SAPinsider

Securing Finance and ERP Data with Encryption, Tokenization and Key Management

Alex Hanway — December 2021

THE MOST TRUSTED INDEPENDENT
INFORMATION SOURCE FOR SAP
ENTERPRISE SOFTWARE CONTENT

SAPINSIDER COMMUNITY
500,000+ STRONG

Alex Hanway

Business Development Director at Thales

- 10+ years' experience in marketing and strategic partnerships
- Database, Big Data and Cloud Native technology partnerships

What We’ll Cover

- Challenges of Securing Sensitive Data
- Strategies for Securing Sensitive Data
- Why You Benefit

Challenges of Securing Sensitive Data

Data Security Can Be A Highly Complex Problem

Explosive Data Growth

175

Zettabytes

Global data In 2025

Evolving Compliance Requirements

1800

Global Privacy Laws

Operational Complexity

39%

Complexity is the top barrier for data security deployment

Rapidly Increasing Data Breaches

7.9

Billion

Records breached in 2019

1 - IDC DataAge 2025 whitepaper, Dec 2018
2 - https://www.pwc.com/us/en/library/risk-regulatory/strategic-policy/top-policy-trends/data-privacy.html
3. Thales DTR 2020
4. Risk based security, 2019 Year end report

Problem statement unique to finance customers

- Increased prevalence of security threats
  - Finance data and applications are attractive targets
- Consumer Expectations & Compliance
  - Customers want their data kept safe. Regulations demand it.
- Supplier Risk
  - Can you trust your partners to secure your data too?
- Privileged Insider Risk
  - Who is watching the watchers?

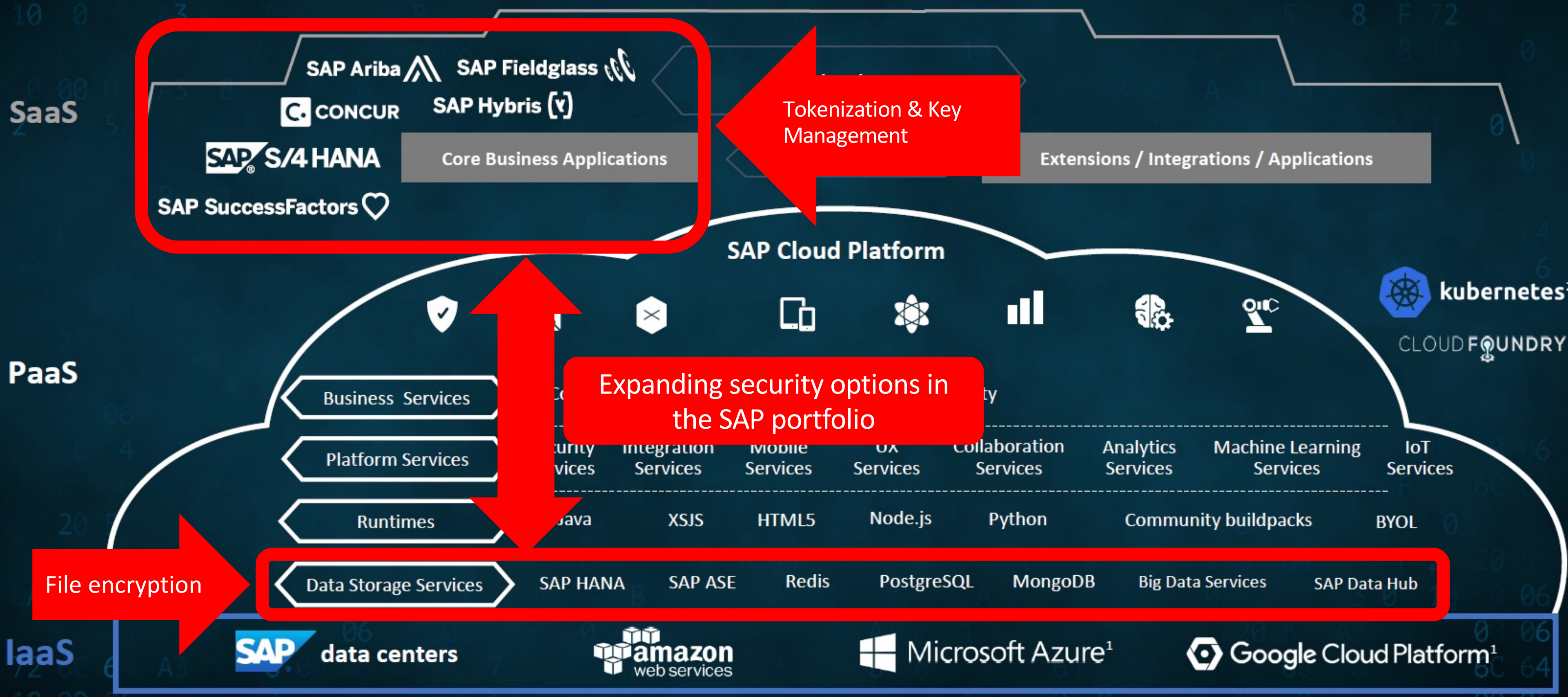
Strategies for Securing Sensitive Data

Database Specific Risk

Technology Layer	Data Risks
Cloud	• Improper access • Data leakage • Compliance violations • Lack of access monitoring
Container	• Improper access • Privilege escalation • Lack of access monitoring
Application	• Data leakage • Compliance violations
Database	• Improper DBA access • Data leakage • Compliance violations
File and Volume	• Improper access • Privilege escalation • Lack of access monitoring
Storage	• Hardware disposal • Physical theft

A Growing Playing Field

Click on Sign to
signatures on a



SaaS

SAP Ariba

SAP Fieldglass

CONCUR

SAP Hybris

SAP S/4HANA

Core Business Applications

SAP SuccessFactors

Tokenization & Key Management

Extensions / Integrations / Applications

SAP Cloud Platform

kubernetes

CLOUD FOUNDRY

PaaS

Business Services

Platform Services

Runtimes

Expanding security options in the SAP portfolio

urity vices

Integration Services

Mobile Services

UX Services

Collaboration Services

Analytics Services

Machine Learning Services

IoT Services

Java

XSJS

HTML5

Node.js

Python

Community buildpacks

BYOL

File encryption

Data Storage Services

SAP HANA

SAP ASE

Redis

PostgreSQL

MongoDB

Big Data Services

SAP Data Hub

IaaS

SAP data centers

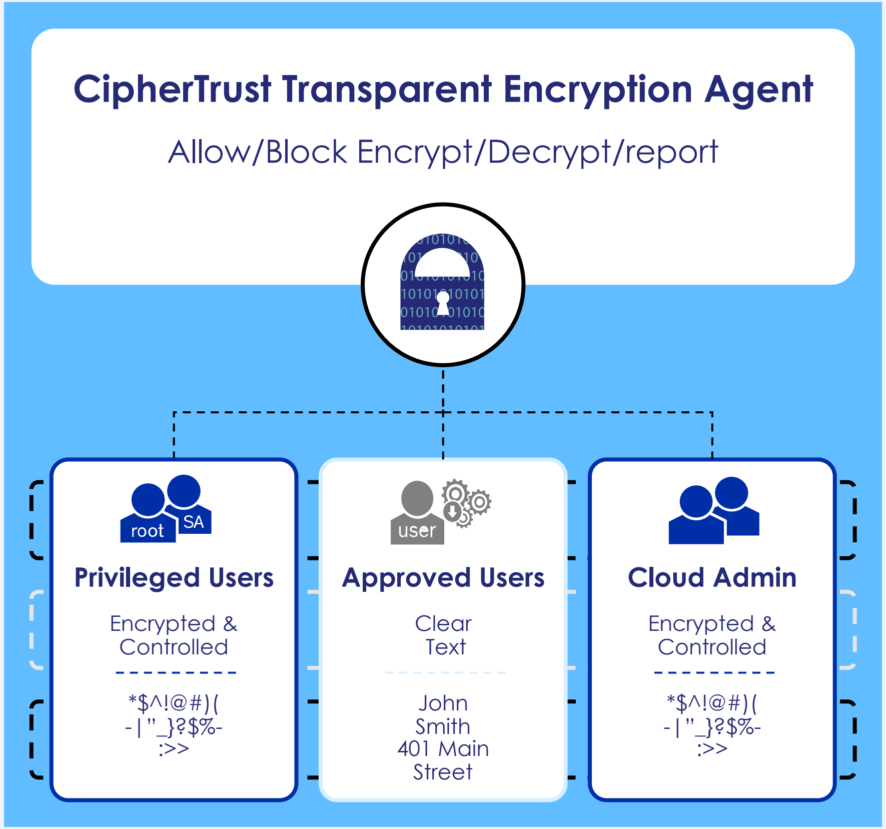
amazon web services

Microsoft Azure[1]

Google Cloud Platform[1]

File System-level Encryption

Transparently protects file system, volume data-at-rest



CipherTrust Transparent Encryption Agent

Allow/Block Encrypt/Decrypt/report

Privileged Users

Encrypted &
Controlled

*$^!@#)(
-|"_}?$%-
:>>

Approved Users

Clear
Text

John
Smith
401 Main
Street

Cloud Admin

Encrypted &
Controlled

*$^!@#)(
-|"_}?$%-
:>>

Transparent, file-level encryption

- No need to re-architect SAP HANA, applications, or storage networks

Privileged user access controls

- Allows root users to do their job, without abusing data

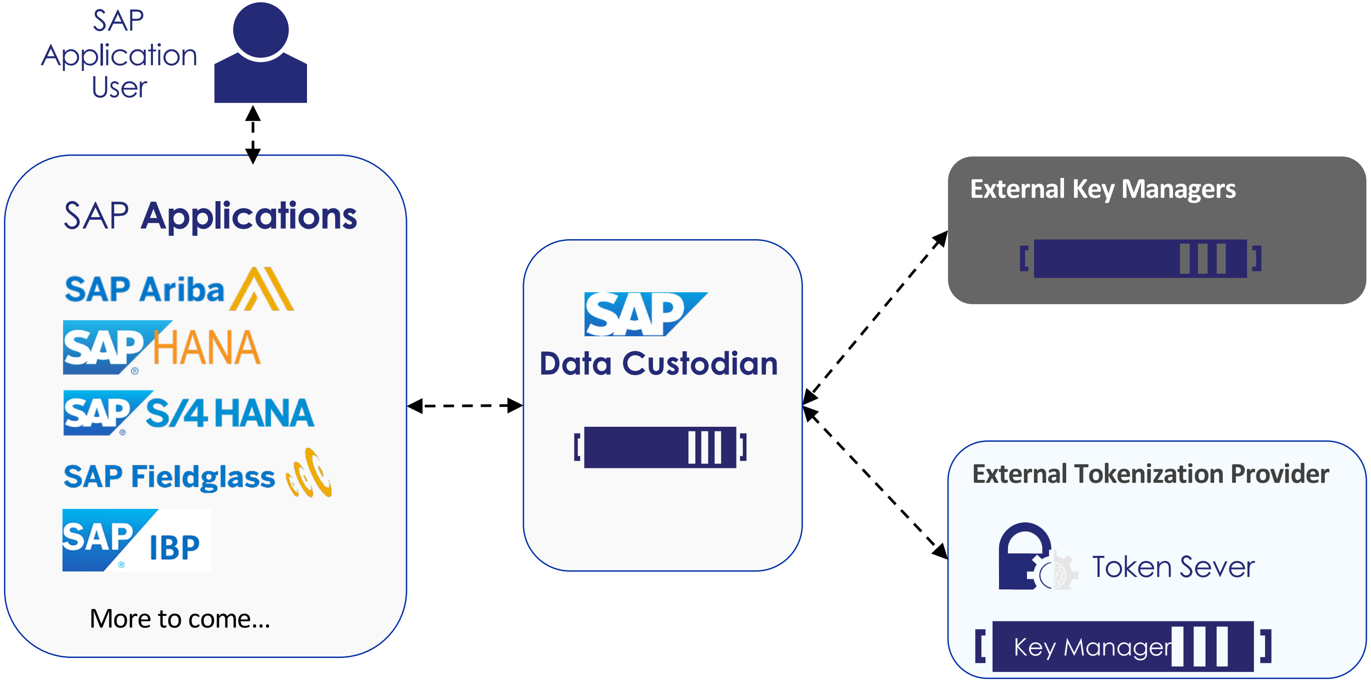
Data access audit logging

- Accelerate threat detection and ease forensics

Centralized encryption key and data access policy management

- Streamline operations, reduce risk, satisfy compliance

SAP Data Custodian: An Interface for 3rd Party Security



Tokenization for SAP

Reduce compliance scope for PCI DSS

Bring data security into SAP applications

Supports any application integrated with the Data Custodian

Policy automation and scheduling

Overview

SAP works with 3rd party security vendors to allow any application that uses the SAP Data Custodian to call out via API for tokenization services. Customers can replace sensitive values with their applications with tokens of the same length and format.

Features

- Administer seamlessly via GUI or API
- Separate responsibilities between token groups with unique access and policies
- Centralized tokenization templates that simplify implementation (i.e. formats, groups, character sets)
- Support for any cloud infrastructure

External Key Management for SAP Data Custodian

FIPS 140-2
Key creation
and backup

Reduce Opex
for key lifecycle
management

AWS
Azure
Salesforce
and more…

Policy
automation and
scheduling

Overview

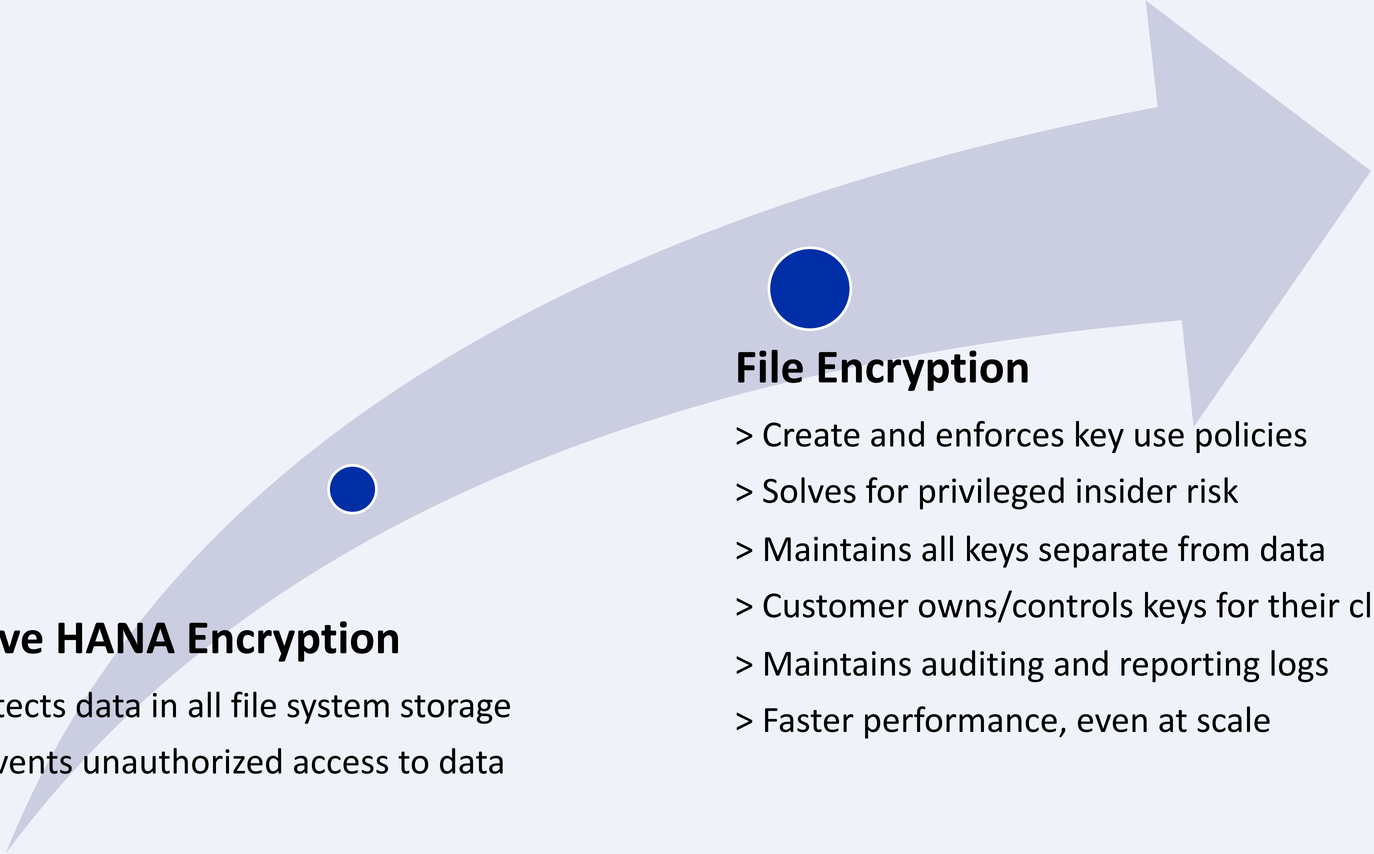
SAP's Data Custodian KMS supports integration with 3rd party key managers to establish stronger controls over a customer's encryption keys and policies to meet compliance and best practice requirements.

Features

- Administer seamlessly via GUI or API
- Abstract Multicloud BYOK Complexity
- Federated User Access to Key Management
- Automated Key Rotation and expiration

Why You Benefit

Native vs. Third Party Encryption – The Difference



Native HANA Encryption

> Protects data in all file system storage

> Prevents unauthorized access to data

File Encryption

> Create and enforces key use policies

> Solves for privileged insider risk

> Maintains all keys separate from data

> Customer owns/controls keys for their cloud data

> Maintains auditing and reporting logs

> Faster performance, even at scale

External Key Management for SAP Data Custodian

Bring your own key to SAP applications

- Centralized key control for SAP applications
- Incorporate SAP keys into your multi-cloud strategy

Enjoy IT efficiency

- Benefit from centralized full key lifecycle management

Inform your IT execution

- Auditing functionality gives customers greater visibility and reporting of their key usage for SAP applications

Achieve internal & industry compliance

- Separate encryption keys from data according to best practice and regulation
- Use key usage reports to demonstrate data control to auditors

Application Tokenization via SAP Data Custodian

1

Greater security within SAP applications

- Protect against external threats: APTs, cloud administrators,
- Protect against internal threats: developers, privileged user access

2

Compliance with industry & government obligations

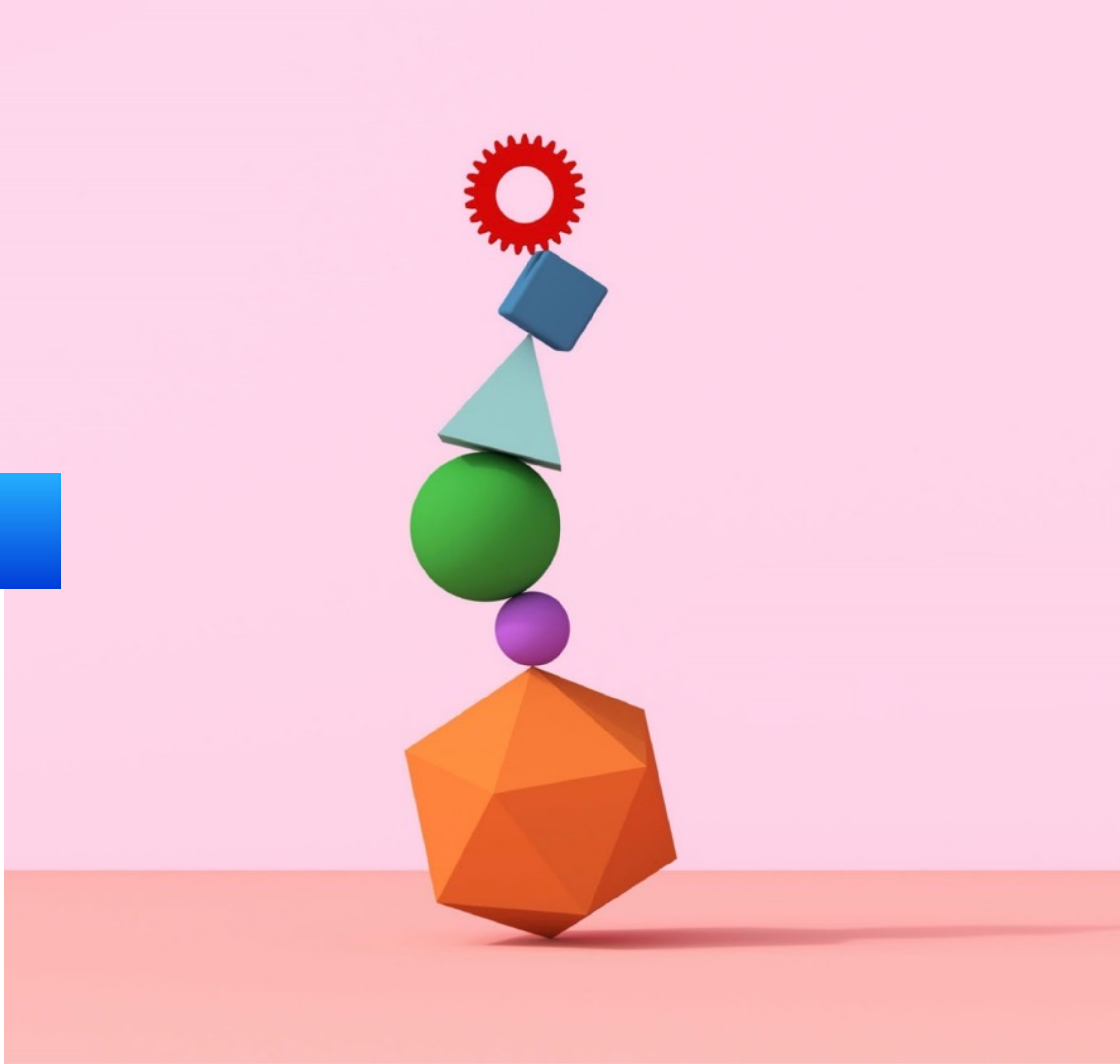
- Customer controlled key and token management for data sovereignty requirements

3

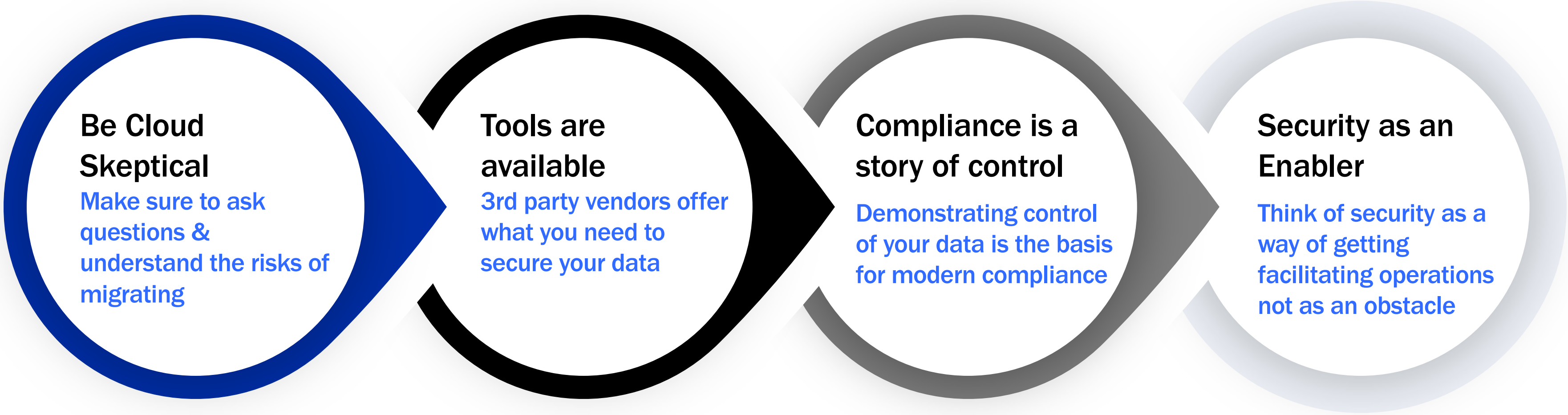
Safer Development

- Use tokenization for build accurate development environments without using real data

Wrap Up



Key Takeaways



Be Cloud Skeptical

Make sure to ask questions & understand the risks of migrating

Tools are available

3rd party vendors offer what you need to secure your data

Compliance is a story of control

Demonstrating control of your data is the basis for modern compliance

Security as an Enabler

Think of security as a way of getting facilitating operations not as an obstacle

Where to Find More Information

- SAPInsider Security Archives
  - https://sapinsider.org/topic/security/
- Thales CPL
  - https://cpl.thalesgroup.com/

SAPinsider

THANK YOU

Alex Hanway

Thales

Alexander.hanway@thalesgroup.com

SAPinsider

PO Box 982Hampstead, NH 03841