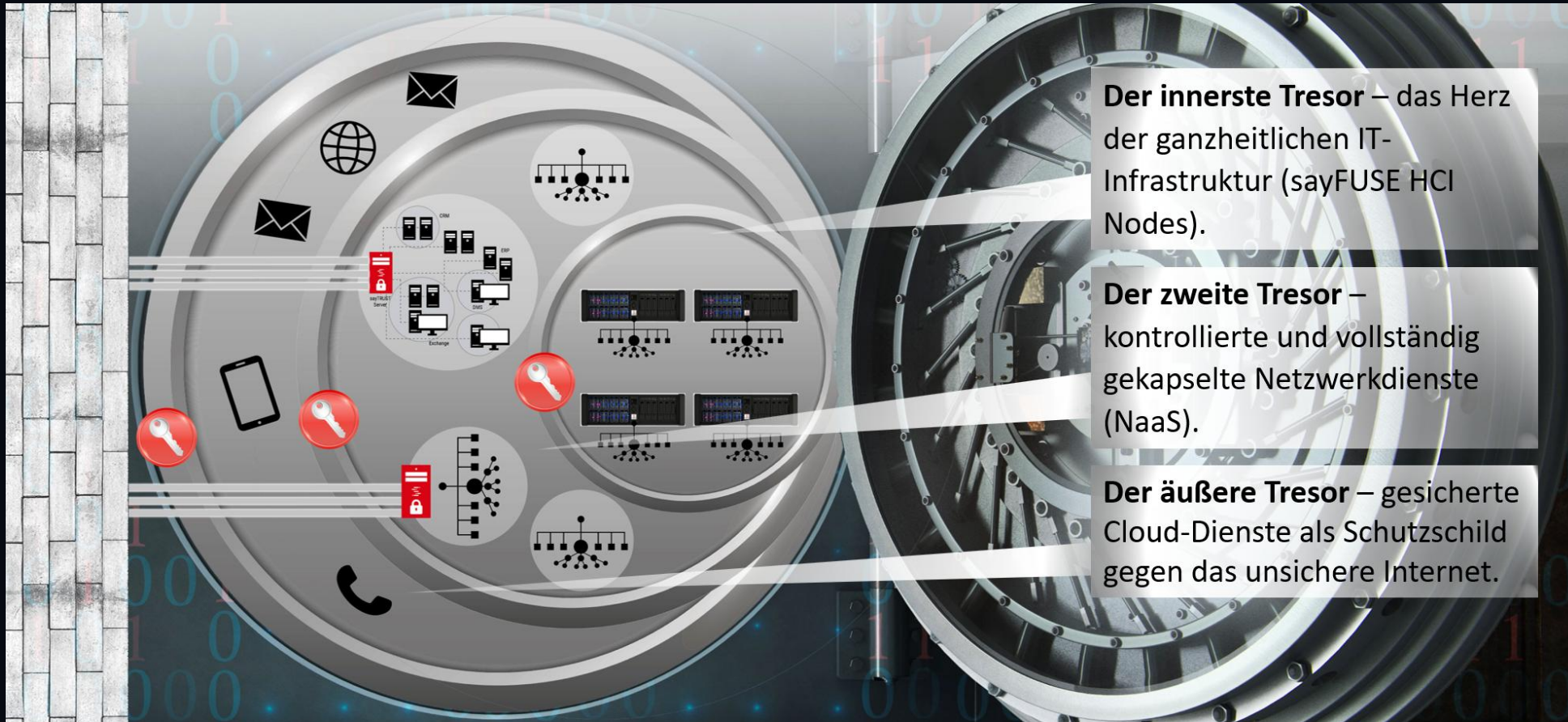
Post Zero Trust schützt den Zugriff – die Betriebsplattform schützt Betrieb, Daten und Wiederherstellbarkeit



Botschaft: Nutzer arbeitet in Anwendungen – nicht im Netzwerk.

Ganzheitliche IT-Betriebsplattform als resilientes Fundament

Tresor-in-Tresor: physische und logische Separation statt unkontrollierter Kopplung



Sie sichert nicht nur Zugriff, sondern Betrieb, Daten, Anwendungen und Wiederherstellbarkeit.

Kernaussage **Schutzschirm für Betrieb, Daten, Anwendungen, Wiederherstellbarkeit und Skalierbarkeit**

Schnittstellen aktiver Zusammenarbeit statt Silos

Partnerlösungen werden nicht addiert — sie werden über definierte Schnittstellen architektonisch integriert



Was TeleTrust-Mitglieder gemeinsam definieren könnten.

1 Referenzarchitektur

2 Schnittstellen

3 Integrationsszenarien

4 Whitepaper