THALES
Building a future we can all trust

Egyszerű, hatékony titkosítás... Mítosz vagy valóság?

HIRSCH Gábor, Thales

Agenda

01

Ahonnan indultunk

02

Jelenlegi hazai helyzet

03

Thales megoldások a megfeleléshez

04

Titkosítás és kulcsmenedzsment egyszerűen

THALES

NIS2 Directive will drive focus on identity and digital trust

- **Announced: 27th of December, 2022.**
- **Deadline of adoption: 17th of October, 2024**
- **NIS2 expands the scope and coverage from the first NIS directive:**
  - New "essential sectors" covered such as energy, transport, banking, health, digital infrastructure, public administration and space sectors
  - The new rules will also protect so-called "important sectors" such as postal services, waste management, chemicals, food, manufacturing of medical devices, electronics, machinery, motor vehicles and digital providers. All medium-sized and large companies in selected sectors would fall under the legislation
  - In addition, it applies to all organizations in the designated sectors with 50 or more employees, increasing reach into the midmarket. Vendors and MSSPs with solutions for these organizations should be ready for this opportunity.
- **Chapter 4, Article 21 of the directive sets out 10 cybersecurity risk management areas as the minimum set of recommended measures for all organizations. Identity security controls play a significant part, from access control policies and advanced authentication to security of the supply chain. The requirements cover incident response, supply chain security, encryption and vulnerability disclosure, among other provisions (Paragraph 51 and 98 specifically mention encryption).**

Policies on risk analysis and information system security	Incident handling	Business continuity and crisis management	Supply chain security	Security in network and information systems acquisition, development, and maintenance
Policies and procedures to assess effectiveness of cybersecurity risk-management measures	Basic cyberhygiene practices and cybersecurity training	Policies and procedures regarding the use of cryptography and encryption	HR security, access control policies, and asset management	Multifactor authentication (MFA), continuous authentication, and secure communications

THALES

Compliance for

Network and Information Security Directive (NIS 2)

Thales helps organizations comply with NIS 2 by addressing requirements under article 21 for cybersecurity risk-management measures.

Requirements	NIS 2 Articles	Thales Supporting Capabilities
Article 21: Cybersecurity risk-management measures		
Risk Analysis	21.2.a	Data Discovery and Classification
Supply chain security	21.2.d	Cloud Key Management; Transparent Encryption
Cryptography and policies	21.2.h	Hardware Security Modules (HSMs); Tokenization; Enterprise Key Management; Transparent Encryption; High Speed Encryptors (HSE)
Access control and multi-factor authentication	21.2.i.j	SafeNet Trusted Access; Identity and Access Management; Transparent Encryption

How Thales Solutions Enable NIS 2 Compliance

NIS 2 Article	Thales Solution	
21.2, a: *"…**policies on risk analysis** and information system security;"*	 **CipherTrust Data Discovery and Classification**	Identifies structured and unstructured sensitive data on-premises and in the cloud. Built-in templates enable rapid identification of regulated data, highlight security risks, and help uncover compliance gaps.
21. 2, d: ***supply chain security****, … concerning the relationships between each entity and its;* ***direct suppliers or service providers***	 **CipherTrust Cloud Key Management**	Reduces third party risks by maintaining on-premises under the full control of the financial institution the keys that protect sensitive data hosted by third party cloud providers.
	 **CipherTrust Transparent Encryption**	Provides complete separation of roles where only authorized users and processes can view encrypted data. This keeps third party cloud provider employees, such as support engineers and DB admins from seeing the data in the clear.
21. 2, h*: "…**policies and procedures** regarding the **use of cryptography and**, where appropriate, **encryption**"*	 **CipherTrust Transparent Encryption**	Delivers data-at-rest encryption for files and folders and privileged user access control with granular policies. Protects data wherever it resides, on-premises, across clouds, and in big data and container environments.
	 **CipherTrust Tokenization**	Permits the pseudonymization of sensitive information in databases while maintaining the ability to analyze aggregate data, without exposing sensitive data during the analysis or in reports.
	 **CipherTrust Enterprise Key Management**	Streamlines and strengthens key management in cloud and on-premises environments for home-grown encryption, as well as third-party applications.
	 **High Speed Encryptor (HSE)**	Provides network-independent, data-in-motion encryption ensuring data, video, voice, and metadata is secure as it moves from site-to-site, or from on-premises to the cloud and back.
	 **Luna HSMs**	Protect cryptographic keys and provide a FIPS 140-2 Level 3 hardened, tamper-resistant environment for secure cryptographic processing, key generation and protection, encryption, and more.

THALES

How Thales Solutions Enable NIS 2 Compliance

NIS 2 Article	Thales Solution		
21. 2, i: *"…**access control policies** and asset management;* ***21. 2, j:*** *the use of **multi-factor authentication or continuous authentication solutions…"*		**OneWelcome Identity & Access Management**	Limits the access of internal and external users based on their roles and context with granular access and authorization policies that help ensure that the right user is granted access to the right resource at the right time.
		**SafeNet Trusted Access**	Enables Multi-factor Authentication with the broadest range of hardware and software methods and form factors, allowing customers to address numerous use cases, assurance levels, and threat vectors with unified policies.
		**CipherTrust Transparent Encryption**	Provides complete separation of roles where only authorized users and processes can view encrypted data through granular access security policies and key management.

Hazai szabályozás

2023. évi XXIII. Törvény (Kibertan tv)

a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről

MK rendelete (tervezet)

a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről

JÖN...

Új Ibtv. 2024 március????

Pénzintézeti Vhr???

Védelmi intézkedések katalógusa 2. fejezet

Ezen kívül még számtalan helyen....

Identity Apps for B2C, B2B & Gig Worker Use Cases

Business identity apps on top of a solid OneWelcome core or augmenting 3rd party IAM

Integrations with 3rd party apps and services:

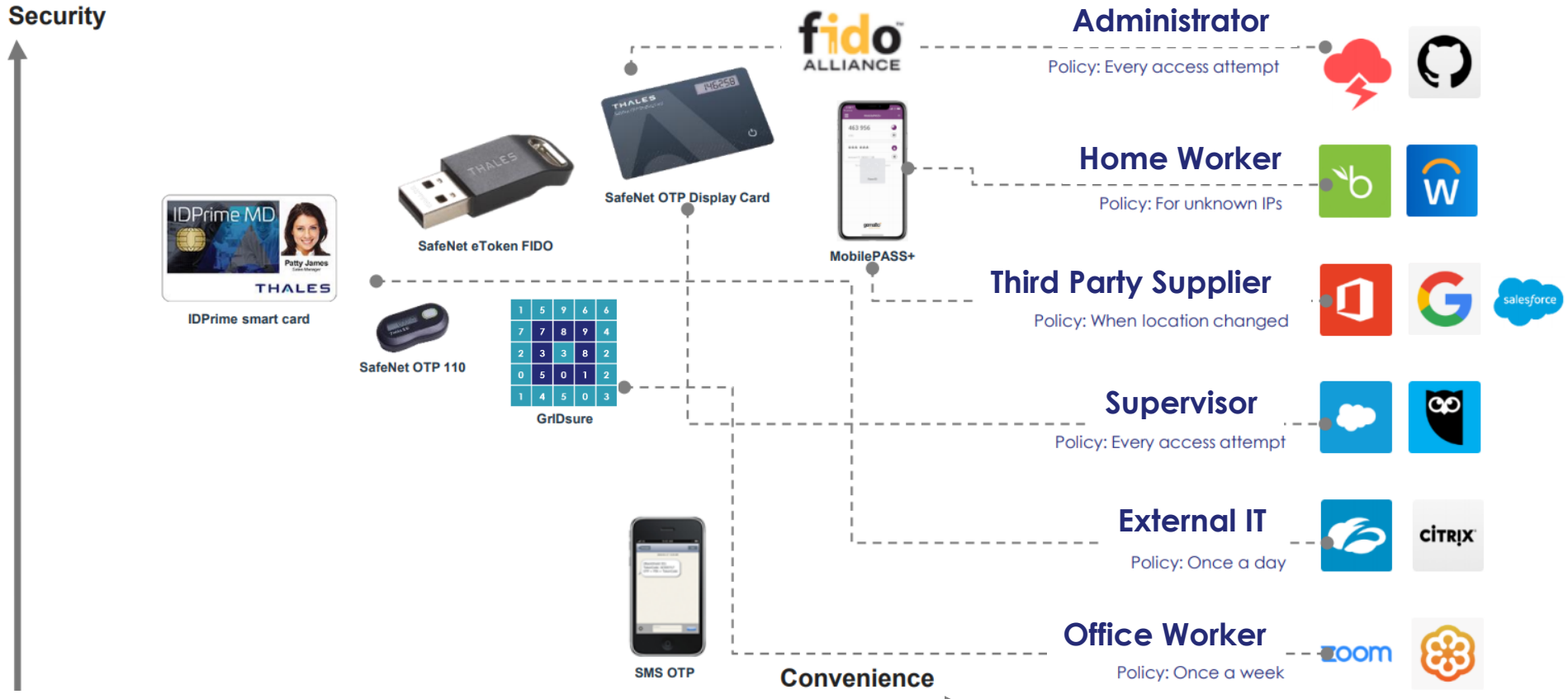
- ID verification, Digital Wallets and certified attribute providers
- EU eID's
- APIs for export and synchronization to identity stores, martech & BI
- Fraud detection & prevention
- Digital Signing

THALES

Védelmi intézkedések katalógusa 8. fejezet

		felhasználók által végzett tevékenységeket.			
4.	8.3. Azonosítás és hitelesítés (felhasználók) – Privilegizált fiókok többtényezős hitelesítése	8.3. A szervezet többtényezős hitelesítést alkalmaz a privilegizált fiókokhoz való hozzáféréshez.	X	X	X
5.	8.4. Azonosítás és hitelesítés (felhasználók) – Nem-privilegizált fiókok többtényezős hitelesítése	8.4. A szervezet többtényezős hitelesítést alkalmaz a nem privilegizált fiókokhoz való hozzáféréshez.	-	X	X
6.	8.5. Azonosítás és hitelesítés	8.5. Amikor a szervezet közös használatú fiókokat vagy	-	-	X

Different authentication paths



Továbbított adatok titkosítása

Védelmi intézkedések katalógusa 17. fejezet

	Különálló analízisek a funkciók elkülönítéséhez	analízisekat alakít ki a szervezet működése szempontjából kritikus rendszerelemek és funkciók elkülönítése érdekében.			
41.	17.40. Az adatátvitel bizalmassága és sértetlensége	17.40. Az EIR megvédi a továbbított információk bizalmasságát és sértetlenségét.	-	X	X
42.	17.41. Az adatátvitel bizalmassága és sértetlensége – Kriptográfiai védelem	17.41. Az EIR kriptográfiai mechanizmusokat alkalmaz az adatátvitel során, hogy megelőzze az információk jogosulatlan felfedését, illetve kimutassa az információk módosításait.	-	X	X
43.	17.42. Az adatátvitel bizalmassága és sértetlensége – Az adatok	17.42. Az EIR fenntartja az információ bizalmasságát és sértetlenségét a továbbítás előkészítése és a fogadás során.	-	-	-

Védelmi intézkedések katalógusa 2. fejezet

		kapcsolatok lehetővé tételét megelőzően			
102.	2.101. Távoli hozzáférés – Felügyelet és irányítás	2.101. A szervezet automatizált mechanizmusokat alkalmaz a távoli hozzáférési módok felügyeletére és ellenőrzésére.	-	X	X
103.	2.102. Távoli hozzáférés – Bizalmasság és sértetlenség védelme titkosítás által	2.102. A szervezet kriptográfiai mechanizmusokat alkalmaz a távoli hozzáférés biztonságának és sértetlenségének biztosítása érdekében.	-	X	X
104.	2.103. Távoli hozzáférés – Menedzselt hozzáférés-felügyeleti pontok	2.103. A szervezet a távoli hozzáféréseket engedélyezett és menedzselt hálózati hozzáférés-felügyeleti pontokon keresztül irányítja.	-	X	X
105.	2.104. Távoli hozzáférés –	2.104. A szervezet:	-	X	X

Thales High Speed Encryption (HSE)

Trusted Security

Globally certified and quantum safe

Maximum Performance

Improved bandwidth and latency efficiency over IPsec

Optimal Flexibility

Vendor agnostic / bump in the wire

Drops seamlessly into

Layer 2, 3, and 4 infrastructure

THALES

Tárolt adatok titkosítása

Védelmi intézkedések katalógusa 17. fejezet

	alkalmazások	EIK-ek köze sorolja.			
82.	17.81. Tárolt (at rest) adatok védelme	17.81. A szervezet megóvja a meghatározott tárolt, illetve archivált (at rest) adatok bizalmasságát és sértetlenségét a feldolgozás vagy továbbítás alatt álló adatokkal megegyező szinten.	-	X	X
83.	17.82. Tárolt (at rest) adatok védelme – Kriptográfiai védelem	17.82. A szervezet meghatározott rendszerelemek vagy adathordozók esetében kriptográfiai mechanizmusokat alkalmaz a szervezet által meghatározott tárolt vagy archivált adatok jogosulatlan felfedésének és módosításának megelőzésére.	-	X	X

Védelmi intézkedések katalógusa 16. fejezet

	Összhangban lévő érdekek	szolgáltatók érdekei sértik-e szervezeti érdeket.			
55.	16.54. Külső információs rendszerek szolgáltatásai – Feldolgozás, tárolás és szolgáltatási helyszín	16.54. A szervezet a meghatározott helyszínekre korlátozza az információ feldolgozásának helyét, valamint az információk vagy adatok elhelyezését, a szervezet által meghatározott követelmények és feltételek alapján.	-	-	-
56.	16.55. Külső információs rendszerek szolgáltatásai – Felügyelt kriptográfiai kulcsok	16.55. A szervezet kizárólagos ellenőrzést gyakorol a külső rendszerekben tárolt, vagy külső rendszerekbe továbbított titkos adatokhoz tartozó kriptográfiai kulcsok felett.	-	-	-
57.	16.56. Külső információs rendszerek szolgáltatásai – Sértetlenség felügyelete	16.56. A EIR képes arra, hogy ellenőrizze a külső rendszerben található információ sértetlenségét.		-	-
58.	16.57. Külső információs rendszerek szolgáltatásai – Feldolgozási és tárolási helyszín – Magyarország joghatósága	16.57. A szervezet az információfeldolgozást és az adattárolást olyan helyszínekre korlátozza, amelyek Magyarország határain belül találhatók.	-	-	-

Belifs of encryption and key management

Costly

Complex

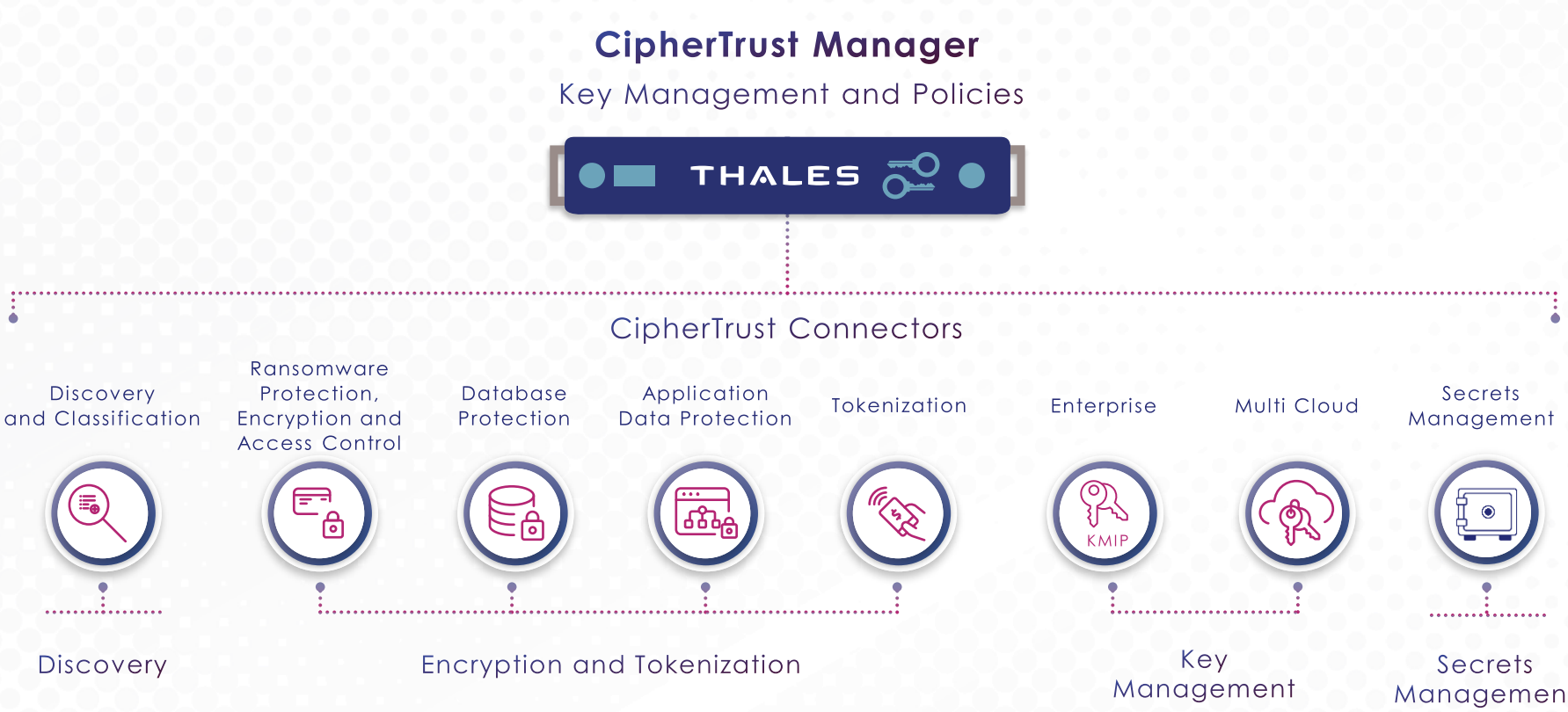
Time-consuming

Complicated deployment and usage

Key recovery

...

CipherTrust Data Security Platform



THALES

Discover and classify your sensitive data

#1 barrier to a successful encryption strategy is the ability to discover where sensitive data resides in the organization

Find any type of sensitive data, anywhere — #1

Risk analysis and reporting — # 2

Proactive protection — #3

CipherTrust Data Discovery and Classification

THALES

Data protection at the file system layer

Secure sensitive data wherever it resides to meet compliance requirements with minimal disruption, effort and cost

Transparent Encryption

Encrypt data and define privileged user access controls without changes to infrastructure, applications or workflow

Live Data Transformation

Zero-downtime deployment and seamless key rotation

Advanced data protection solution integrations

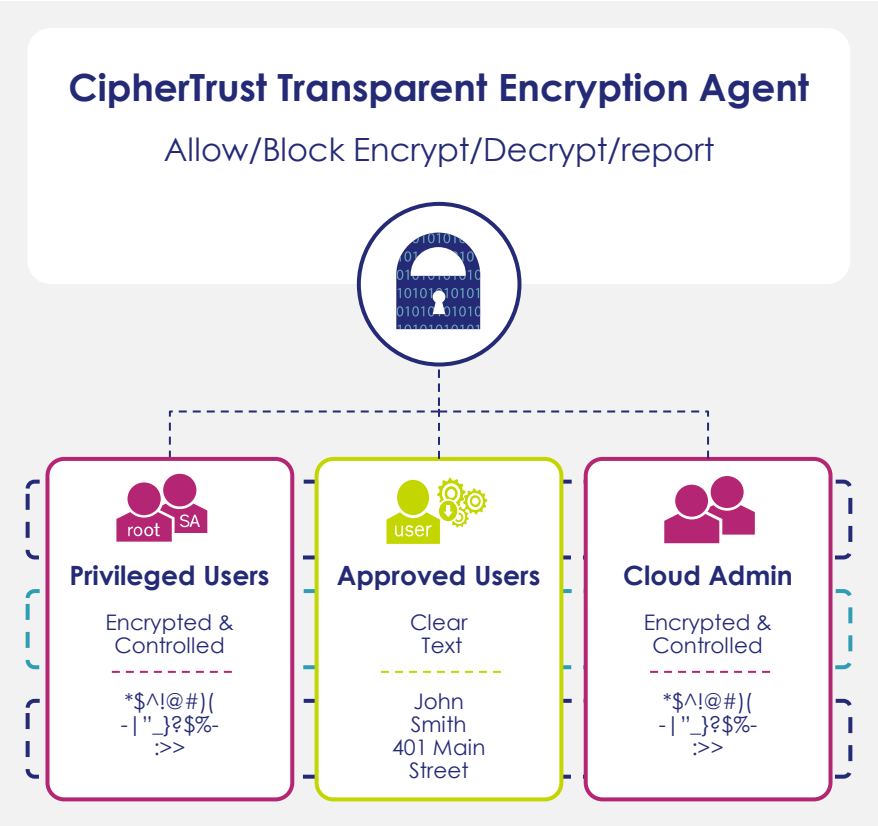
Windows, aws, hadoop, Red Hat Enterprise Linux, SUSE, teradata., ORACLE, Ubuntu, UNIX, Microsoft SQL Server, SAP HANA

...and more

THALES

CipherTrust Transparent Encryption (CTE)

Transparently protects file system, volume data-at-rest



Transparent, file-level encryption

For all databases and file types

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

THALES

Centralize key management across your enterprise

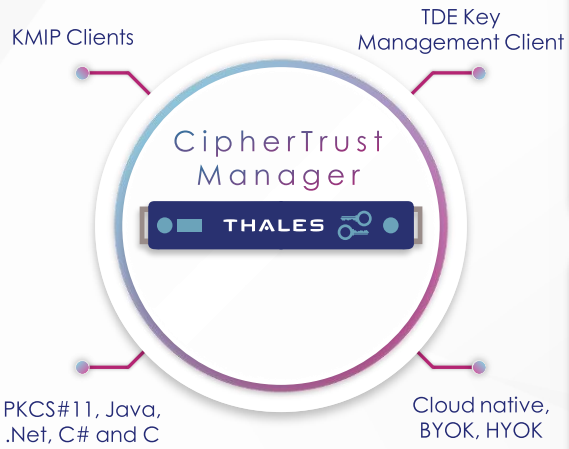
Extensive partner integrations with leading enterprise storage, server, database, cloud and SaaS vendors

Data storage vendors, big data

PURESTORAGE, NUTANIX, vmware READY vSAN, mongoDB., Hewlett Packard Enterprise, IBM, DELL EMC, NetApp

Home-grown apps, web servers

Microsoft, HashiCorp, NGINX, APACHE SOFTWARE FOUNDATION, ORACLE



Database (TDE) Key Management

ORACLE EXADATA, Microsoft SQL Server, ORACLE

Cloud Key Management

Azure, Microsoft 365, Google Cloud, Google Workspace, aws, ORACLE, SAP, salesforce

THALES

providing a broad range capabilities to **protect what matters most**

THALES

THALES

“Hope is not a strategy”

THALES
Building a future we can all trust

Questions?

www.thalesgroup.com

THALES

Köszönöm a figyelmet!

HIRSCH Gábor
+36305263024
gabor.hirsch@thalesgroup.com