

Fallstudie eines Kunden

Finanzsektor – Prävention von Datenschutzverletzungen



Seit der Installation des eperi Gateway hat der Kunde keinerlei offensichtliche Datenschutzverletzungen erlebt.



Fallstudie eines Kunden

Finanzsektor – Prävention von Datenschutzverletzungen

On-Premises



- Data Residency bei der Übertragung, Verwendung und Speicherung
- Schutz vor internen und externen unbefugten Datenzugriffen



- 100%ige Verhinderung eines Datenzugriffs durch interne System- und Datenbank-Administratoren
- 0 offengelegte Datenschutzverletzungen seit Installation des eperi Gateway



„Seit der Installation der eperi Datenschutzlösung können wir alle kritischen Kundendaten ohne Leistungsminderung schützen.“

Kunde

Internationale
Privatbank mit Sitz in der Schweiz

Problem

Unser Kunde, eine in der Schweiz ansässige Bank, die **405 Milliarden Euro an Vermögenswerten** managt, verwaltete ihre Kundendaten früher über intern ungeschützte Rechenzentren. Geheime Kundendaten waren für Systemadministratoren im Klartext zugänglich. Aufgrund verschiedener Datenschutzverletzungen in der Vergangenheit entschied die Unternehmensleitung, weitere **Datenverluste mithilfe eines Dienstes für die Verschlüsselung und Tokenisierung** schutzpflichtiger Daten zu verhindern.

Lösung

Mit dem **eperi Gateway** zum sicheren Schutz vertraulicher Kundendaten werden kritische **Unternehmensdaten in den verschiedenen Rechenzentren** weltweit pseudonymisiert.

Projekt

Verschlüsselung von sensiblen Kundendaten

