Mega Trends Impacting Cyber Resilience

jukka.nokso-koivisto@thalesgroup.com
Tel +358 440 110 110

www.thalesgroup.com

Mega Trends Impacting Cyber Resilience & Compliance

AI

Supply Chain Security

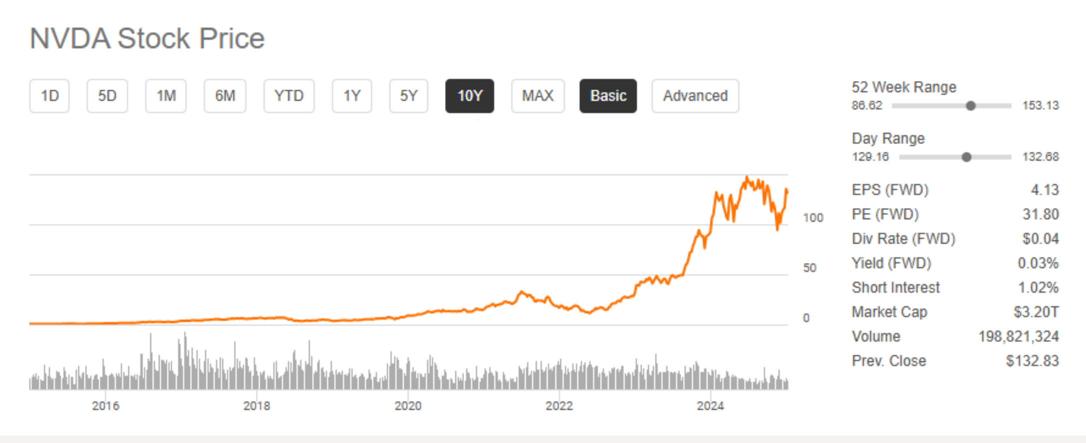
DevSecOps

Sovereignty

Regulation

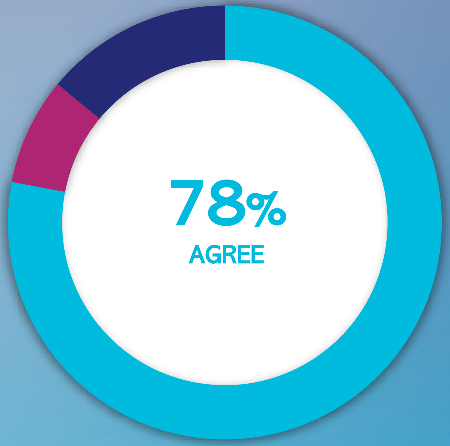
MegaTrend #1 Artificial Intelligence

AI related investments growing rapidly


NVDA Stock Price

52 Week Range	86.62 – 153.13
Day Range	129.16 – 132.68
EPS (FWD)	4.13
PE (FWD)	31.80
Div Rate (FWD)	$0.04
Yield (FWD)	0.03%
Short Interest	1.02%
Market Cap	$3.20T
Volume	198,821,324
Prev. Close	$132.83

AI believed to give significant competitive advantage in corporations



Scaling AI/ML use cases to AI in order to create business value is a top priority

More data = more risk

AI, ML, DNN, GenAI… What are we Talking About?

Artificial Intelligence

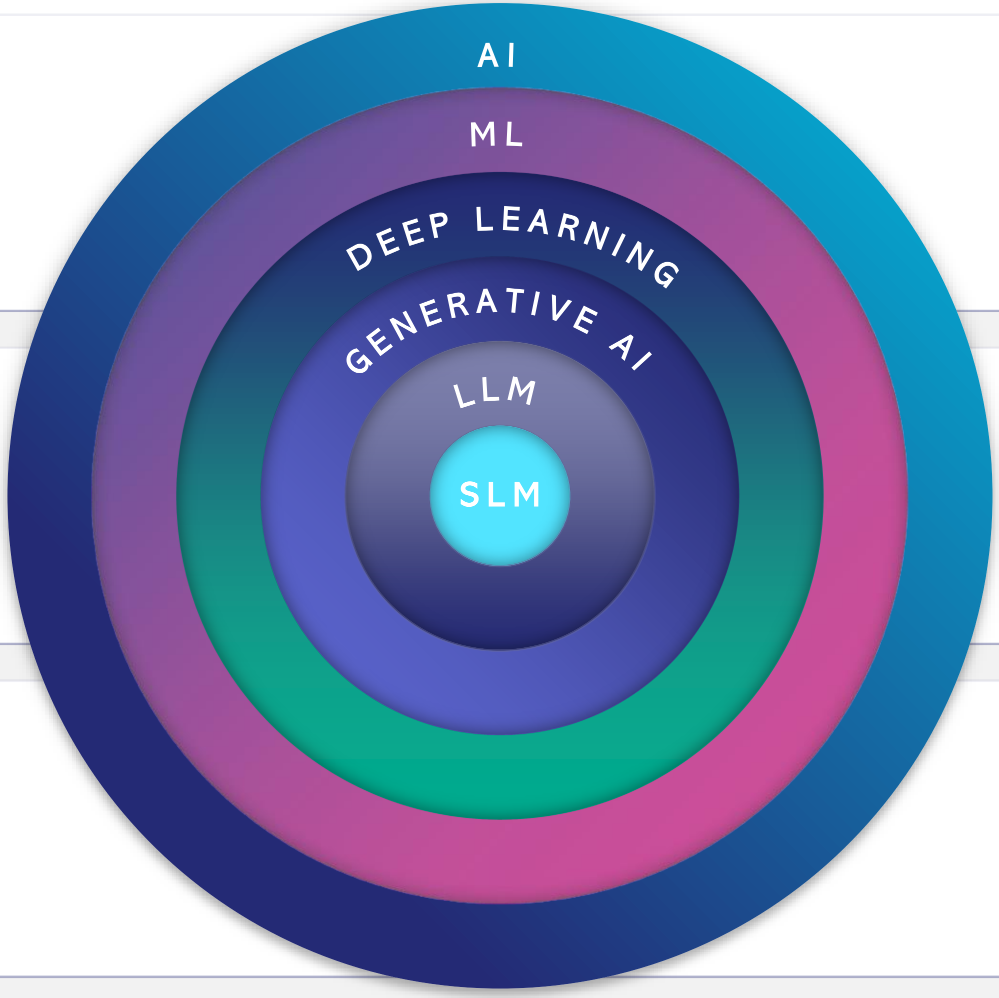
Any techniques that enable computers to mimic human intelligence

Machine Learning

A branch of AI that focus on the creation of intelligent machines that learn from data.

Deep Learning

Is a subset of Machine Learning methods, based on Artificial Neural Networks.



Generative AI

A type of artificial neural network that generate data that is similar to the data it was trained on.

Large Language Models

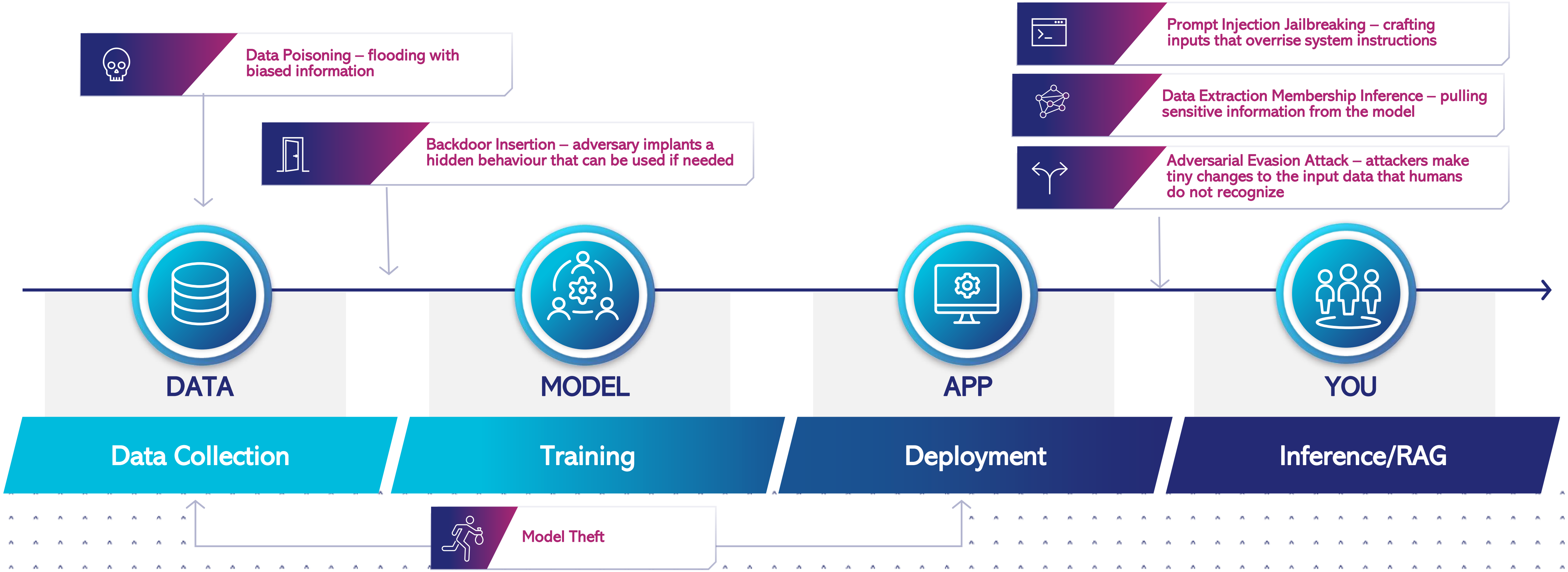
Specific application of GenAI. It revolutionized many Natural Language Processing Tasks

Small Language Models

THALES
Building a future we can all trust

Vulnerabilities in the Artificial Intelligence Lifecycle

Attacks on AI can happen at any stage of the AI Lifecycle, from the poisoning or extraction of data the data used by the model, to the theft of a whole model.



Data Poisoning – flooding with biased information

Backdoor Insertion – adversary implants a hidden behaviour that can be used if needed

Prompt Injection Jailbreaking – crafting inputs that overrise system instructions

Data Extraction Membership Inference – pulling sensitive information from the model

Adversarial Evasion Attack – attackers make tiny changes to the input data that humans do not recognize

DATA

MODEL

APP

YOU

Data Collection

Training

Deployment

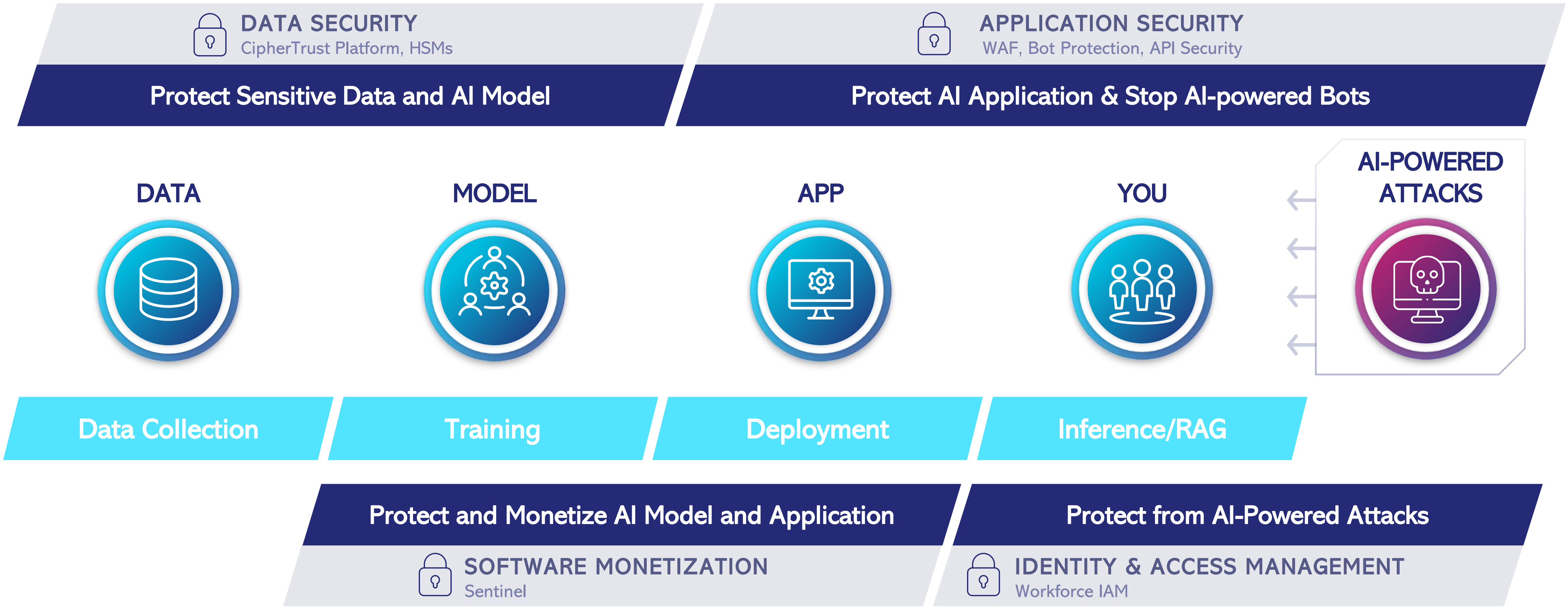
Inference/RAG

Model Theft

THALES
Building a future we can all trust

Secure the AI Lifecycle with Thales

Thales helps organizations protect the AI lifecycle from model development and training to deployment and usage.



DATA SECURITY
CipherTrust Platform, HSMs

Protect Sensitive Data and AI Model

APPLICATION SECURITY
WAF, Bot Protection, API Security

Protect AI Application & Stop AI-powered Bots

DATA

MODEL

APP

YOU

AI-POWERED ATTACKS

Data Collection

Training

Deployment

Inference/RAG

Protect and Monetize AI Model and Application

SOFTWARE MONETIZATION
Sentinel

Protect from AI-Powered Attacks

IDENTITY & ACCESS MANAGEMENT
Workforce IAM

Next steps: Learn More

White Paper

Protect LLMs with CipherTrust Transparent Encryption

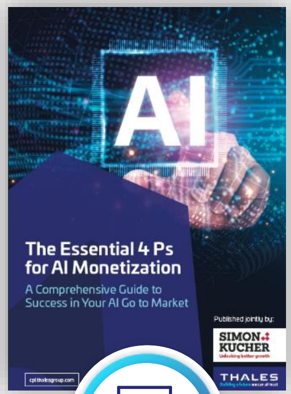
cpl.thalesgroup.com

THALES

Building a future we can all trust

WHITE PAPER

Protect LLMs
with Transparent Encryption



AI

The Essential 4 Ps for AI Monetization

A Comprehensive Guide to Success in Your AI Go to Market

Published jointly by:

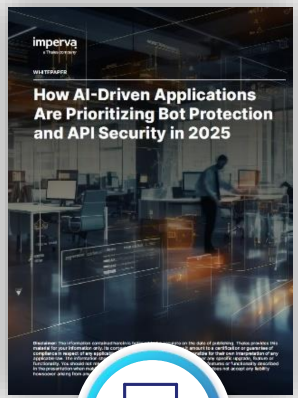
SIMON-KUCHER

THALES

cpl.thalesgroup.com

WHITE PAPER

Protect and Monetize Your Machine Learning Models



imperva

a Thales company

WHITEPAPER

How AI-Driven Applications Are Prioritizing Bot Protection and API Security in 2025

WHITE PAPER

AI-Driven Applications Prioritizing Bot Protection and API Security in 2025

BLOG

Deepfake Fraud – Protection Strategies

SCHEDULE A DEMO

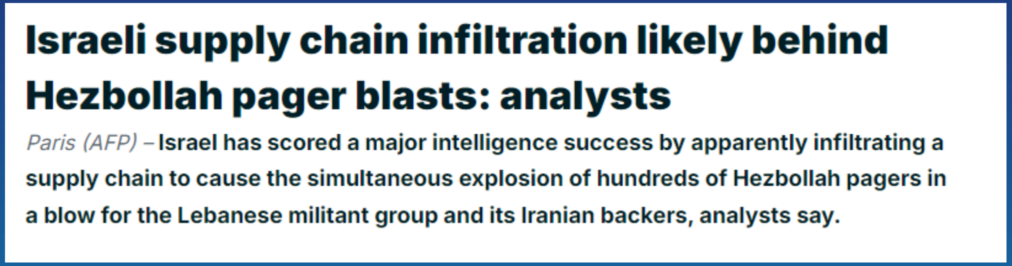
LEARN MORE ABOUT OUR USE CASES

TALK TO A REPRESENTATIVE

THALES

Building a future we can all trust

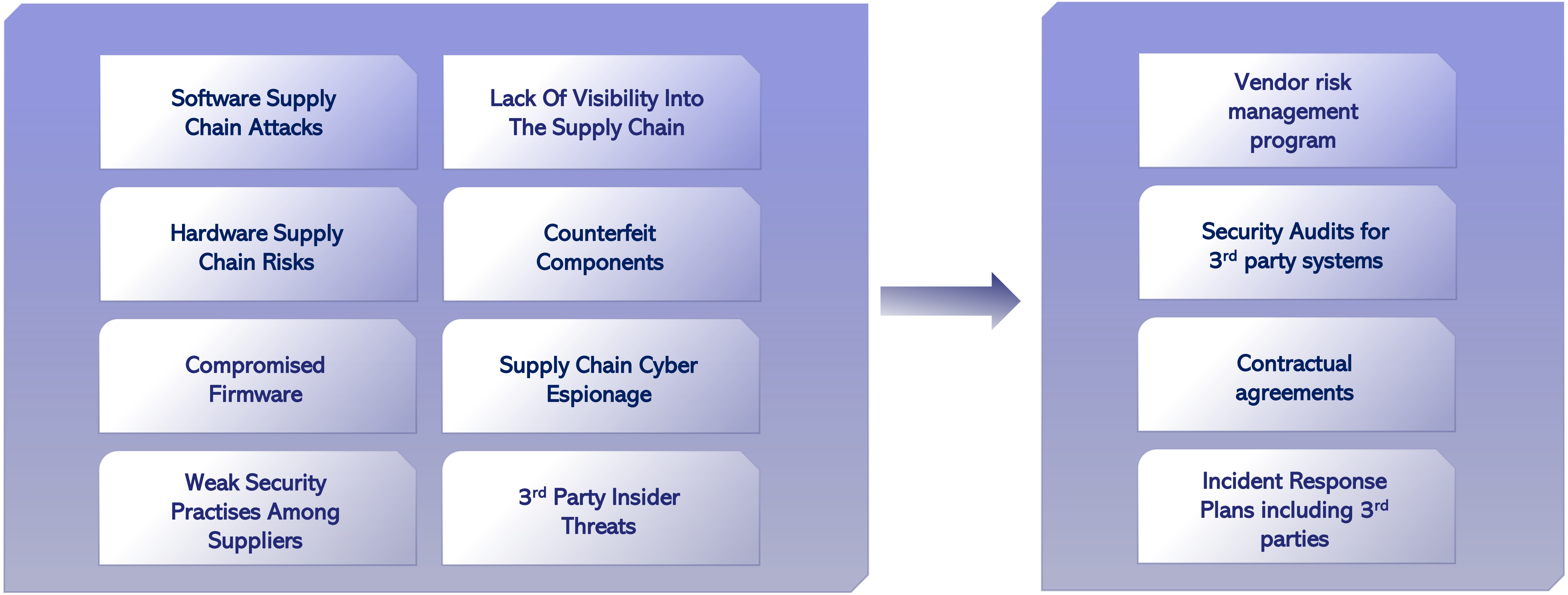
MegaTrend #2 Supply Chain Security



Israeli supply chain infiltration likely behind Hezbollah pager blasts: analysts

Paris (AFP) – **Israel has scored a major intelligence success by apparently infiltrating a supply chain to cause the simultaneous explosion of hundreds of Hezbollah pagers in a blow for the Lebanese militant group and its Iranian backers, analysts say.**

MegaTrend 2: Supply Chain Security



Software Supply Chain Attacks

Lack Of Visibility Into The Supply Chain

Hardware Supply Chain Risks

Counterfeit Components

Compromised Firmware

Supply Chain Cyber Espionage

Weak Security Practises Among Suppliers

3rd Party Insider Threats

Vendor risk management program

Security Audits for 3rd party systems

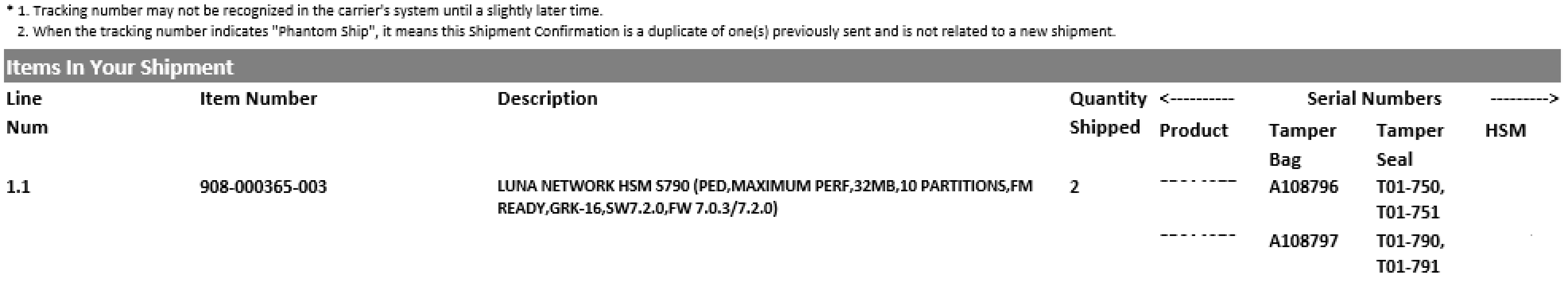
Contractual agreements

Incident Response Plans including 3rd parties

THALES
Building a future we can all trust

MegaTrend 2: Supply Chain Security

Physical protection:

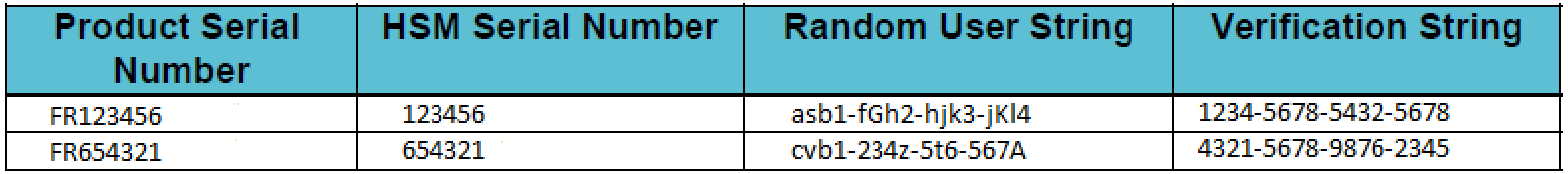


* 1. Tracking number may not be recognized in the carrier's system until a slightly later time.
2. When the tracking number indicates "Phantom Ship", it means this Shipment Confirmation is a duplicate of one(s) previously sent and is not related to a new shipment.

Items In Your Shipment

Line Num	Item Number	Description	Quantity Shipped	<---------- Serial Numbers Product	Tamper Bag	Tamper Seal	HSM --------->
1.1	908-000365-003	LUNA NETWORK HSM S790 (PED,MAXIMUM PERF,32MB,10 PARTITIONS,FM READY,GRK-16,SW7.2.0,FW 7.0.3/7.2.0)	2	--- - ----	A108796	T01-750, T01-751	
				--- - ----	A108797	T01-790, T01-791	

Digital protection:



Product Serial Number	HSM Serial Number	Random User String	Verification String
FR123456	123456	asb1-fGh2-hjk3-jKl4	1234-5678-5432-5678
FR654321	654321	cvb1-234z-5t6-567A	4321-5678-9876-2345

Code Signing

THALES
Building a future we can all trust

MegaTrend #3 - Cloud & Sovereignty

Cloud: a question of who you can trust

Cloud Services

Can you trust on agreements?

Responsibility
Security of the cloud

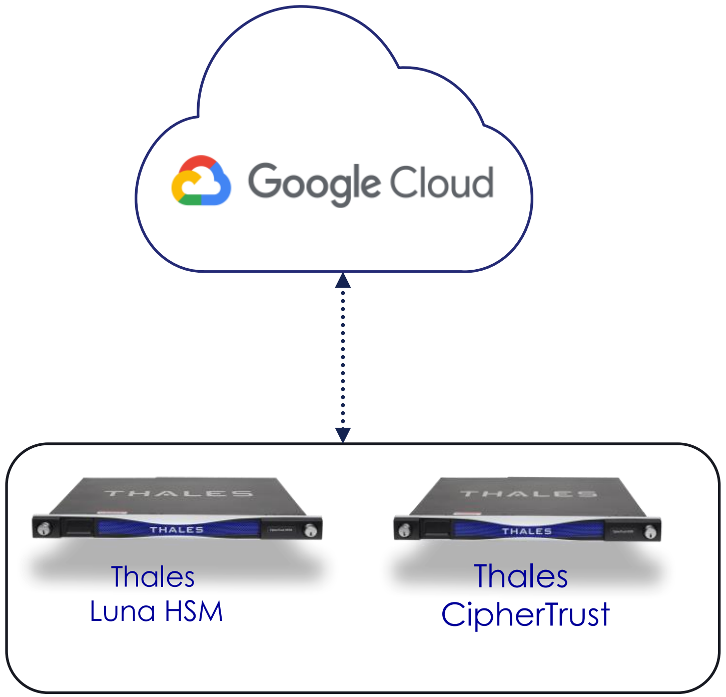
Responsibility
Security IN the cloud

> “#1 driver for sovereignty: need to ‘future-proof’ the security & portability of cloud resources
>
> Thales, *Cloud Security Study*

THALES
Building a future we can all trust

Case 1 – Large private healthcare provider

Data at rest in GCP is encrypted with encryption keys that are under the customer's control and operated in a domestic data center.



New digital services are at the core of the customer's strategy. Significant investment in digital development.

Cloud-native software development, modern development tools, and the flexibility of the cloud provide a framework that accelerates digital services development.

The customer considers hardening the cloud environment, along with related technical security and processes, as very important enablers for new business.

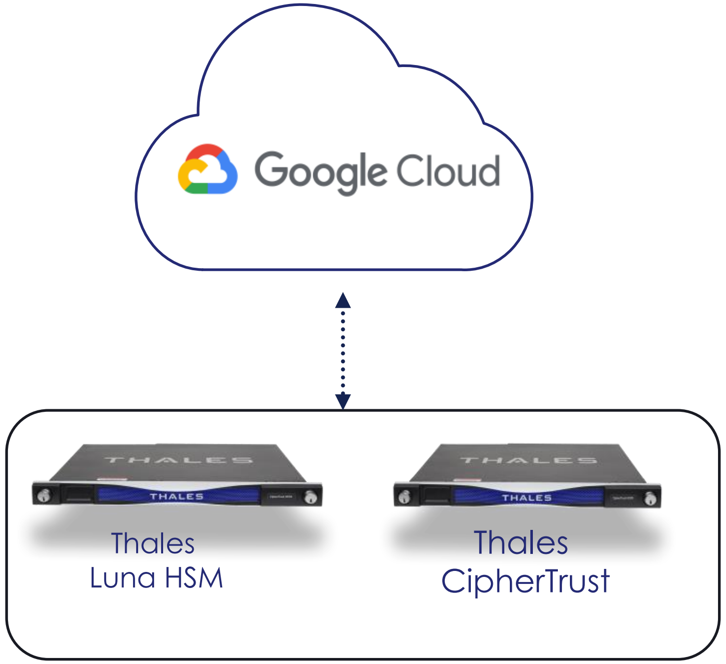
Data protection matters and data privacy impact assessment played a key role.

Google & Thales together helped the customer build a hardened GCP environment.

Project duration: approximately 12 months.

Case 2 – Large telecom manufacturer

vSAN encryption is used in the Google Cloud VMware environment. The customer manages the vSAN encryption keys themselves.



The customer sought cost benefits by moving a large number of legacy applications to the cloud.

In a lift & shift migration, 470 virtual machines were moved to the GCP cloud's VMware environment.

vSAN encryption was implemented in the VMware environment. Everything written to disk/storage is encrypted with the customer's own encryption keys.

The encryption keys are 100% under the customer's control and are operated in the Thales CipherTrust environment.

Project duration: approximately 3 months

MegaTrend #4 - DevSecOps

DevSecOps was

the number one concern for nearly two-thirds of the respondents (63%).

Secrets Management (56%) is the number one DevOps challenge

Thales, Data Threat Report

- Integrates security early in the Sw. development lifecycle
- Catches vulnerabilities before they reach production.
- Reduces risk and cost
  Fixing issues early is cheaper and safer.
- Enables faster, secure delivery
  Security is automated alongside development and operations.
- Promotes team collaboration
  Breaks down silos between Dev, Sec, and Ops.
- Supports compliance and governance
  Automates security policies and reporting.

MegaTrend #4 - DevSecOps

Secure by Design
Include threat modeling and security requirements from day one.

SBOMs (Software Bill of Materials)
More teams are tracking all components and dependencies for transparency and compliance.

Automation & Policy-as-Code
Security policies are enforced automatically in the CI/CD pipeline. Automation tools such as secrets management systems are implemented.

AI in DevSecOps
AI is being used to detect anomalies, automate threat detection, and enhance code reviews.

Continuous Compliance
Automate compliance checks (e.g., for GDPR, ISO 27001) throughout development.

Developer Empowerment
Give developers the tools and training to write secure code from the start.

MegaTrend #5 – Regulation – NIS2-DORA-EU-NATO

Regulations like **DORA** and **NIS2** reflect the EU's stronger stance on cybersecurity and IT risk management. Organizations are now required to implement more robust, secure, and resilient IT systems. Compliance is no longer optional—it's essential for operational continuity and legal accountability

DORA – Digital Operational Resilience Act

ICT Risk Management

ICT 3rd Party Risk Management

ICT Incident Management

Data and Cyber resilience

Cloud and Digital Sovereignty

Latest Regulations mandate:

- Access control & monitoring
- Data encryption At rest, in motion, in use, with 3rd party
- Crypto Key lifecycle management
- Crypto agility & PQC
- Fast Detect, Respond and Forensic Reporting
- Cloud / 3rd Party Risk Management
- Cyber Resilience stress tests
- AI Risk Management

MegaTrend #5 – Regulation – EU & NATO

EU classified data

EU Top Secret
EU Secret
EU Confidential
EU Restricted

Nato classified data

Cosmic Top Secret
Nato Secret
Nato Confidential
Nato Restricted

National – Finland- Estonia

Finland TL1 - Top Secret – Täiesti salajane
Finland TL2 – Secret - Salajane
Finland TL3 - Confidential - Konfidentsiaalne
Finland TL4 - Restricted - Piiratud

KeyTrend:

National authorities in Nordics and Baltics have taken a very strict position that only approved products should be used for each confidentiality level.

The Cryptel-IP TCE 621 – for all NATO security levels

> High grade network encryption

- Approved by NATO for all security levels

> Securing communication networks

- From strategic to tactical solutions
- From administrative, to command and control and real time networks

> In use in NATO, NATO operations and in all NATO membership countries

- De-facto industry standard

Thales Mistral for EU & NATO restricted

IPsec Gateways

IP9001
Up to 1Gb/s

IP9010
Up to 10 Gb/s

VM (virtual Machine)

IPsec client (Windows)

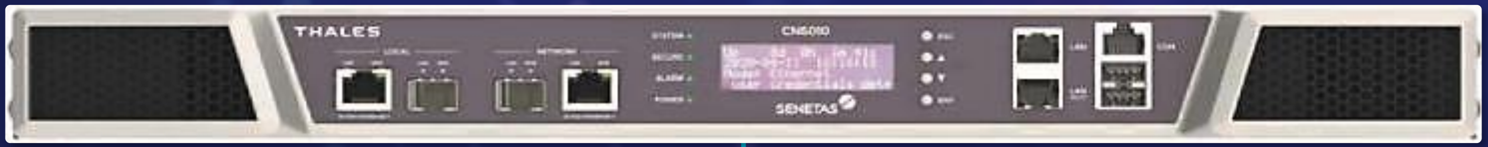
Centralized Management

Virtualized Management Center Software

Customer Services

Expertise and Architects
Training
Installation
Engineering / deployment
Technical Support

Thales Layer 2 High Speed Encryption (HSE)



Trusted Security

Globally certified
and quantum safe

Maximum Performance

Up To 100 Gbit/s

Improved bandwidth and
latency efficiency over IPsec

Optimal Flexibility

Vendor agnostic / bump in the
wire Drops seamlessly into Layer
2, 3, and 4 infrastructure

MegaTrend #5 – Regulation – How Thales can help?

Thales in an European Company

Many of our products are on the NATO & EU approved product list

Our products also have NIST & Common Criteria Approvals

Lunch