Building a future we can all trust

CipherTrust Secrets Management Powered by Akeyless Vault

Thales on Tour
2023/12/05

Thales Offers a Unified Approach to Data Security

DISCOVER

Discover data wherever it resides and classify it

PROTECT

Protect sensitive data with encryption or tokenization

CONTROL

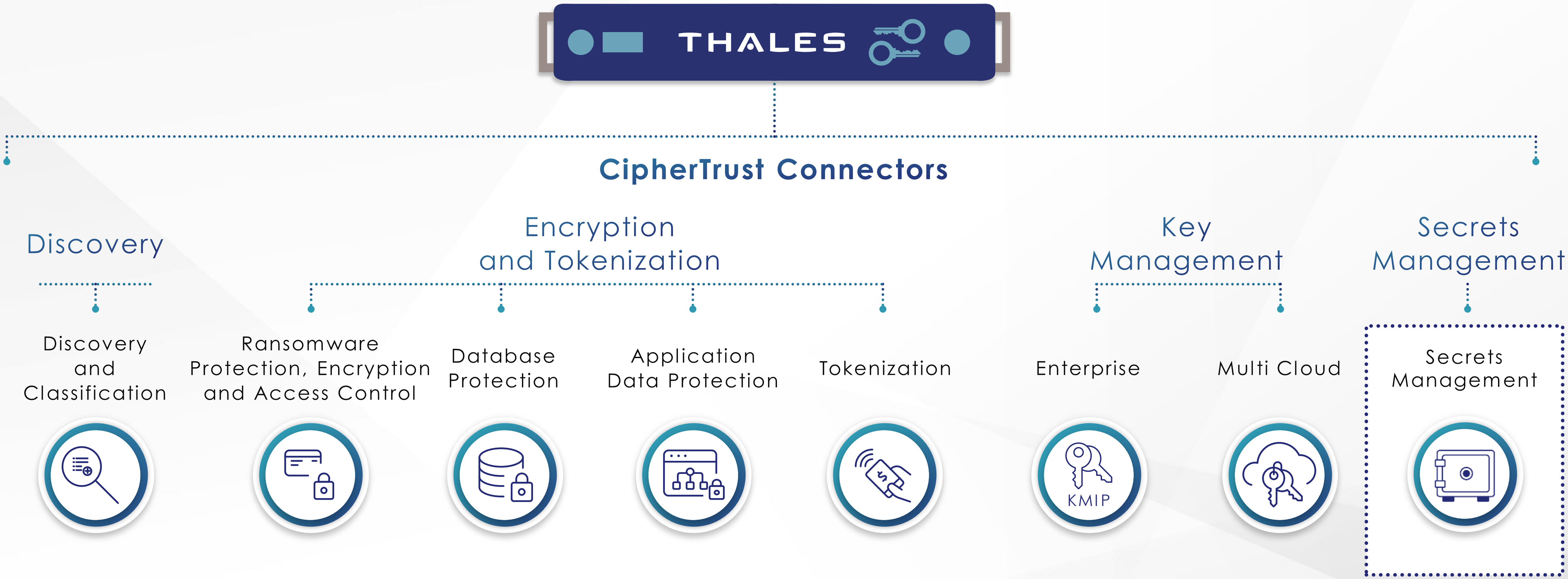
Control access to the data and centralize key management and policies

THALES

CipherTrust Data Security Platform

CipherTrust Manager

Key Management and Policies



CipherTrust Connectors

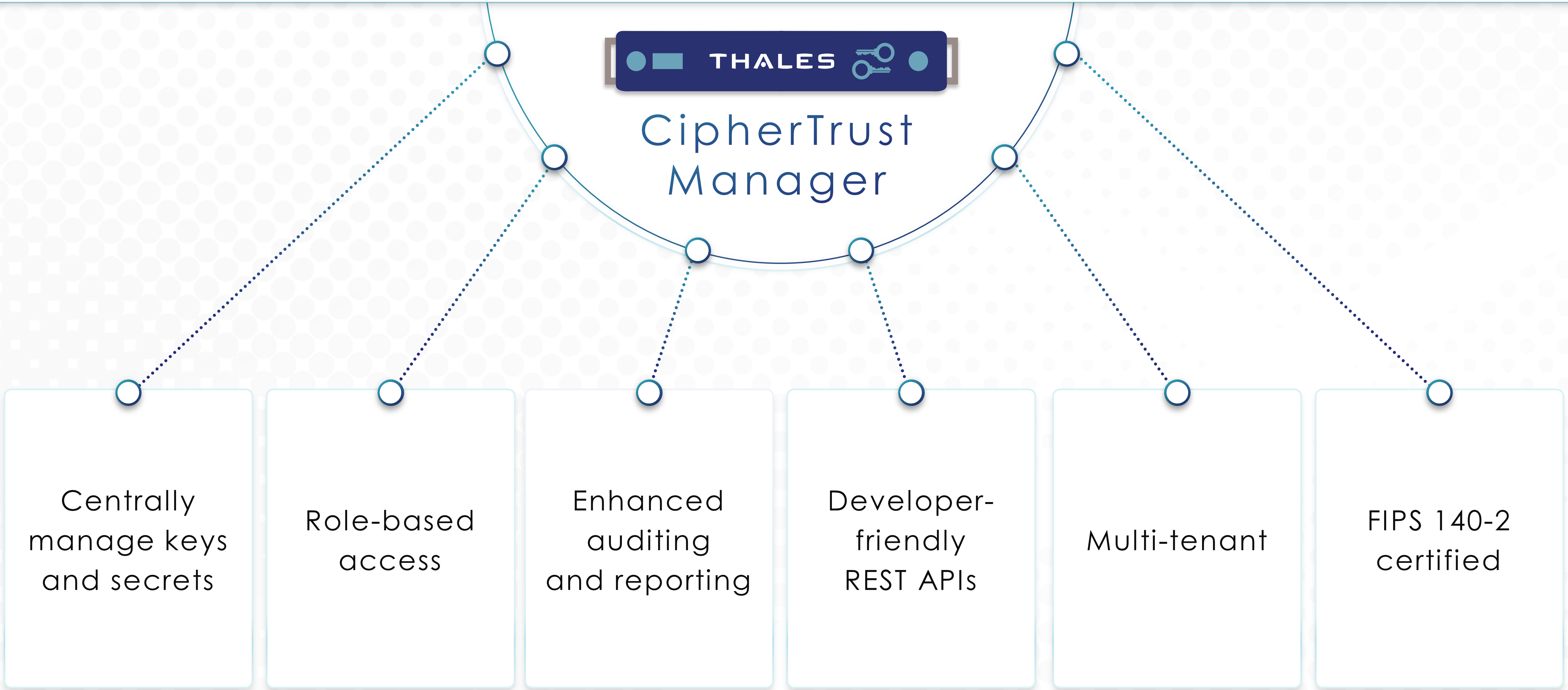
Discovery
- Discovery and Classification

Encryption and Tokenization
- Ransomware Protection, Encryption and Access Control
- Database Protection
- Application Data Protection
- Tokenization

Key Management
- Enterprise
- Multi Cloud

Secrets Management
- Secrets Management

CipherTrust Manager Centralizes Management Across the Connectors



CipherTrust Manager

Centrally manage keys and secrets

Role-based access

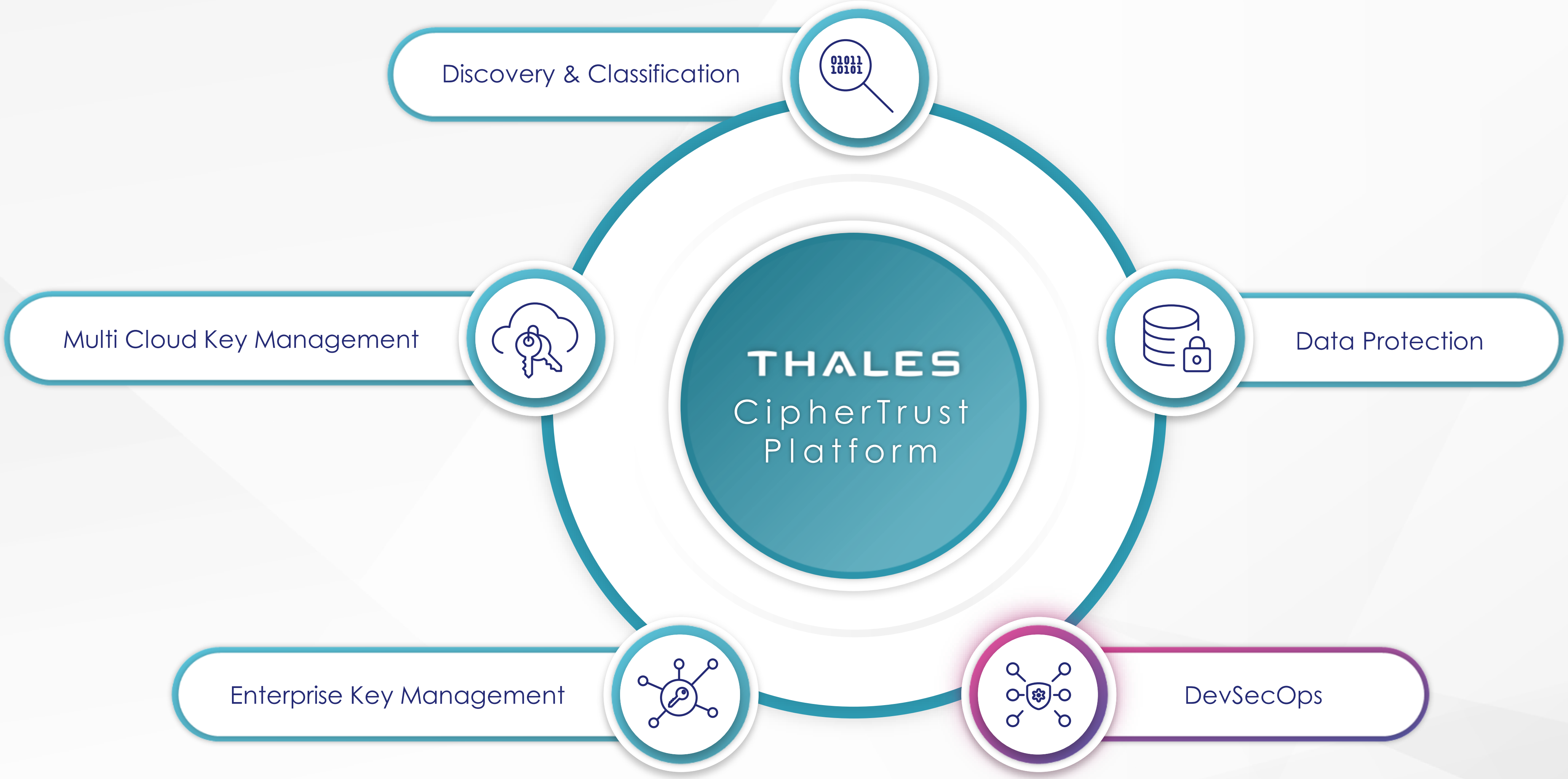
Enhanced auditing and reporting

Developer-friendly REST APIs

Multi-tenant

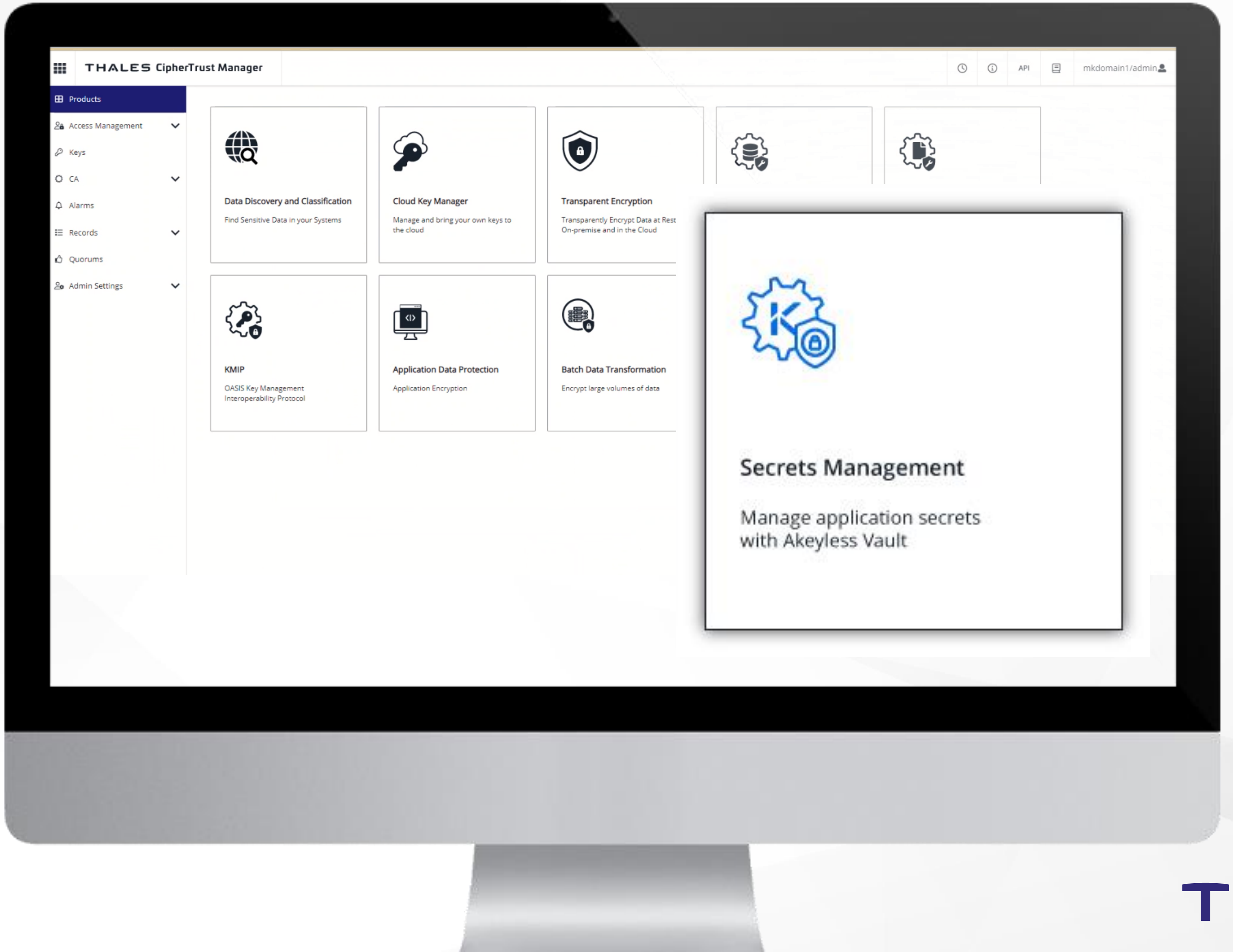
FIPS 140-2 certified

CipherTrust Data Security Platform use cases


THALES
CipherTrust Platform
Discovery & Classification
Multi Cloud Key Management
Data Protection
Enterprise Key Management
DevSecOps
01011
10101

THALES

Comprehensive Data Protection in One Tool



Data Discovery and Classification

Find Sensitive Data in your Systems

Cloud Key Manager

Manage and bring your own keys to the cloud

Transparent Encryption

Transparently Encrypt Data at Rest On-premise and in the Cloud

KMIP

OASIS Key Management Interoperability Protocol

Application Data Protection

Application Encryption

Batch Data Transformation

Encrypt large volumes of data

Secrets Management

Manage application secrets with Akeyless Vault

Secrets Management for DevSecOps: **Securing Secrets at Scale**

CipherTrust Secrets Management*

Automate access to

Secrets

Credentials

Certificates

API keys

Tokens

Centralized management for all secret types

Easy to use for DevSecOps

SaaS (Software as a Service) scalability for hybrid and multi-cloud environments

Automate processes for

Creating

Storing

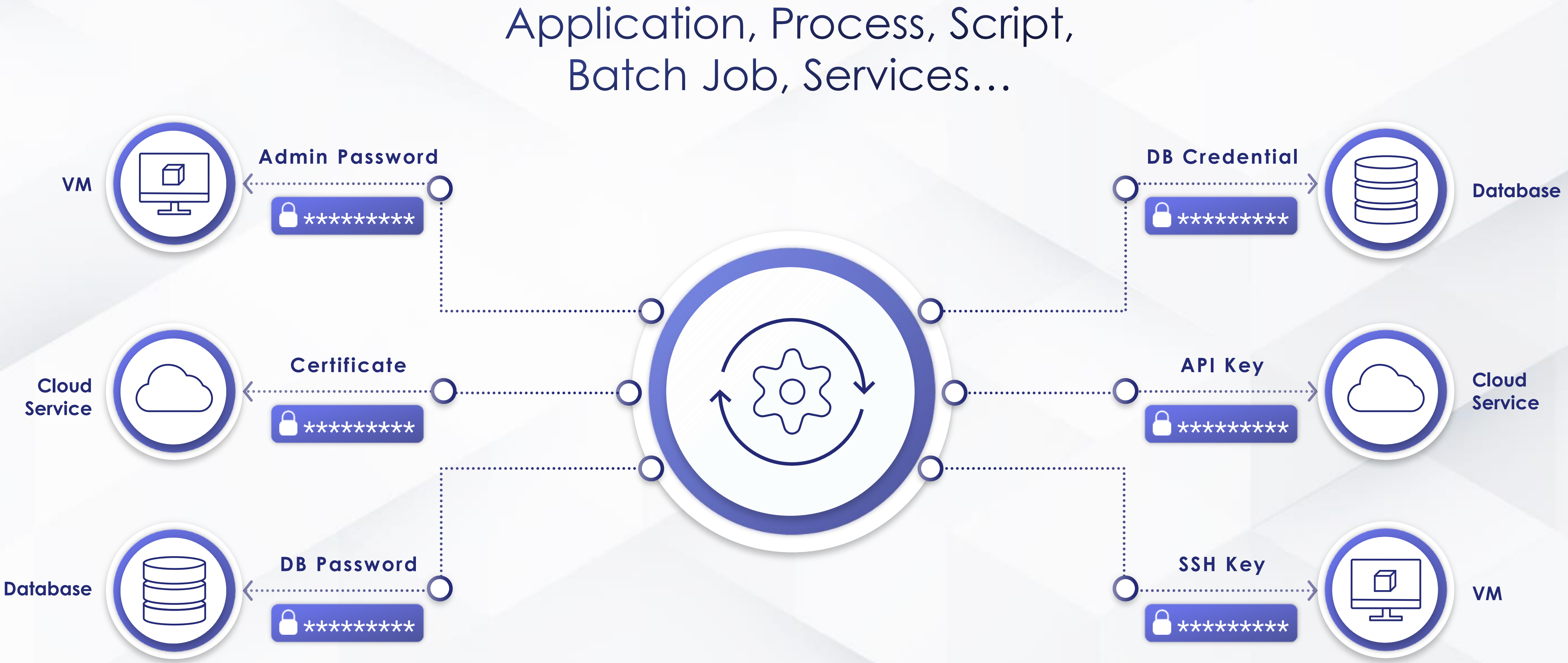
Rotating

Removing

*Powered by Akeyless Vault

PROTECT

Machine-to-Machine Connectivity Requires **Massive** Use of Secrets

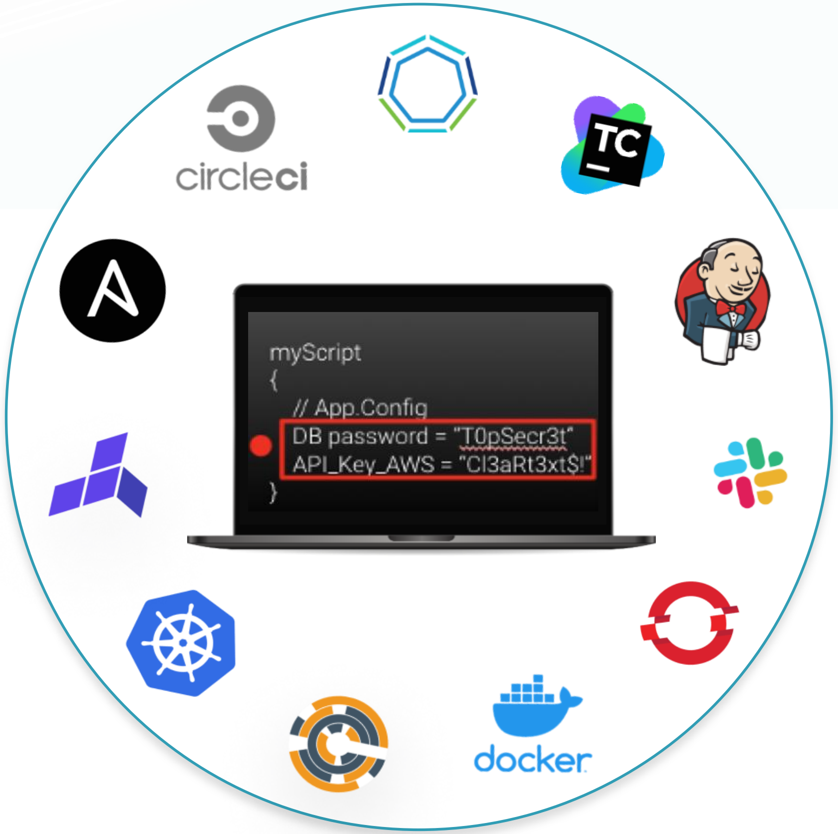


THALES

Major Risk and Hassle

Massive Sprawl of Secrets

Source Code, Scripts, CI/CD, DevOps, Production



```
mySript
{
  // App.Config
  DB password = "T0pSecr3t"
  API_Key_AWS = "Cl3aRt3xt$!"
}
```

74%

Operational Complexity - It's Chaos!
Don't know how many keys and certificates they have

Widespread Secrets Leaks
GitHub repositories have leaked keys.
Recent cases: Equifax, Mercedes, UN, LastPass

>100k

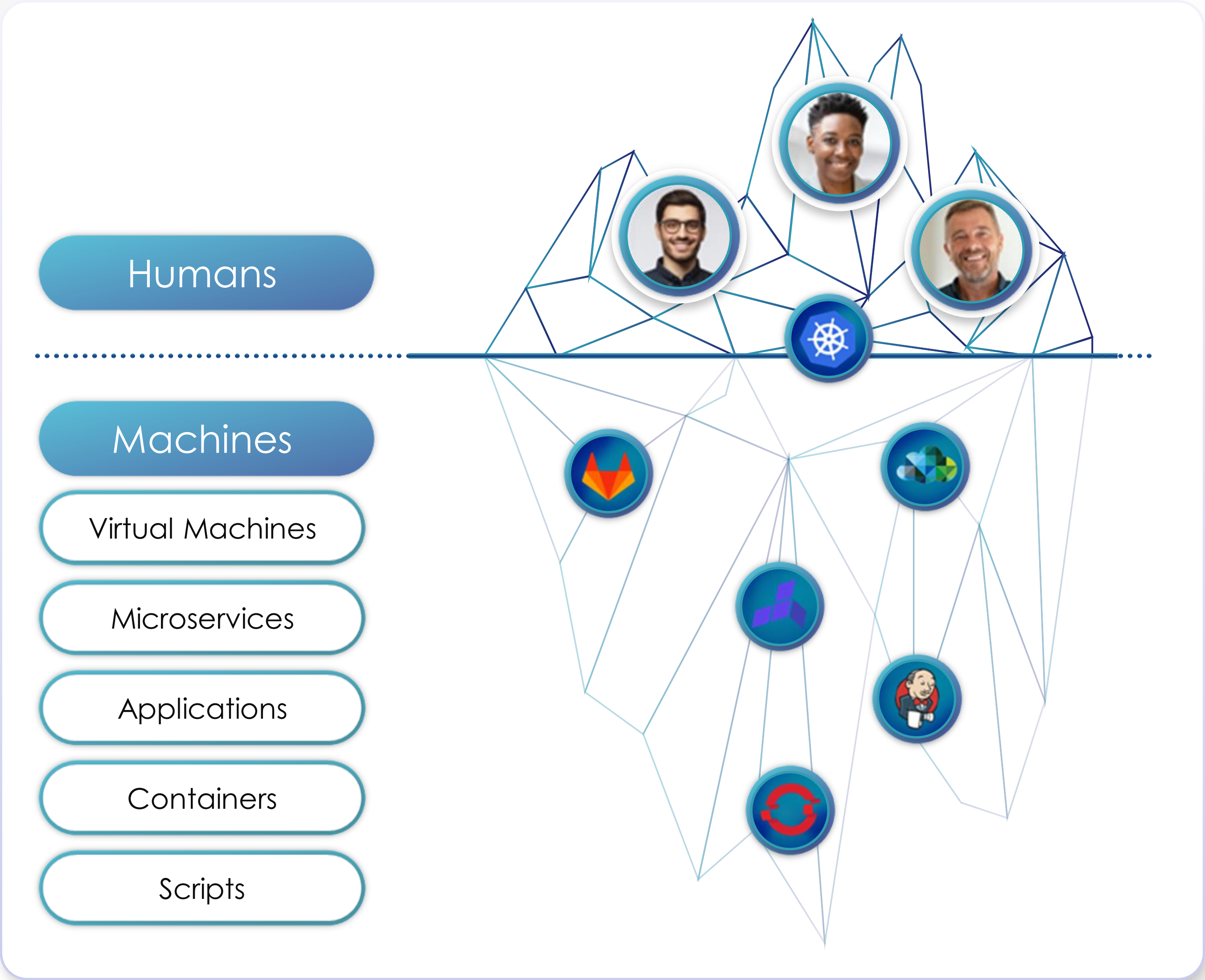
61%

Mission-Critical
of all breaches involve hacked credentials.

What are Secrets?

Types of Secrets

- Static secrets
- Dynamic secrets
- SHH Keys
- API Keys
- Tokens



Humans

Machines

- Virtual Machines
- Microservices
- Applications
- Containers
- Scripts

THALES

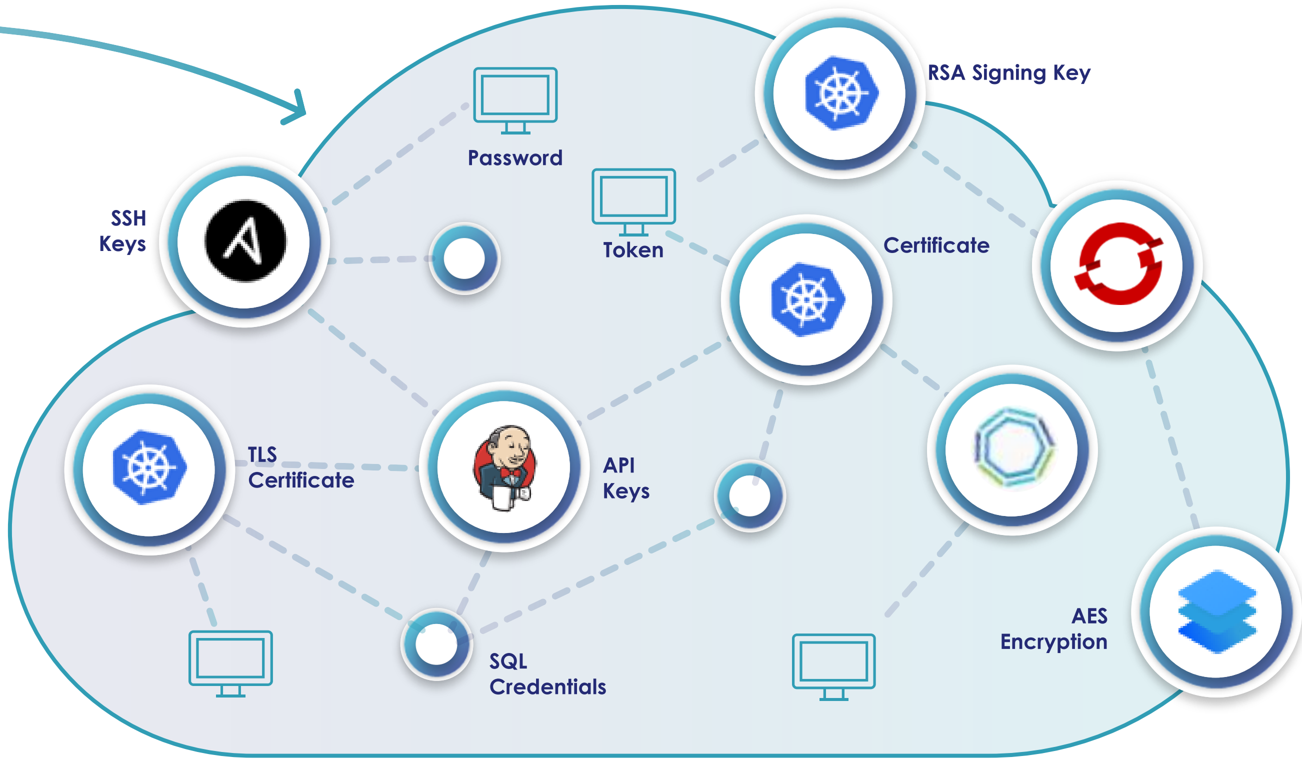
Cloud: Massive Increase in Use of Secrets

Zero-Trust Access
Identity validation is a MUST

DevOps & Automation
Less manual-initialed processes

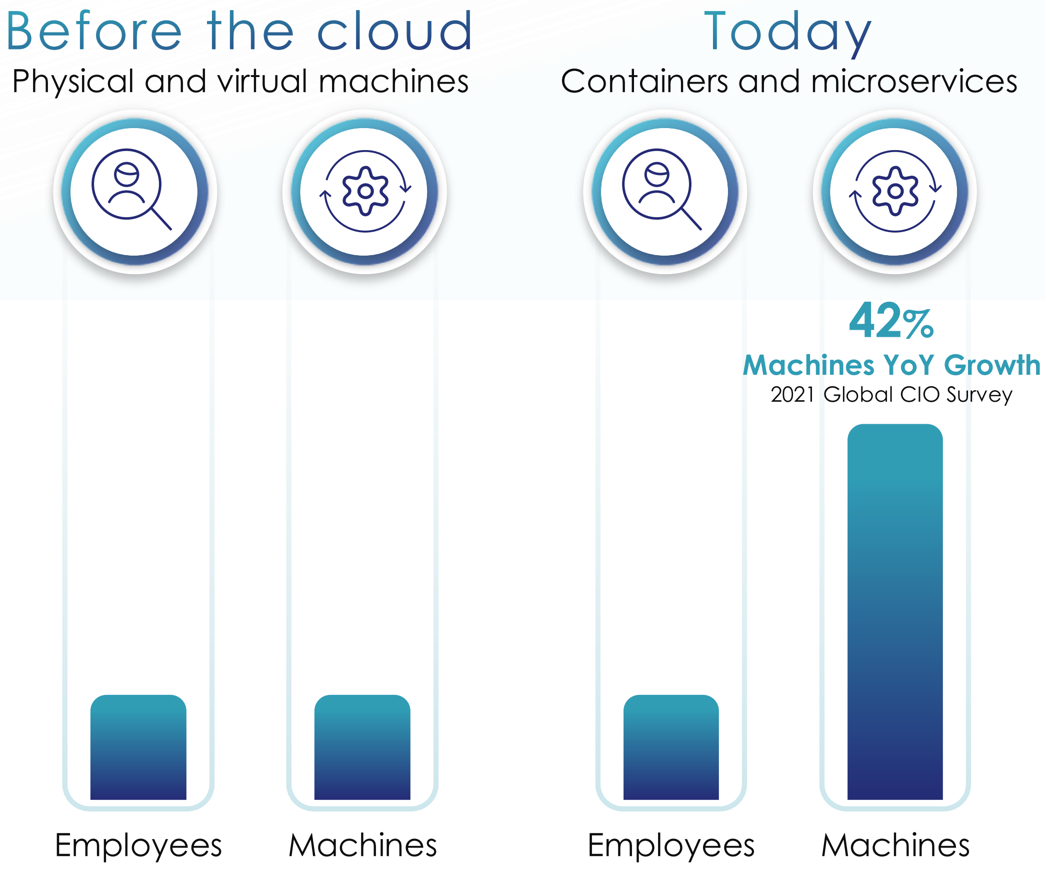
Containerization
Kubernetes, Docker, Microservices

Private, Hybrid, Multi Cloud
Multi-environments connectivity



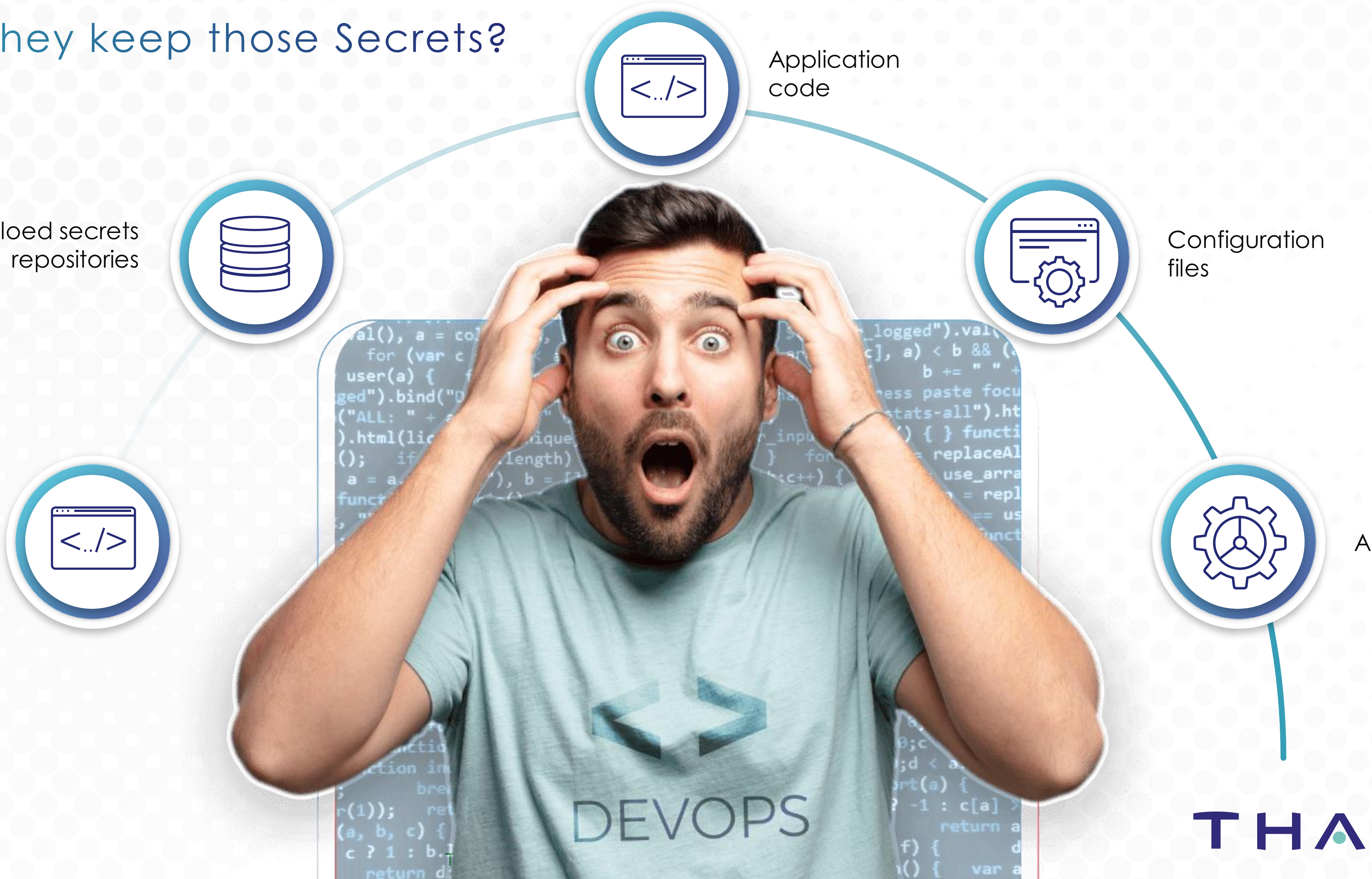
Customer Challenge: Secrets sprawl

> "62% of organizations do not know how many keys or certificates they have throughout their company."
>
> Keyfactor



DevOps Teams Facing the Overwhelming Phenomenon of Secrets Sprawl

Where do they keep those Secrets?



Application code

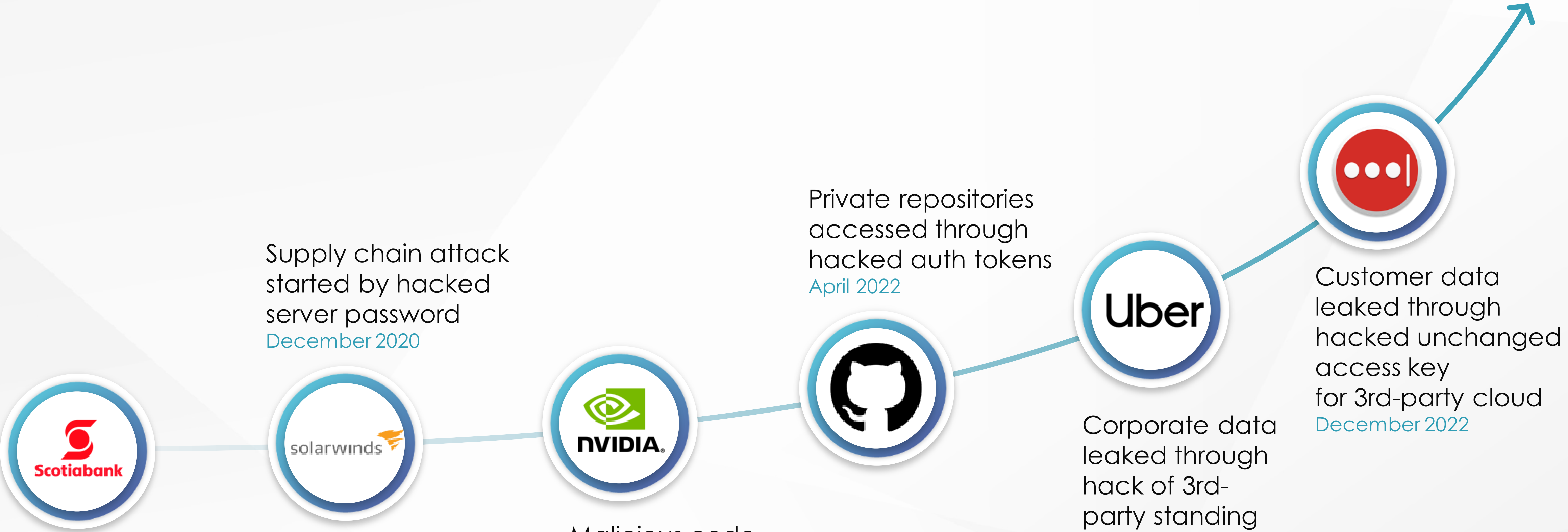
Siloed secrets repositories

Configuration files

Infrastructure scripts

Automation tools

Danger of the Status Quo: **Breaches from Leaked Credentials**



Customer accounts compromised by Credential leak
September 2019

Supply chain attack started by hacked server password
December 2020

Malicious code published following code-signing certificate leak
February 2022

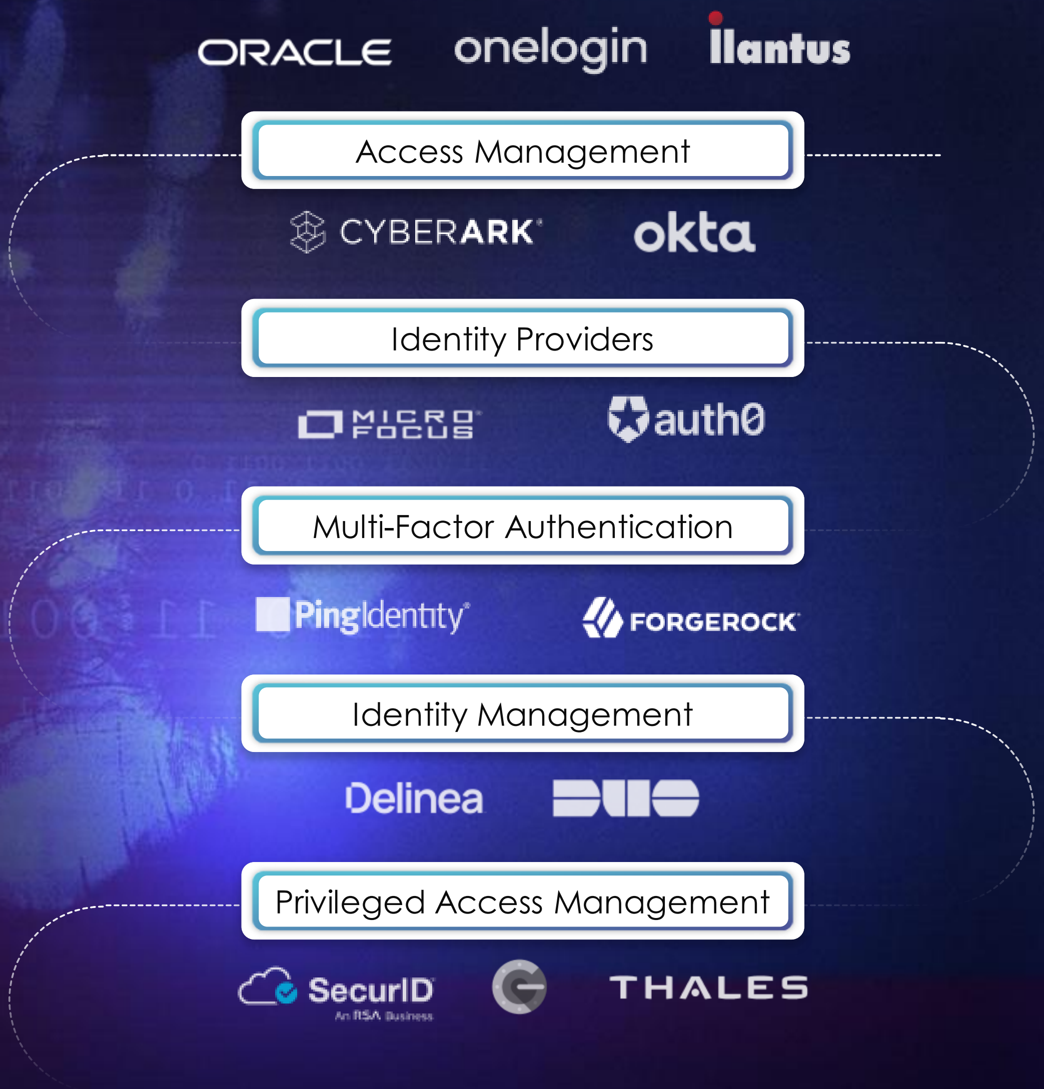
Private repositories accessed through hacked auth tokens
April 2022

Corporate data leaked through hack of 3rd-party standing privileges
December 2022

Customer data leaked through hacked unchanged access key
for 3rd-party cloud
December 2022

The Need to Invest in Secrets Management

We have invested so much to secure **human** identities and access



Access Management

Identity Providers

Multi-Factor Authentication

Identity Management

Privileged Access Management

Gartner’s View: Managed vs. Unmanaged Secrets

Unmanaged Secrets	Secrets Manager
Storing secrets in clear text	Vaulted and encrypted secrets
Not rotating secrets	Automated rotation
Not revoking secrets	TTL, lease time
Reusing secrets	Dynamic secrets
Unable to track secrets use	Full auditing
Rogue/unknown secrets	Ownership established

A Secure Vault for All Types of Secrets

Reduce the potential for human error and consistently enforce security policies across your organization

Enterprise-ready secrets management

Centralized management for all secret types

Easy to use, automated functionality for DevSecOps

Separation of duties to prevent breaches

Enterprise scalability for hybrid and multi cloud environments

Secrets store
Secure your credentials, certificates and keys

Credential rotation
Maintain compliance and security across you organization

Secrets sharing
Collaborate more securely and enable auditing with secure secrets sharing

Secure Kubernetes Secrets
Automate, encrypt, and manage all your Kubernetes secrets

Short-lived SSH Certificates
Simplify management of SSH keys

Just-in-time credentials
Eliminate standing privileges with temporary access

THALES

Customer Business Drivers

Mitigate risk

Reduce vulnerabilities

Accelerate time to compliance

Improve customer experience

Protect and control customer data without impacting the customer experience

Decrease cost

Improve operational efficiency

Consolidate on a data security platform versus using point solutions

THALES

Securing Secrets in Every Environment

Fits all environments:
Hybrid & Multi-cloud

Connectivity
to third party tools
and environments

Unified secrets management
across teams and technologies

Exclusive ownership
of secrets and secret access

THALES

Customer Outcomes

Centralized management for all Secret types

The management of secrets including automatic rotation SSH, AWS, Azure, Database, Custom, LDAP, Docker and Manual Rotation.

Log reporting UI and analytics.

FIPS 140-2 Level 3 Root of Trust with HSMs.

Lower TCO

No hidden costs such as infrastructure, time, resources and support.

SaaS model quickly scales across departments and regions.

Easy to use for DevOps

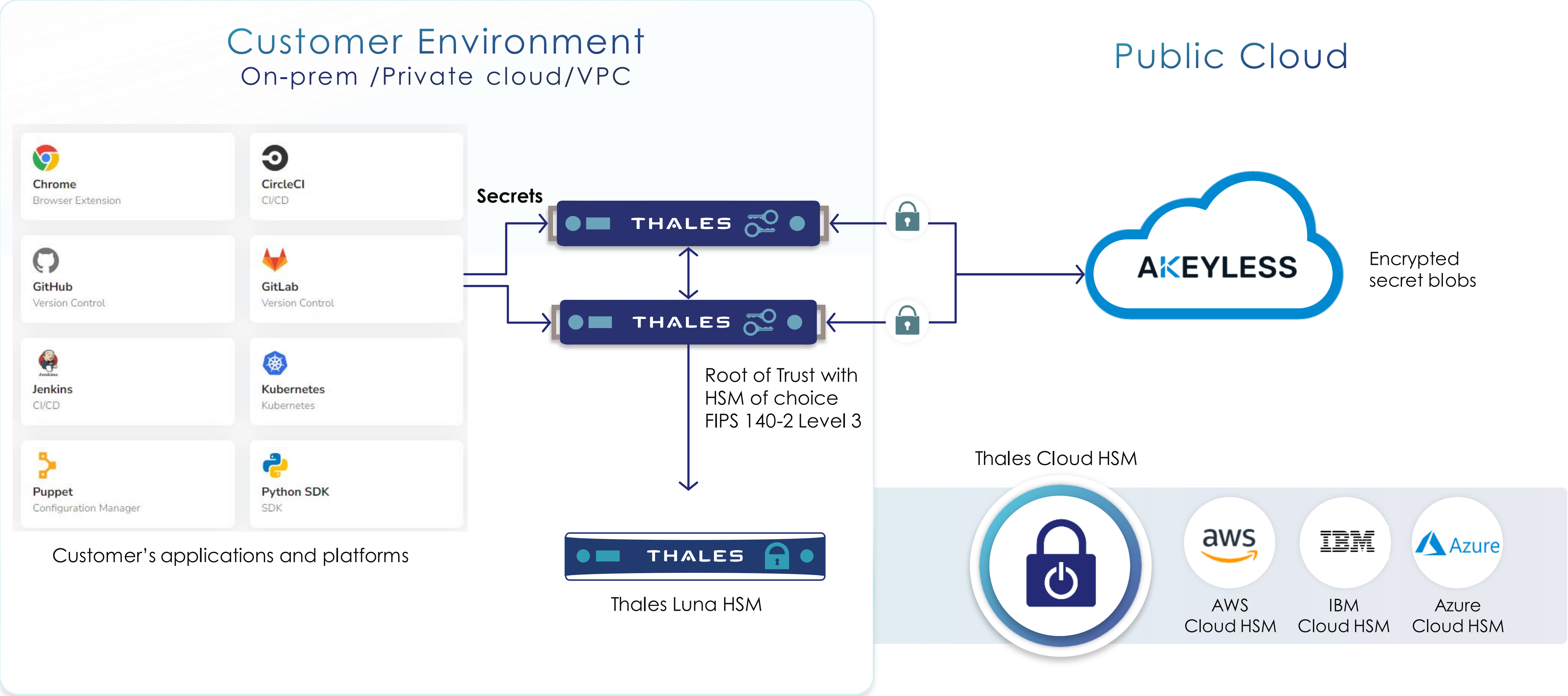
Quick deployment and shorter learning curve with built-in integrations to a host of DevOps tools.

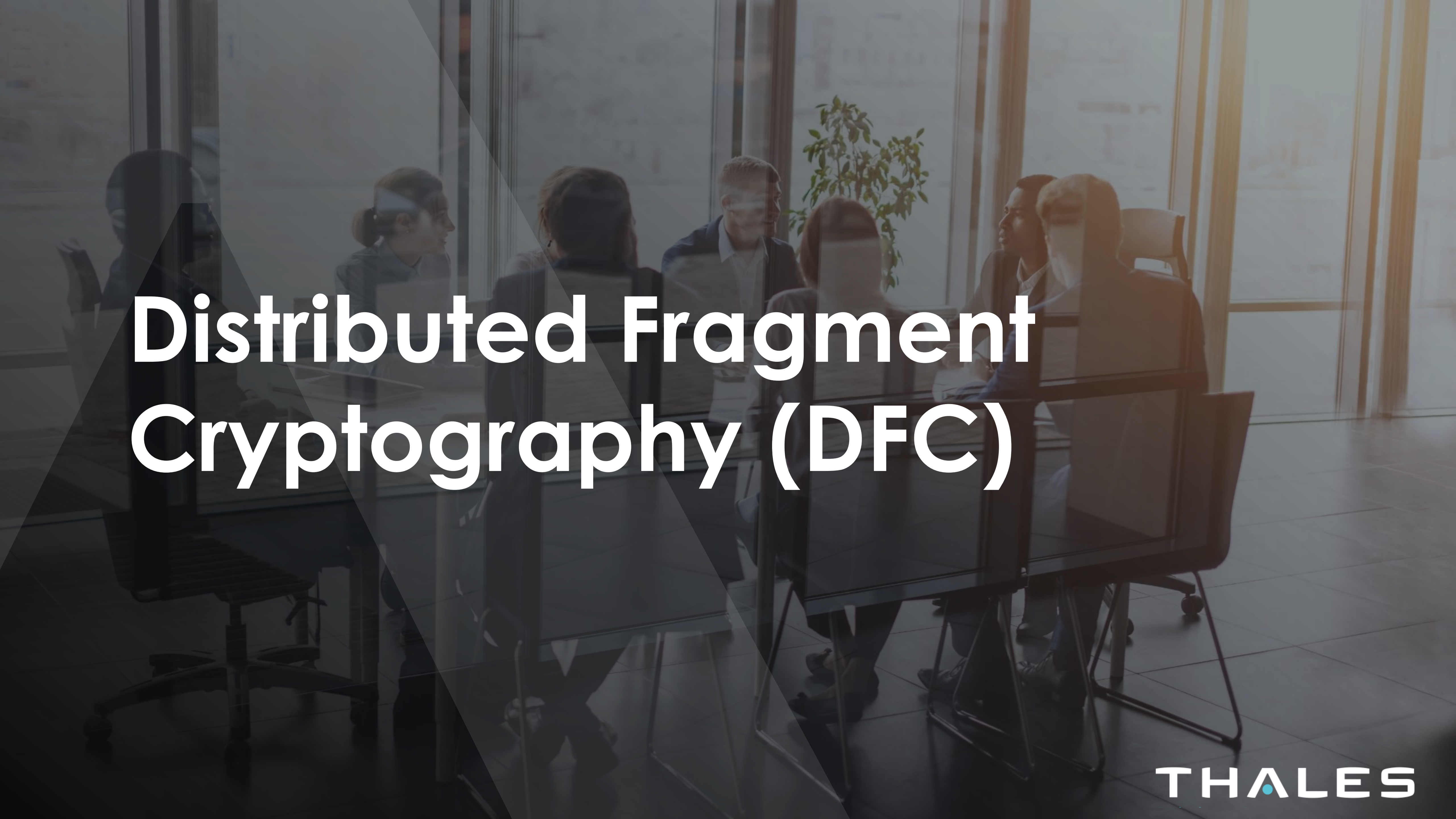
CipherTrust Manager provides **one straightforward UI** to manage all data protection features, providing for **higher efficiency** and compliance to **data protection mandates**, such as those relating to digital sovereignty.

THALES

Technology Overview

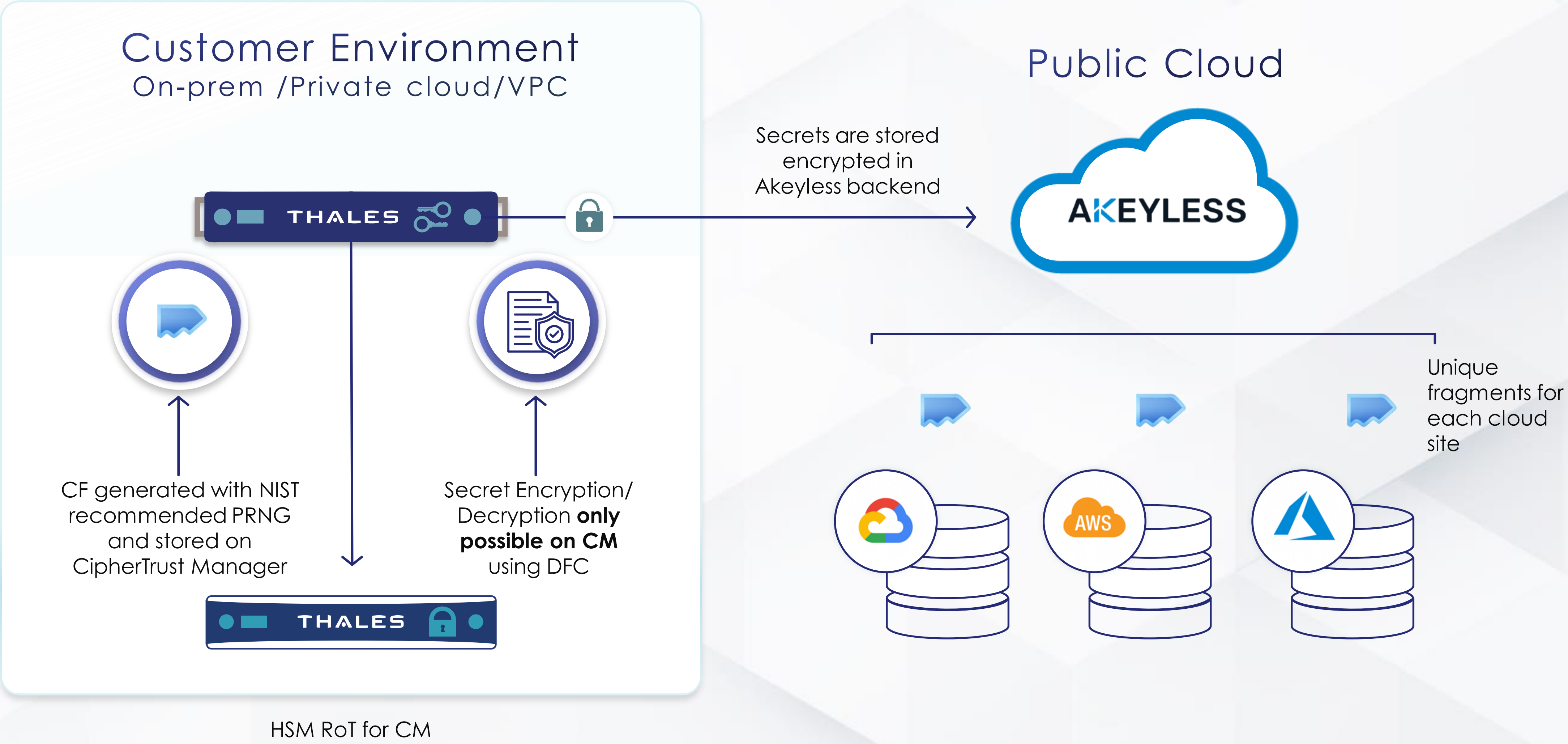
CipherTrust Secrets Management Deployment





Distributed Fragment Cryptography (DFC)

CipherTrust Secrets Management Deployment



Customer Environment
On-prem /Private cloud/VPC

CF generated with NIST recommended PRNG and stored on CipherTrust Manager

Secret Encryption/ Decryption **only possible on CM** using DFC

HSM RoT for CM

Public Cloud

Secrets are stored encrypted in Akeyless backend

Unique fragments for each cloud site

Buyer Personas

InfoSec Director/CISO

Their challenge:

- Manage security risk and compliance
- Adoption of security solutions across org
- Integrate into DevOps process -- keep everything working smoothly
- Keep costs low
- Support solutions with small team
- Support compliance and regular audits

Our winning arguments

- **SaaS solution: Lower cost in resources - frees up security team**
- **Fast deployment & low maintenance**
- **Scales easily**
- **High visibility for audits and centralized control across the organization**
- **Multi-tenancy reduces bottlenecks for business units and teams**
- Multi-cloud and on-prem
- Doesn't disrupt DevOps flow, working with standard DevOps tools: higher adoption
- Supports a wide range of necessary security functionality, with automated rotation and dynamic secrets

DevOps Engineers

Their challenge:

- Rising pressure to innovate & develop faster
- Not enough resources (people, time, infrastructure) to deliver on competing requests
- Managing competing expectations – speed versus stability versus security
- Unnecessary manual security requirements
- Need to manage secrets across a wide variety of tools

Our winning arguments

- **Doesn't slow DevOps down** - easily use your existing tools to inject secrets (Proof: our integrations page)
- **SaaS** for quick deployment and simple maintenance
- **SDKs and APIs** for streamlined integration
- **Automated functionality** for the development team, saving time:
  - Automated secret injection
  - Rotated secrets
  - Integration with the CI/CD pipeline
- **Self-service and multi-tenancy** for DevOps and other teams -- less need for Security resources, supports team independence

Thank you.