Controlware Security Day 2022

THALES

controlware

Schrems II und dessen Folgen – Wie erreiche ich Konformität bei den Hyperscalern?

Compliance und Datensicherheit mittels Verschlüsselung

Tobias Pollett
Channel Sales Manager

Agenda

01 Ausgangslage Datensicherheit

02 Compliance - Schrems II

03 Digitale Souveränität

04 Nächste Schritte

Wie steht es um Datensicherheit?

Source: 2022 Thales Data Threat Report

Wieso speichern Unternehmen sensible Daten in der Cloud?

Cloud-first Strategie

Kostensenkung

Innovative Services

THALES
Building a future we can all trust

THALES
Building a future we can all trust

controlware

Compliance

Grundlagen von Schrems II

Schrems II – EuGH Urteil vom 16. Juli 2020

Übertragung personenbezogener Daten

- Privacy-Shield mit USA für ungültig erklärt

Standardvertragsklauseln können weiterhin genutzt werden

- technische und organisatorische Maßnahmen
- DSGVO verlangt Verschlüsselung & Kontrolle über Schlüssel

Frist zur Umstellung für Bestandsverträge 27.12.22

- Datenübermittlung einstellen oder Bußgeld

Privacy Shield 2.0

Privacy Shield 2.0: USA geloben "beispiellose" Überwachungsreform

Die EU-Kommission und die US-Regierung haben erste Details zum geplanten neuen "Transatlantischen Datenschutzrahmen" bekannt gegeben.

Lesezeit: 5 Min. In Pocket speichern 53

US-Präsident Joe Biden und Kommissionspräsidentin Ursula von der Leyen nach ihrem Treffen am Freitag in Brüssel. (Bild: EU-Kommission/Christophe Licoppe)

26.03.2022 17:08 Uhr

Schrems: Nur Zusicherungen, nicht einklagbar

Zugleich bestätigten die Kommission und die US-Regierung, dass die Zusagen Washingtons nur in eine Durchführungsverordnung ("Executive Order") aufgenommen werden sollen. Die von Schrems gegründete Datenschutzorganisation Noyb hatte zuvor kritisiert, dass die USA "keine Änderungen ihrer Überwachungsgesetze, sondern lediglich Zusicherungen der Exekutive" planten. Diese hätten "keine externe Wirkung und können nicht eingeklagt werden". Eine echte Lösung wie ein "No-Spy-Abkommen" mit "Basisgarantien unter gleichgesinnten Demokratien" stehe weiter aus.

CSP investieren hohe Summen in Cloud-Security. Sind die nativen Security-Optionen ausreichend?

Native Verschlüsselung der Hyperscaler

CMEK, CKMS, Cloud HSM

Für personenbezogene Daten nicht geeignet !

KEK, SSE, TDE, CLE, MEK, DEC

*Data-at-Rest-Verschlüsselung auch in Kombination“ (stellt) „**keine zusätzliche Maßnahme** dar, die ein im Wesentlichen gleichwertiges Schutzniveau gewährleistet, wenn der **Datenimporteur im Besitz der kryptografischen Schlüssel ist.“***

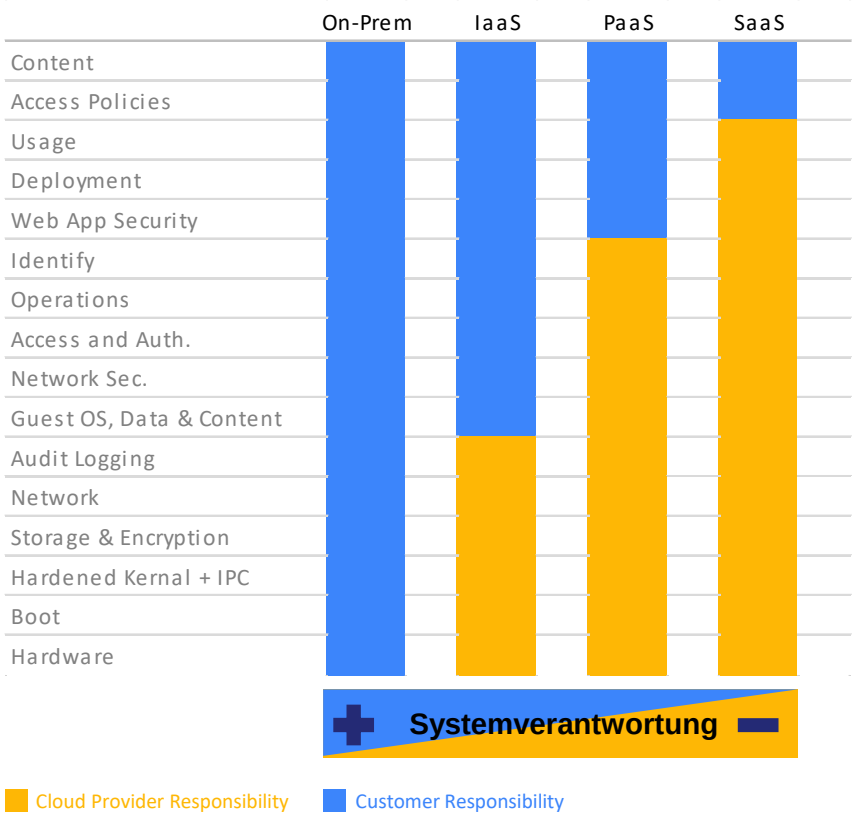
Modell der geteilten Verantwortung

CSP-Verantwortlichkeit

- Sicherheit der Cloud

Kundenverantwortlichkeit

- Sicherheit in der Cloud



THALES
Building a future we can all trust

THALES
Building a future we can all trust

controlware

Wie erreicht man Compliance in der Cloud?

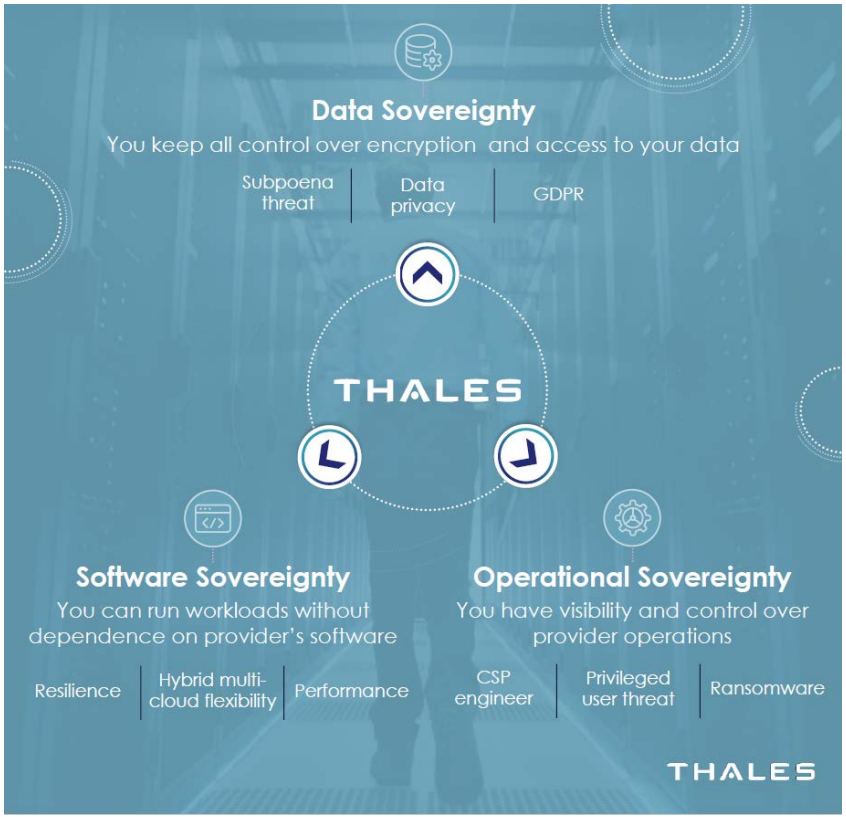
Digitale Souveränität

Was bedeutet Digitale Souveränität?

> **Digitale Souveränität meint die Kontrolle über das eigene digitale Schicksal zu bewahren – die Daten, Hardware und die Software, von denen Sie abhängig sind.**

Sources: übersetzt aus https://www.weforum.org/agenda/2021/03/europe-digital-sovereignty/

3 Säulen der Digitalen Souveränität



Datensouveränität

- Kontrolle über die Verschlüsselung und den Zugriff auf Ihre Daten

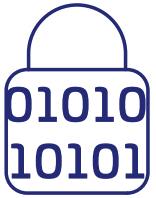
Operative Souveränität

- Sichtbarkeit und Kontrolle über den Betrieb des Anbieters

Software Souveränität

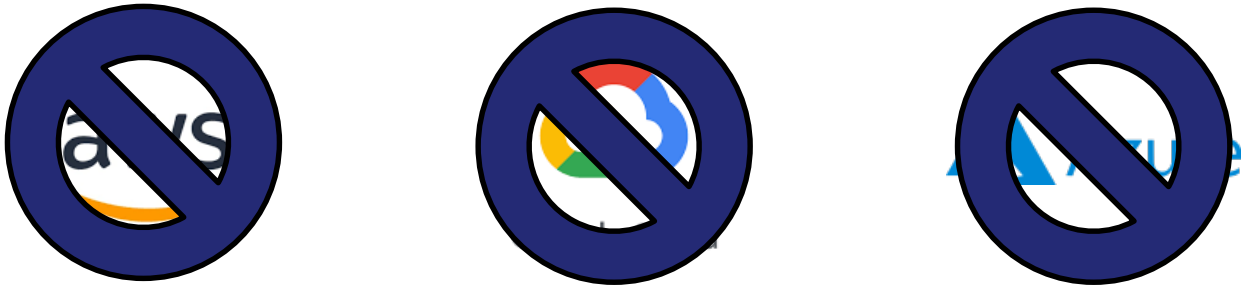
- Workloads ohne Abhängigkeit des Providers ausführen

THALES
Building a future we can all trust



Wie kann man Datensouveränität technisch umsetzen?

Lösungsansatz #1: Datentransfer stoppen



Datensouveränität durch Verschlüsselung

Native Verschlüsselung

- Für Daten ohne sensiblen Inhalt

BYOK

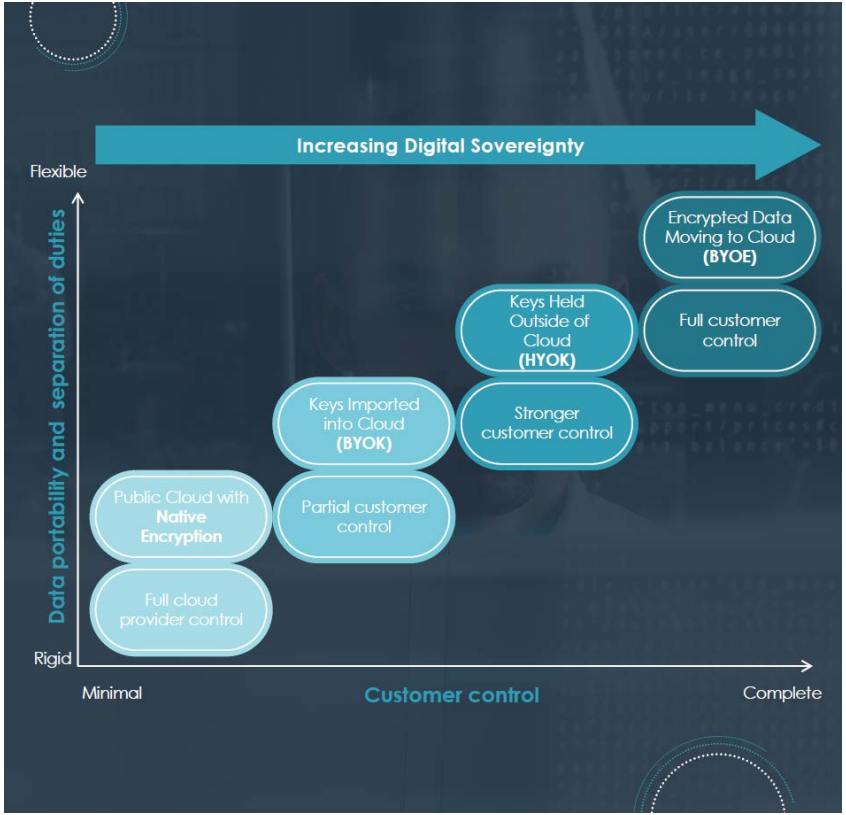
- Erhöht die Kontrolle des Kunden, da Schlüssel extern erstellt und verwaltet werden

HYOK

- Kunde behält die volle Kontrolle über seine Schlüssel und erfordert somit die Anforderungen von Schrems II

BYOE

- Bietet Cloud-Kunden die größte Kontrolle, da die eigene Verschlüsselungssoftware genutzt wird



THALES
Building a future we can all trust

Lösungsansatz #2: Key Management Plattform

Discover

Daten finden und klassifizieren

Protect

Daten überall schützen

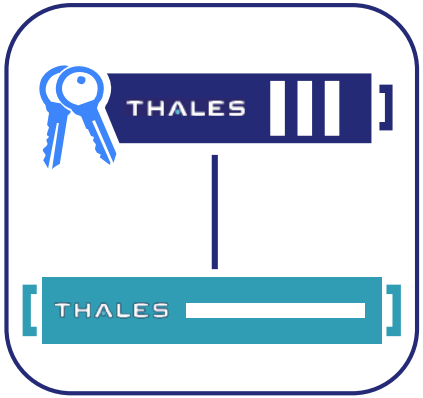
Control

Betrieb sicherstellen und Monitoring

Key Management System

Hardware Security Module

Key Management Plattform



THALES
Building a future we can all trust

Integrationen mit Hyperscalern

aws

Thales Solutions for Amazon Web Services
Bring Your Own Advanced Encryption, Bring Your Own Key or
AWS xKS

Microsoft Azure

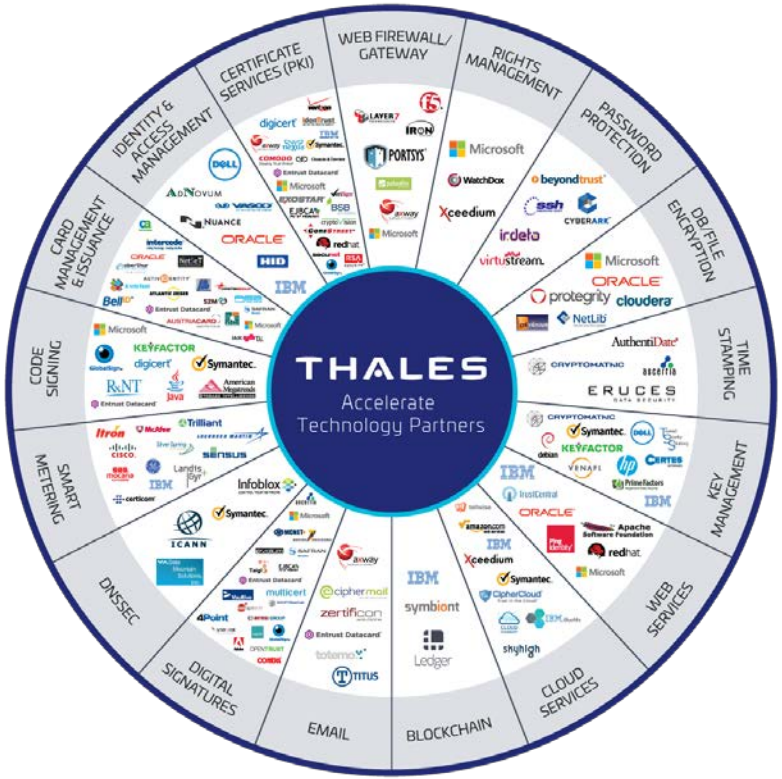
Announcing Thales HSM Backed Double Key Encryption for Microsoft Office 365 – The best of both worlds.

October 5, 2020

Google Cloud

Enhancing Encryption Key Control and Data Security in Google Cloud Platform

Technologiepartner & Use-Cases



Mehr als 400 Lösungsintegrationen, die auf der CipherTrust Plattform basieren

- App, File & Database Encryption
- Big Data
- Blockchain
- Card issuance/Mgmt
- Cloud Services
- Code Signing
- Container
- Data Tokenization
- Digital Signatures
- EID ePassport
- Email
- EMV Test Tools
- Firewall
- HCI
- IAM
- IoT
- Key Management
- Mobile Payments
- OS Encryption
- PAM
- Password Protection
- Payments
- Rights Management
- PKI / Cert Services
- Secure Manufacturing
- Quantum
- Secrets Management
- SIEM Tools
- Smart Metering
- Storage
- Time Stamping
- TLS/SSL
- Web Firewall / Gateway

THALES
Building a future we can all trust

controlware

Nächste Schritte

Der Weg zur Datensicherheit

Mal abwarten ...

“Firewall”
Native Verschlüsselung

Verschlüsseln, um compliant zu sein

HYOK

Verschlüsseln, um sicher zu sein

BYOE

Next steps

Lassen Sie uns einen **Security Workshop** planen. Was wollen wir im Detail besprechen?

- **Compliance & Datensouveränität**
- **Datenströme im Unternehmen absichern**
- **Multi-Cloud Key Management**
- **Modernisierung der unternehmensweiten Authentifizierung**

controlware

THALES
Building a future we can all trust

controlware

Data Protection

Tobias Pollett – Channel Sales Manager