
THALES
Building a future we can all trust
Partner
CONNECT
2025
www.thalesgroup.com

Vielen Dank
an unsere Sponsoren

ADN®

infinigate
spark your growth

ARROW

THALES
Building a future we can all trust

Partner
CONNECT

Der Vormittag

Begrüßung

Rückblick ’24=Ausblick ’25
Kai Wolff

Die Thales Channel-Methode und was unsere Partner davon haben
Tobias Pollett

Unternehmenssicherheit 2025
Armin Simon

12:00 Lunch

Der Mittag ab 13:30

Der Thales Schutzschirm und die Last Line of Defense: der umfassende Schutz kritischer Daten

Markus Hofbauer

Der Schutzschirm: Applikationssicherheit für eine reibungslose Wertschöpfung

Stephan Dykgers & Kattia Wiemann

Reifegraderhöhung in der Informationssicherheit

Martin Gegenleitner

14:45 Kaffeepause

Der Nachmitag ab 15:15

DevSecOps-Relevanz nimmt massiv zu. Was kann man tun?

Martin Gegenleitner, Julian Iavarone

Projekt Highlights, die Spaß machen

Kattia Wiemann, Sascha Pfadenhauer & Martin

Die Zukunft der Thales Security

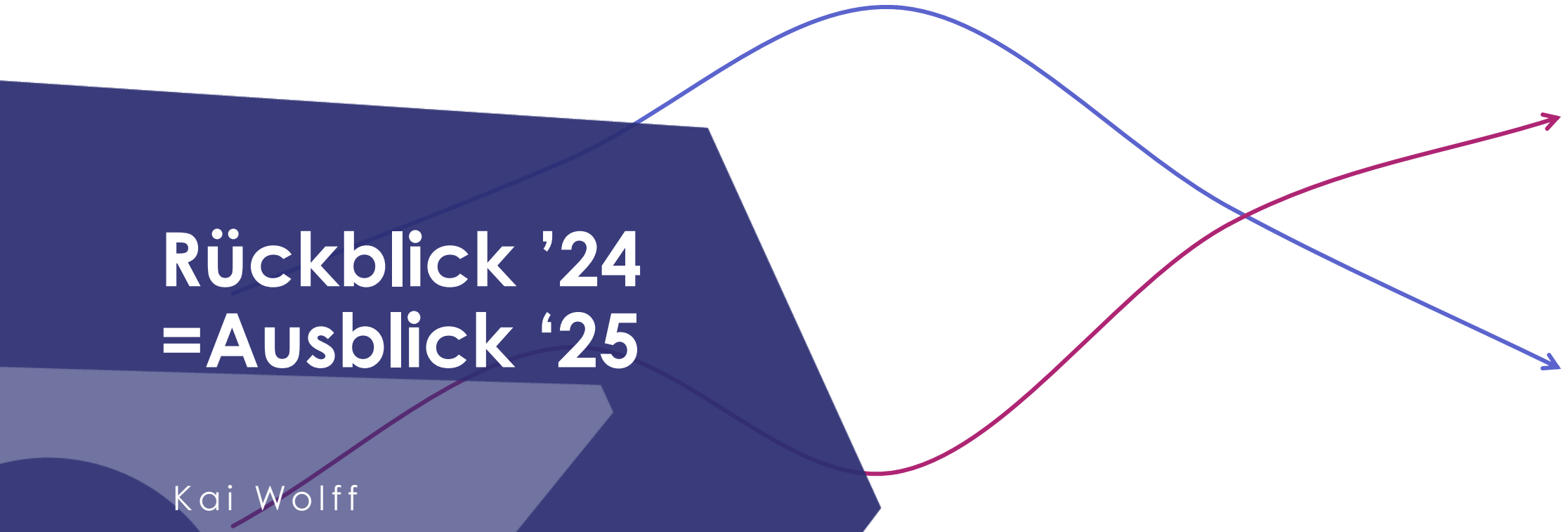
Tim Ayling, VP EMEA Cyber Specialists

Q&A, Abschluss gegen **17:00**

Thales-Team

Ab 18:00 Abendessen und Networking

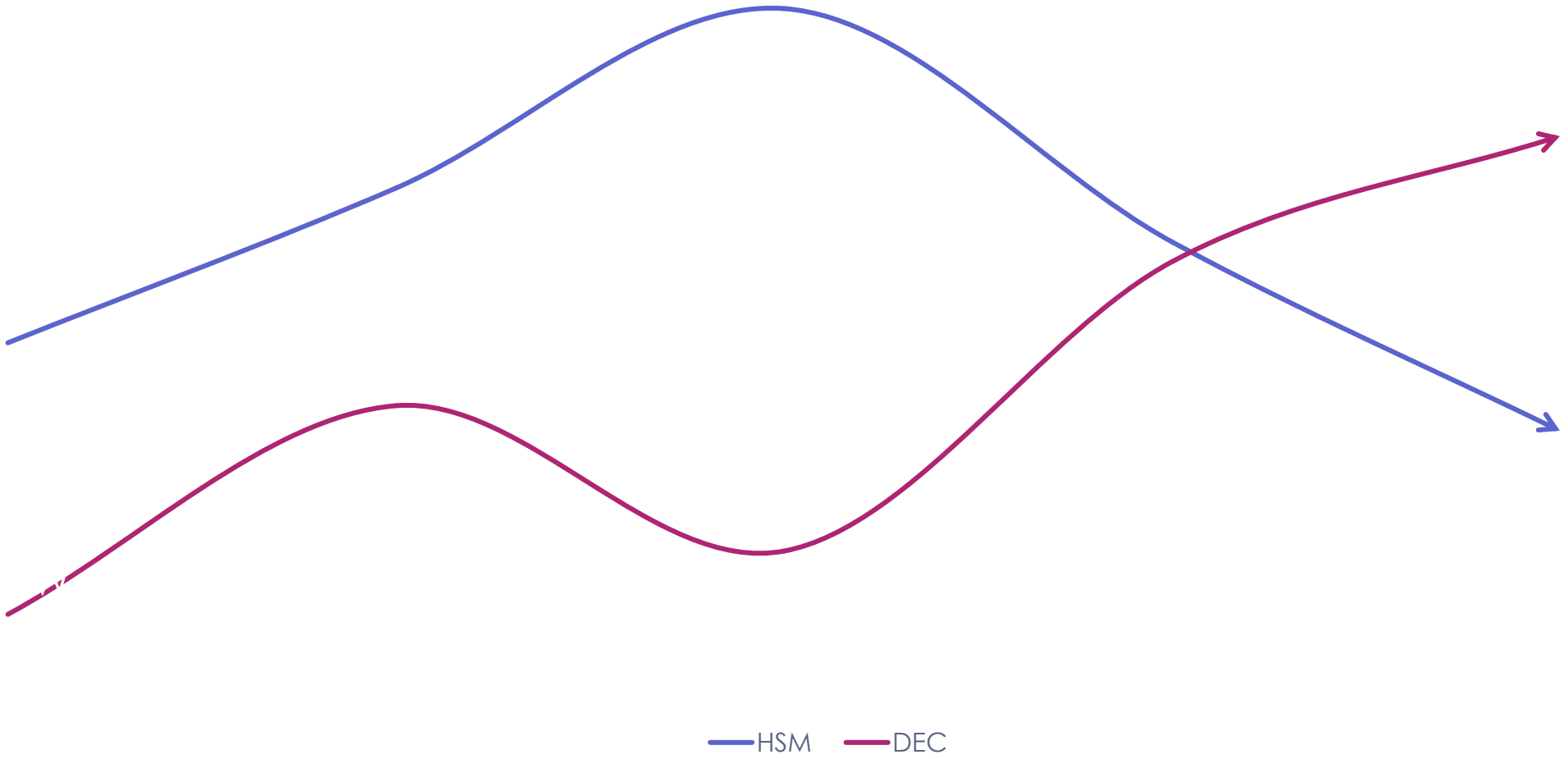
Produktsplit New Business



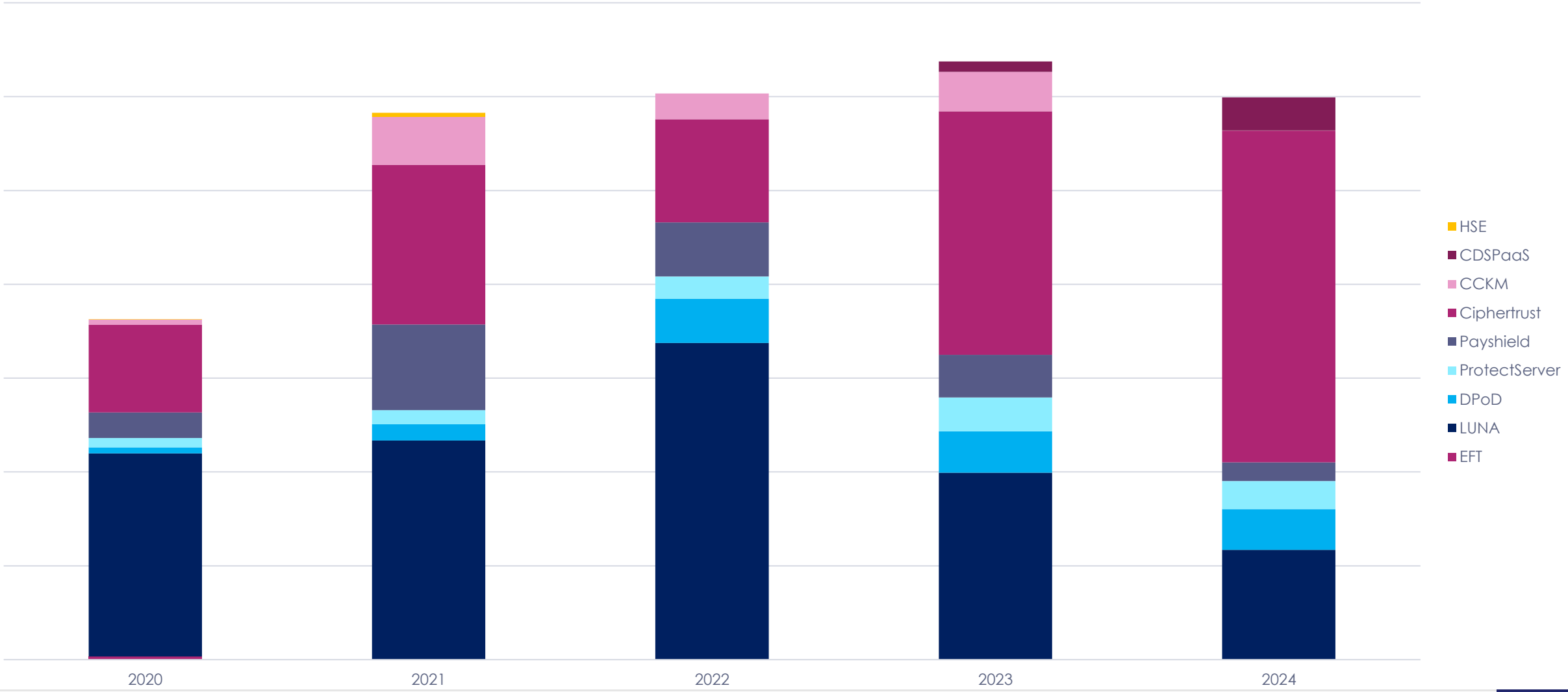
Rückblick ’24 =Ausblick ‘25

Kai Wolff

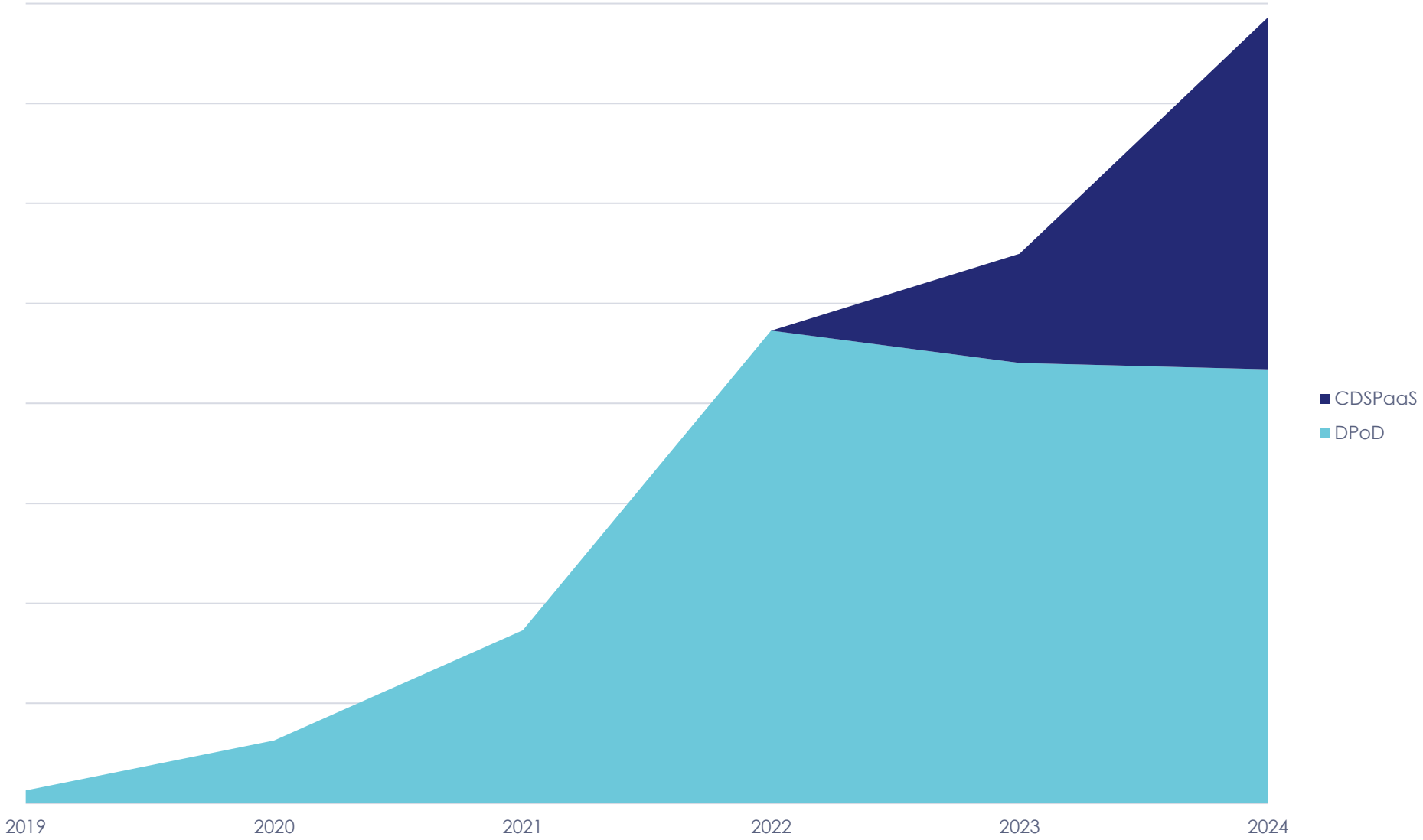
Produktsplit New Business



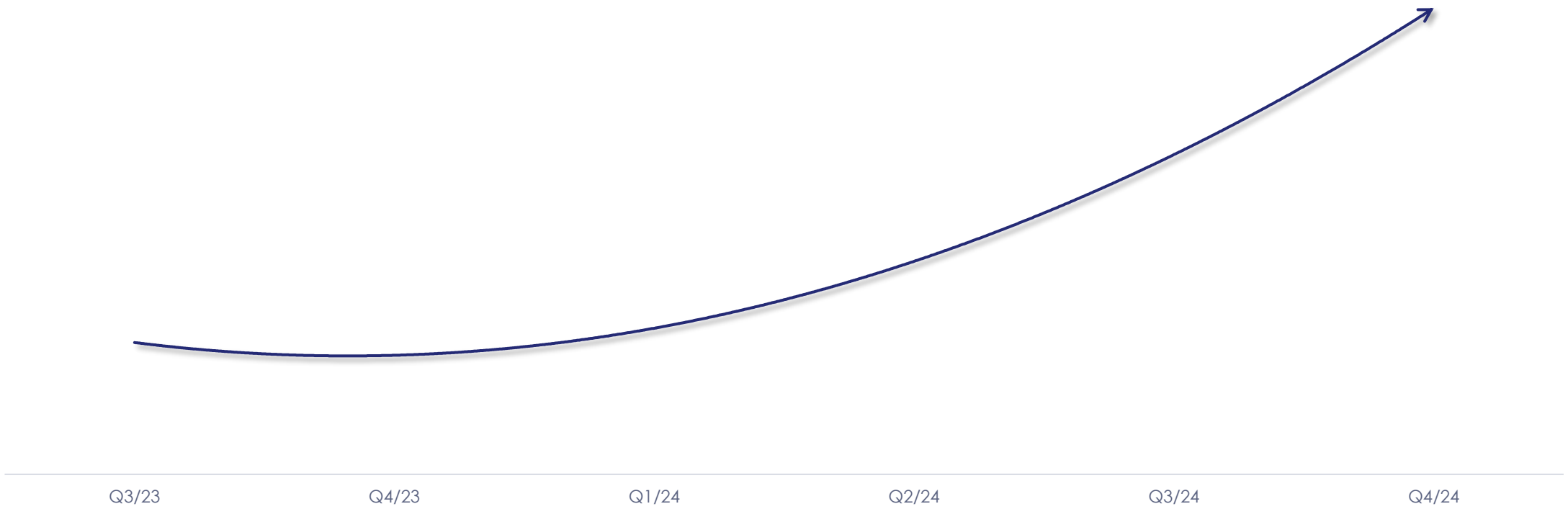
Produktsplit New Business



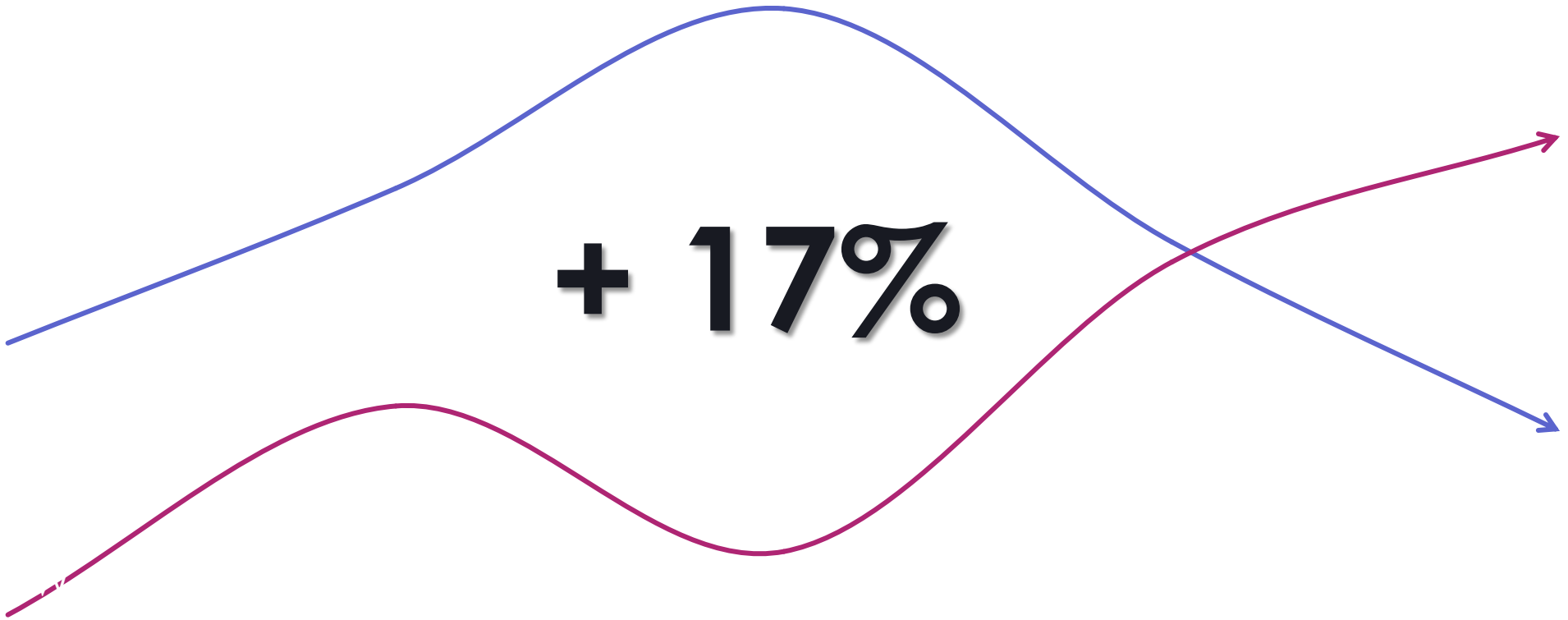
DPoD Germany Entwicklung



AppSec-Umsatzentwicklung 2024



Umsatzsteigerung zum Vorjahr




THALES
Building a future we can all trust
Partner
CONNECT
Die Thales Channel Methode
und was unsere Partner
davon haben
Tobias Pollett
Channel Account Manager
www.thalesgroup.com

HENRY FORD

"Coming together is a beginning.

Keeping together is progress.

Working together is success."

Herausforderungen Thales

> Kleines Team – Großer Markt

> Teil von etwas Großen

> Komplexes Thema

Herausforderungen Reseller

- Differenzierung
- Intensiver Wettbewerb
- Direktvertrieb Hersteller

Thales Channel-Methode

Wir verstehen unsere Partner

> Individuelle Stärken

> Beratung oder Abwicklung

> Erfahrung bei Resellern

Wir schulen unsere Partner

> Wissen ist Macht

> Basis für Differenzierung

> Professional Service

Wir wachsen mit unseren Partnern

> Wachstumsmarkt

> Marktführer

> Erweitertes Portfolio

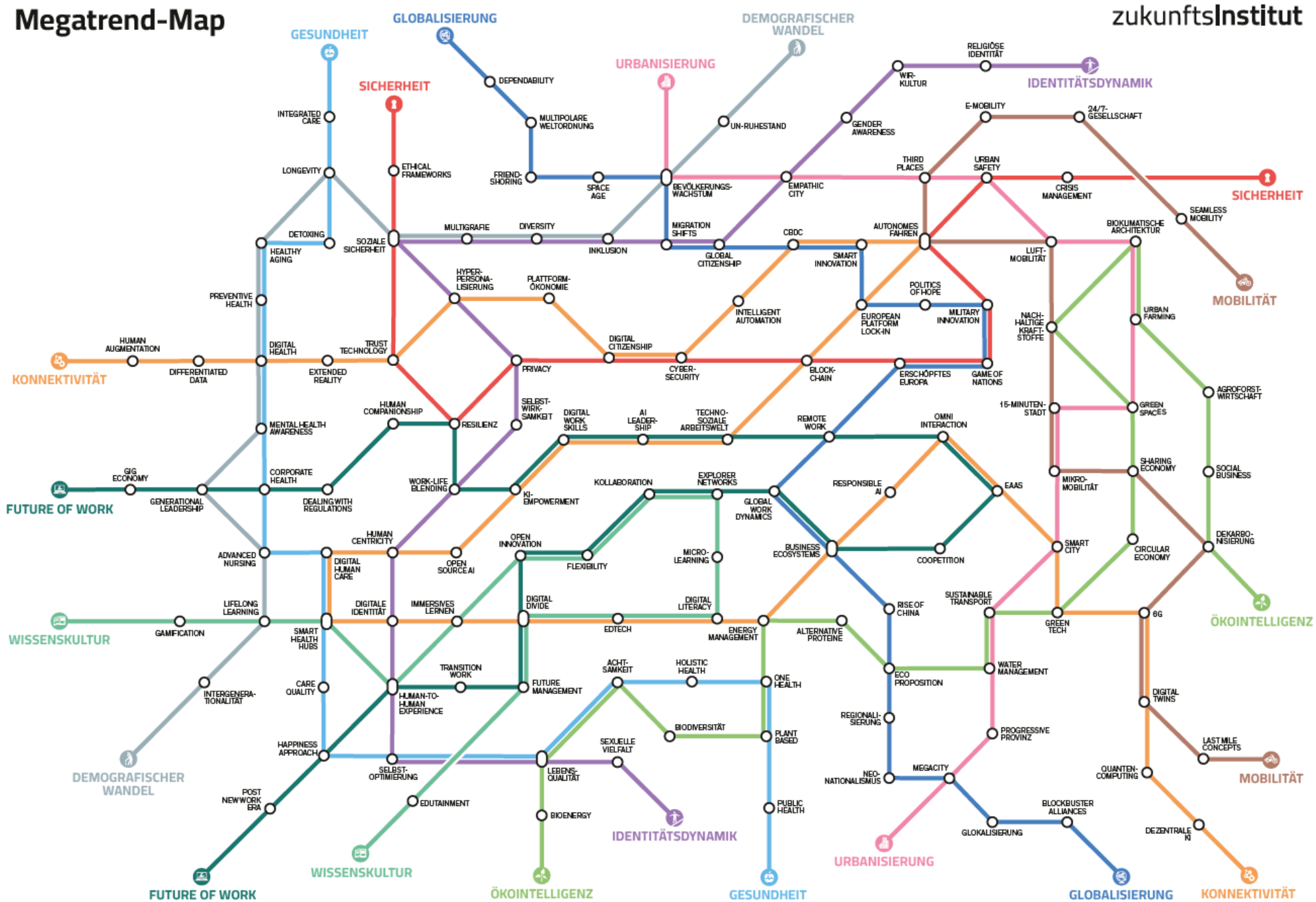
Danke!

Hmm ...

In was für einer Welt leben wir eigentlich?

https://megatrends.fandom.com/de/wiki/Proll-Professionals

https://www.zukunftsinstitut.de/megatrends



https://megatrends.fandom.com/de/wiki/Proll-Professionals

https://www.zukunftsinstitut.de/megatrends

Hi, ich werde einen Vortrag zu Thema MegaTrends vor etwa 50 Leuten haben. Ich möchte den Vortrag mit der Frage "In was für einer Welt leben wir eigentlich?" beginnen. Wie würdest Du in diesem Zusammenhang diese Frage beantworten?

Hallo! Das ist ein spannendes Thema für einen Vortrag. Um die Frage „In was für einer Welt leben wir eigentlich?“ zu beantworten, könntest du verschiedene Aspekte und MegaTrends ansprechen. Hier sind einige Ansätze, die dir helfen könnten, deine Antwort zu strukturieren:

1. **Technologischer Fortschritt**: Wir leben in einer Zeit rasanter technologischer Entwicklungen. Künstliche Intelligenz, Automatisierung und das Internet der Dinge verändern unser tägliches Leben und die Arbeitswelt grundlegend.
2. **Globalisierung**: Die Welt ist stärker vernetzt als je zuvor. Informationen, Waren und Dienstleistungen bewegen sich schnell über Grenzen hinweg, was sowohl Chancen als auch Herausforderungen mit sich bringt, etwa in Bezug auf Kultur, Wirtschaft und Umwelt.
3. **Nachhaltigkeit und Umweltbewusstsein**: Angesichts des Klimawandels und der Ressourcenknappheit ist ein wachsendes Bewusstsein für Nachhaltigkeit zu beobachten. Unternehmen und Gesellschaften versuchen zunehmend, umweltfreundliche Praktiken zu integrieren.
4. **Demografische Veränderungen**: Die Weltbevölkerung wächst, aber sie altert auch. Diese Veränderungen beeinflussen die Märkte, die Gesundheitssysteme und die sozialen Strukturen weltweit.
5. **Soziale Veränderungen und Werte**: Die Gesellschaft verändert sich in Bezug auf Gleichheit, Diversität und soziale Gerechtigkeit. Die Stimmen der jüngeren Generationen werden lauter und fordern Veränderungen in der Politik und in Unternehmen.
6. **Gesundheit und Lebensqualität**: Die COVID-19-Pandemie hat unser Verständnis von Gesundheit und Wohlbefinden in Frage gestellt und gezeigt, wie wichtig Resilienz und Vorbereitung auf Krisen sind.

Indem du diese Aspekte ansprichst, kannst du eine umfassende Vorstellung davon vermitteln, in was für einer Welt wir leben, und die Zuhörer dazu anregen, über die Entwicklungen und deren Auswirkungen nachzudenken. Viel Erfolg mit deinem Vortrag!

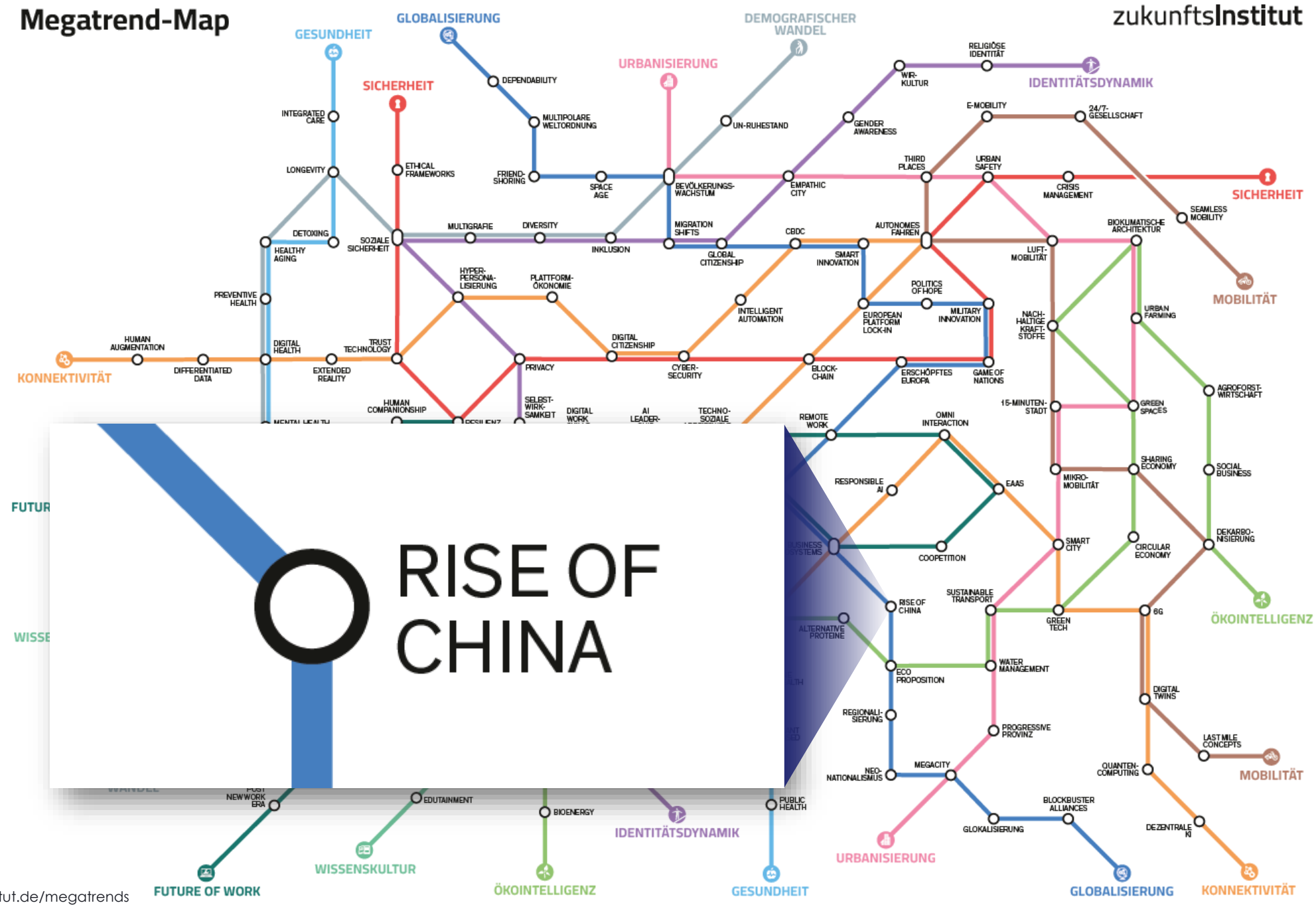

DIESEL

Hi, ich werde einen Vortrag zu Thema MegaTrends vor etwa 50 Leuten haben. Ich möchte den Vortrag mit der Frage "In was für einer Welt leben wir eigentlich?" beginnen. Wie würdest Du in diesem Zusammenhang diese Frage beantworten?

Hallo! Das ist ein spannendes Thema für einen Vortrag. Um die Frage „In was für einer Welt leben wir eigentlich?“ zu beantworten, könntest du verschiedene Aspekte und MegaTrends ansprechen. Hier sind einige Ansätze, die dir helfen könnten, deine Antwort zu strukturieren:

1. **Technologischer Fortschritt**: Wir leben in einer Zeit rasanter technologischer Entwicklungen. Künstliche Intelligenz, Automatisierung und das Internet der Dinge verändern unser tägliches Leben und die Arbeitswelt grundlegend.
2. **Globalisierung**: Die Welt ist stärker vernetzt als je zuvor. Informationen, Waren und Dienstleistungen bewegen sich schnell über Grenzen hinweg, was sowohl Chancen als auch Herausforderungen mit sich bringt, etwa in Bezug auf Kultur, Wirtschaft und Umwelt.
3. **Nachhaltigkeit und Umweltbewusstsein**: Angesichts des Klimawandels und der Ressourcenknappheit ist ein wachsendes Bewusstsein für Nachhaltigkeit zu beobachten. Unternehmen und Gesellschaften versuchen zunehmend, umweltfreundliche Praktiken zu integrieren.
4. **Demografische Veränderungen**: Die Weltbevölkerung wächst, aber sie altert auch. Diese Veränderungen beeinflussen die Märkte, die Gesundheitssysteme und die sozialen Strukturen weltweit.
5. **Soziale Veränderungen und Werte**: Die Gesellschaft verändert sich in Bezug auf Gleichheit, Diversität und soziale Gerechtigkeit. Die Stimmen der jüngeren Generationen werden lauter und fordern Veränderungen in der Politik und in Unternehmen.
6. **Gesundheit und Lebensqualität**: Die COVID-19-Pandemie hat unser Verständnis von Gesundheit und Wohlbefinden in Frage gestellt und gezeigt, wie wichtig Resilienz und Vorbereitung auf Krisen sind.

Indem du diese Aspekte ansprichst, kannst du eine umfassende Vorstellung davon vermitteln, in was für einer Welt wir leben, und die Zuhörer dazu anregen, über die Entwicklungen und deren Auswirkungen nachzudenken. Viel Erfolg mit deinem Vortrag!



https://www.zukunftsinstitut.de/megatrends

https://www.zukunftsinstitut.de/megatrends

https://www.zukunftsinstitut.de/megatrends

THALES
Building a future we can all trust

Partner CONNECT

Unternehmenssicherheit 2025

Armin Simon,
Regional Sales Director Germany

Weltlage

Bild: AdobeStock-andy

Foto: Ben Curtis / AP

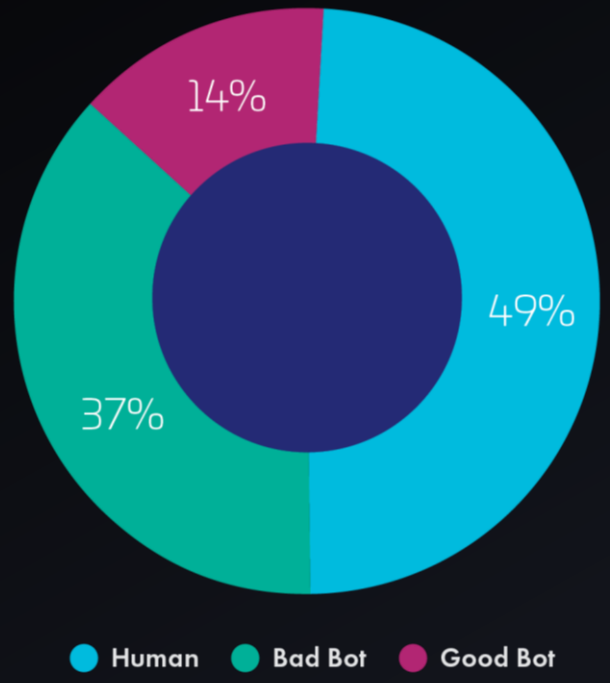
Bild: © Michael Bihlmayer / Action Press

Es besteht eine erhöhte Gefährdung in Bezug auf Sabotageaktivitäten, beziehungsweise entsprechende Vorbereitungshandlungen in Deutschland.

Sicherheitshinweis des Bundesamtes für Verfassungsschutz,
26. Juli 2024

Thales BOT Report 2025

GLOBAL INTERNET TRAFFIC PROFILE IN 2024



AI

DAILY AVERAGE NUMBER OF AI-ENABLED ATTACKS

2 MILLION

Verstärkter Einsatz von BOT Netzen

<u>klassische Bad BOT Aktivitäten</u>

- *Scraping* – unerlaubtes kopieren von Inhalten und Preisdaten
- *DDoS Angriffe* – Services lahmlegen
- *Manipulation* des Dynamic Pricing
- *Ticket-Scalping* – Automatischer Aufkauf von Tickets
- *Fake-Bewertungen*
- *Brute-Force-Angriffe* - Passwörter knacken

<u>BOT Sabotage Aktivitäten in DE (BSI)</u>

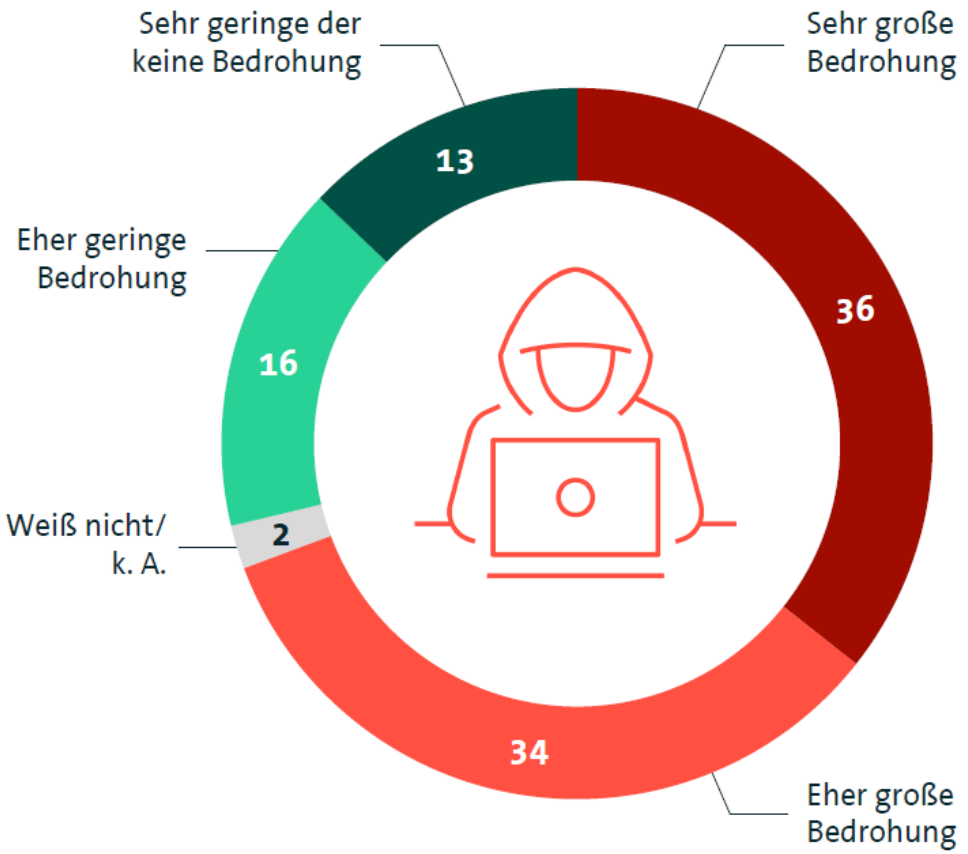
- *Desinformation* durch Social Bots und Fake Profile
- *Verbreitung gefälschter Terrorwarnungen* durch Russlandnahe Bot-Netzwerke
- *Sabotage* durch mittels Chat Bots angeworbener Agenten
- *Gezielte Angriffe* auf deutsche Unternehmen durch Bot-Netze

Studie Bitkom – Wirtschaftsschutz vom 24.08.2024

7 von 10 Unternehmen fühlen sich stark durch analoge und digitale Angriffe bedroht

Inwieweit sehen Sie analoge und digitale Angriffe wie Datendiebstahl, Industriespionage und Sabotage als Bedrohung für Ihr Unternehmen?

in Prozent



2 Basis: Alle Unternehmen (n=1.003) | Abweichungen von 100 Prozent sind rundungsbedingt | Quelle: Bitkom Research 2024

bitkom

Studie Bitkom – Wirtschaftsschutz 2024

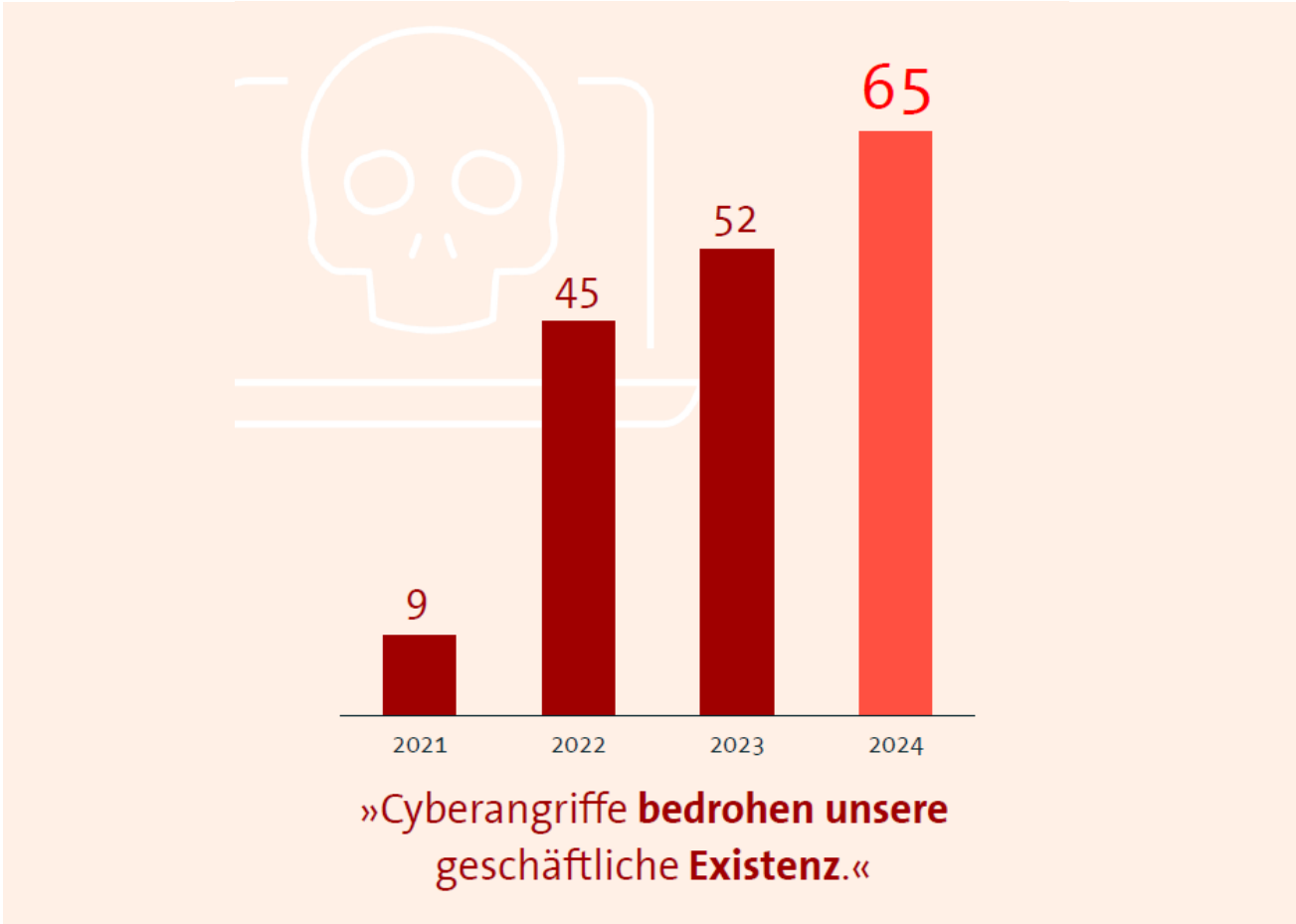
Zwei Drittel der Unternehmen sehen sich durch Cyberattacken in ihrer Existenz bedroht

Inwieweit treffen die folgenden Aussagen zu?

53%

»Unser Unternehmen ist auf Cyberangriffe sehr gut vorbereitet.«

in Prozent



14 Basis: Alle Unternehmen (n=1.003) | Prozentwerte für »Trifft voll und ganz zu« und »Trifft eher zu« | Quelle: Bitkom Research 2024

bitkom

Insolvenzen durch Cyberangriffe

VARTA

SCHUMAG
Neuer Schub für die Zukunft.

ERFO
be yourself

Gigaset

KREISEL
since 1912

Schäden durch Cyberangriffe 2024
+ 29% / 267 Mrd € (Bitkom)

Aktuelle Herausforderungen und Strategien zur Unternehmenssicherheit

Aktuelle Herausforderungen und Strategien zur Unternehmenssicherheit

Allianz Risk Barometer 2025
Hauptrisiko - Cyber Vorfälle:

- Cyber Crime
- IT-network and Service Disruption
- Malware/Ransomware
- Data Breaches
- Fines and Penalties

Awareness Training sind Standard

- erste Verteidigungslinie
- Reduzierung menschlicher Fehler
- Bewusstsein für Bedrohungen verbessern

Technische Schutzmassnahmen unbedingt erforderlich!

Mit Chat GPT erstellt

Aktuelle Herausforderungen und Strategien zur Unternehmenssicherheit

SIMON Armin

An: Armin Simon
Betreff: Wichtige Aktualisierung Deiner Gehaltsdaten – Aktion erforderlich bis 28.04.

Hallo Armin,

Im Rahmen der laufenden Lohn- und Gehaltsanpassung bitten wir Dich, Deine persönlichen Angaben in unserem HR-System zu bestätigen und ggf. zu aktualisieren.

Dies betrifft insbesondere:

- Deine Bankverbindung
- Deine Steuer-ID
- Deine Anschrift

Bitte überprüfe Deine Daten bis spätestens 28. April 2025

Solltest Du keine Aktualisierung vornehmen, kann es zu Verzögerungen bei der Gehaltsauszahlung kommen.

Viele Grüße,

Dein Thales HR Team

Mit Chat GPT erstellt

Aktuelle Herausforderungen und Strategien zur Unternehmenssicherheit

Compliance-Anforderungen haben die gleiche Basis

Verschärfte Complianceanforderungen

- **DORA**
  - Drittanbieterrisiko – Exitstrategie
  - Encryption in use
  - Key Lifecycle Management
  - Krypto Agilität → PQC
- **NIS2 -** In Deutschland verzögert. Somit noch nicht verbindlich
  - Massiv verstärkte Haftung der GF (Know-How-Aufbau Pflicht!)
  - BSI NIS-2 Betroffenheitsprüfung verfügbar (Stark ausgeweitet)
  - BSI Kritisprüfungen – Reifegrad wird schon abgefragt

Aktuelle Herausforderungen und Strategien zur Unternehmenssicherheit

Neue politische und wirtschaftliche Unsicherheiten

1. Veränderungen in der internationalen Handelspolitik
2. Data Privacy Framework steht auf der Kippe - „Schrems III“
3. Missbrauch der Technologie-Lieferanten für politische Zwecke

„digitale Souveränität“ bekommt höhere Bedeutung,
Abhängigkeiten vermeiden

Aktuelle Herausforderungen und Strategien zur Unternehmenssicherheit

Digitale Souveränität – zwischen Fremdbestimmung und Autarkie

Fremdbestimmung	Souveränität	Autarkie
Andere entscheiden, was wir tun.	Wir sind handlungsfähig und entscheiden selbst, was wir tun!	Wir machen alles selbst!
Wir verfügen in digitalen Schlüsseltechnologien über keine eigene Kompetenz.	Wir verfügen in zentralen Technologiefeldern, Diensten und Plattformen über eigene Fähigkeiten auf weltweitem Spitzenniveau.	Wir entwickeln und fertigen Schlüsseltechnologien mit eigenen Ressourcen.
Uns fehlt die Fähigkeit, Technologien in puncto Sicherheit zuverlässig zu bewerten und sie im Bedarfsfall zu härten.	Wir sind in der Lage, selbstbestimmt und selbstbewusst zwischen Alternativen leistungsfähiger und vertrauenswürdiger Partner zu entscheiden.	Wir ziehen Technologien aus eigener Fertigung Technologien Dritter auch dann vor, wenn sie weniger leistungsfähig sind.

BITKOM

ten

tik

rems III“

che Zwecke

Fazit


COMPLIANCE
CURRENT CHALLENGGES
AND STRATEGGIES FOR
CORPORATE SECURITY
COMPLLIENCE

Zusammenfassung

Awareness nicht überfokussieren !

- Absicherung Webservices optimieren
- “Secure the breach”
- Zero Trust

Der Gesetzgeber hat reagiert

- Cybersicherheit ist unumgänglich
- Reifegrad Modell wird Standard
- Gestiegene Wichtigkeit von Crypto

Digitale Soveränität als Ziel

- Abhängigkeiten reduzieren
- Exitstrategien einplanen
- Alternativen ermöglichen

Technische Schutzmassnahmen
unbedingt erforderlich!

Zwei letzte Dinge

Mehrwerte der Zusammenarbeit mit Thales :

1. Innovative marktführende Sicherheitslösungen
2. Partnerschaftliche Zusammenarbeit
3. Größter Cyber Security Anbieter Europas
4. Globale Expertise
5. Zukunftsorientierte Entwicklung

„Verschlüsselung funktioniert! **Sauber implementierte, starke Verschlüsselung** ist eines der wenigen Dinge, auf die man sich noch verlassen kann.“

heise Security 09.06.2013

THALES
Building a future we can all trust

Thank you

cpl.thalesgroup.com


Rezeption
THALES
Building a future we can all trust
Partner
CONNECT
THALES
Building a future we can all trust

THALES
Building a future we can all trust

Partner CONNECT

Der Thales Schutzschirm und die Last Line of Defense: der umfassende Schutz kritischer Daten

Markus Hofbauer
Manager Sales Engineer
DACH

www.thalesgroup.com

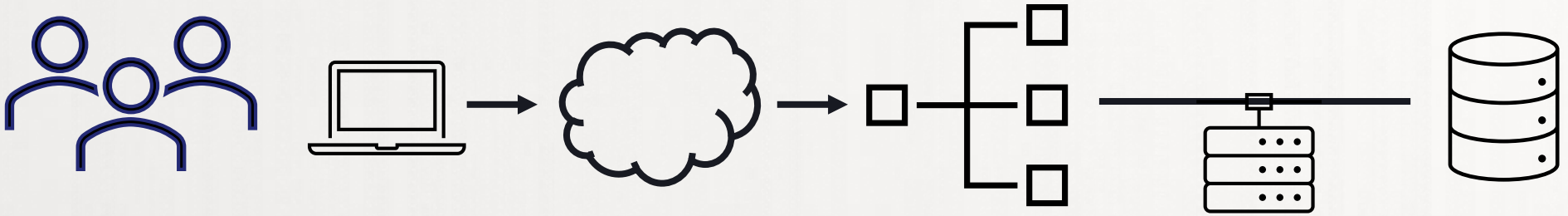
Danke Markus!

Die Thales Story

Die Thales Story

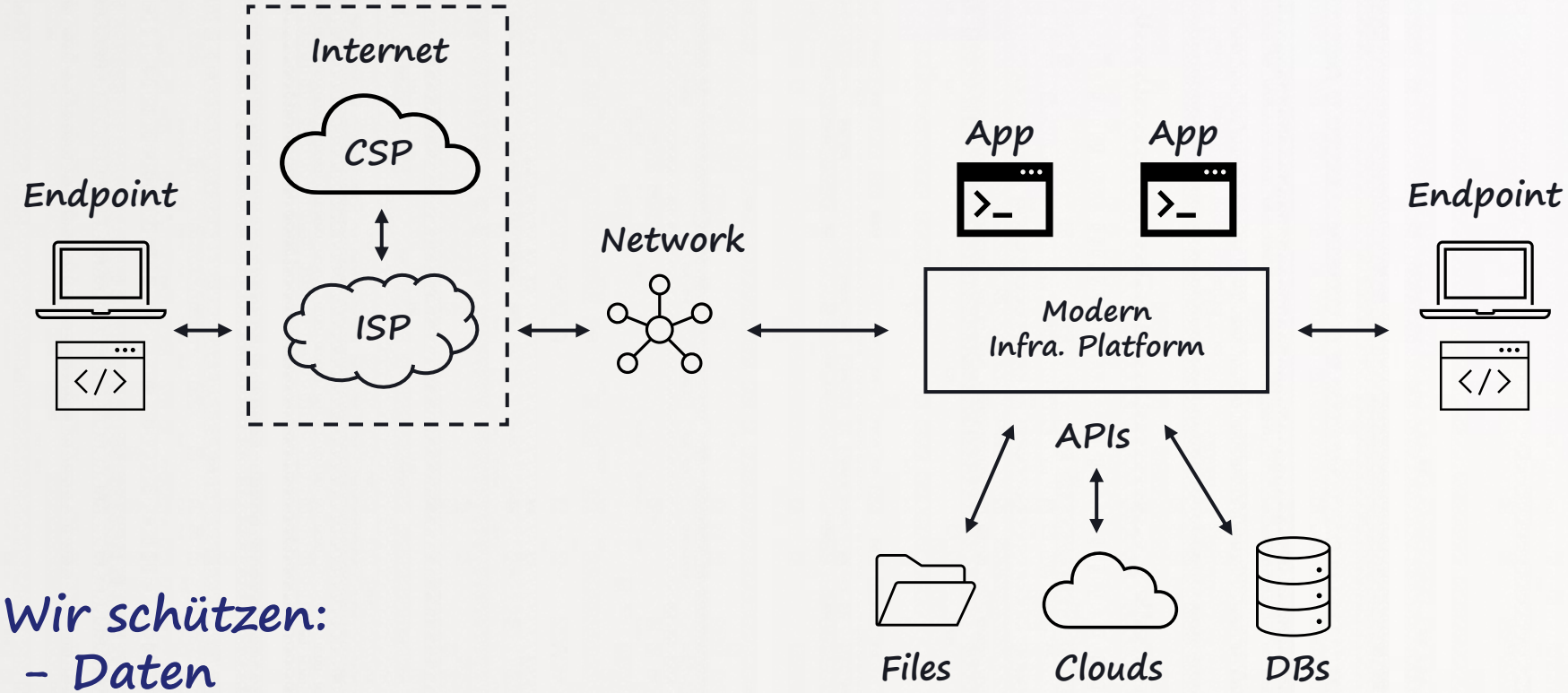
Wir schützen kritische Daten, Applikationen
und die Wege dahin.

Daten



Daten

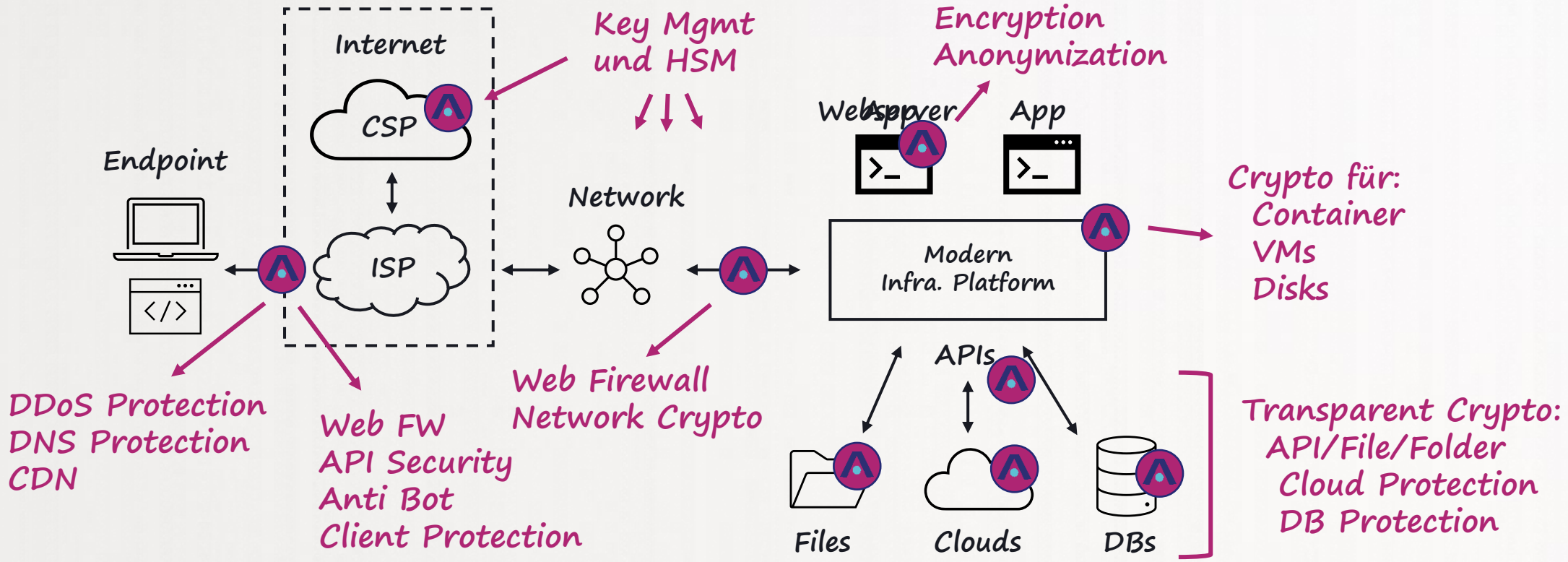
Die Thales Story



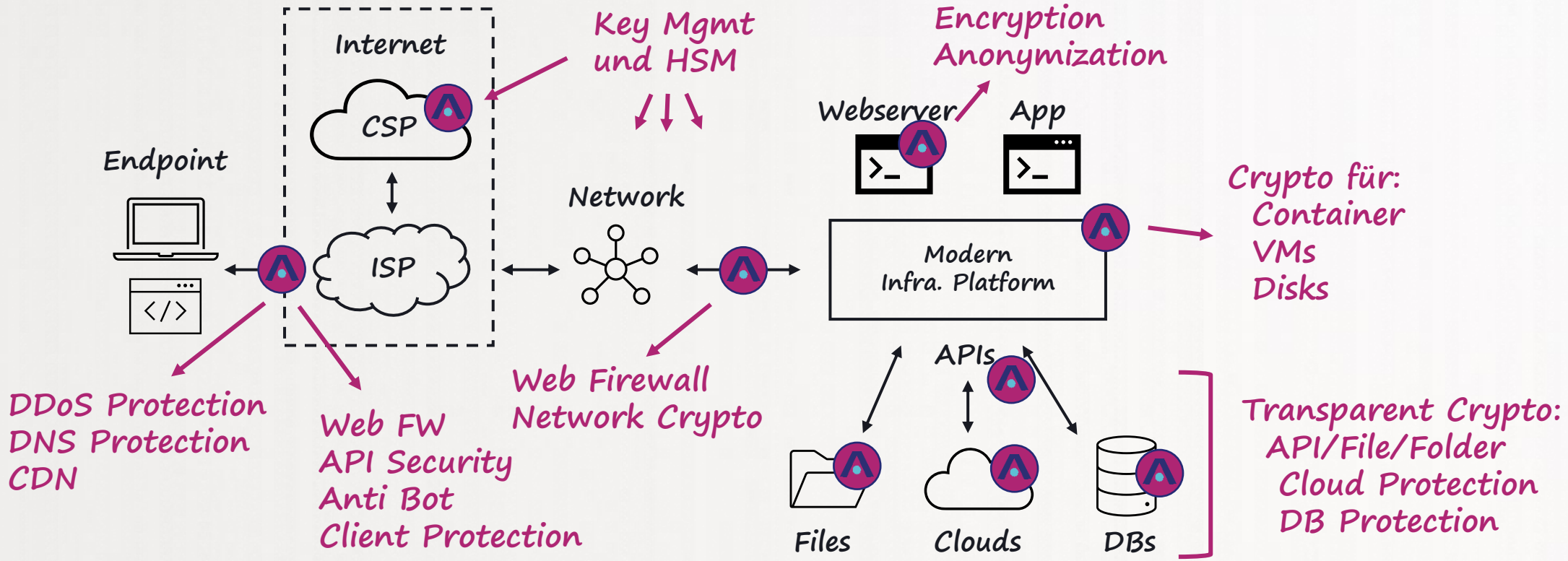
Wir schützen:

- Daten
- Applikationen
- und die Wege dahin

Die Thales Story



Die Thales Story



Thales Data Security Platform

Access Control
Data Discovery
Risk Analytics

Data Intelligence
Data Sovereignty
Data Privacy

Incident Response
Threat Analytics
Compliance Audit

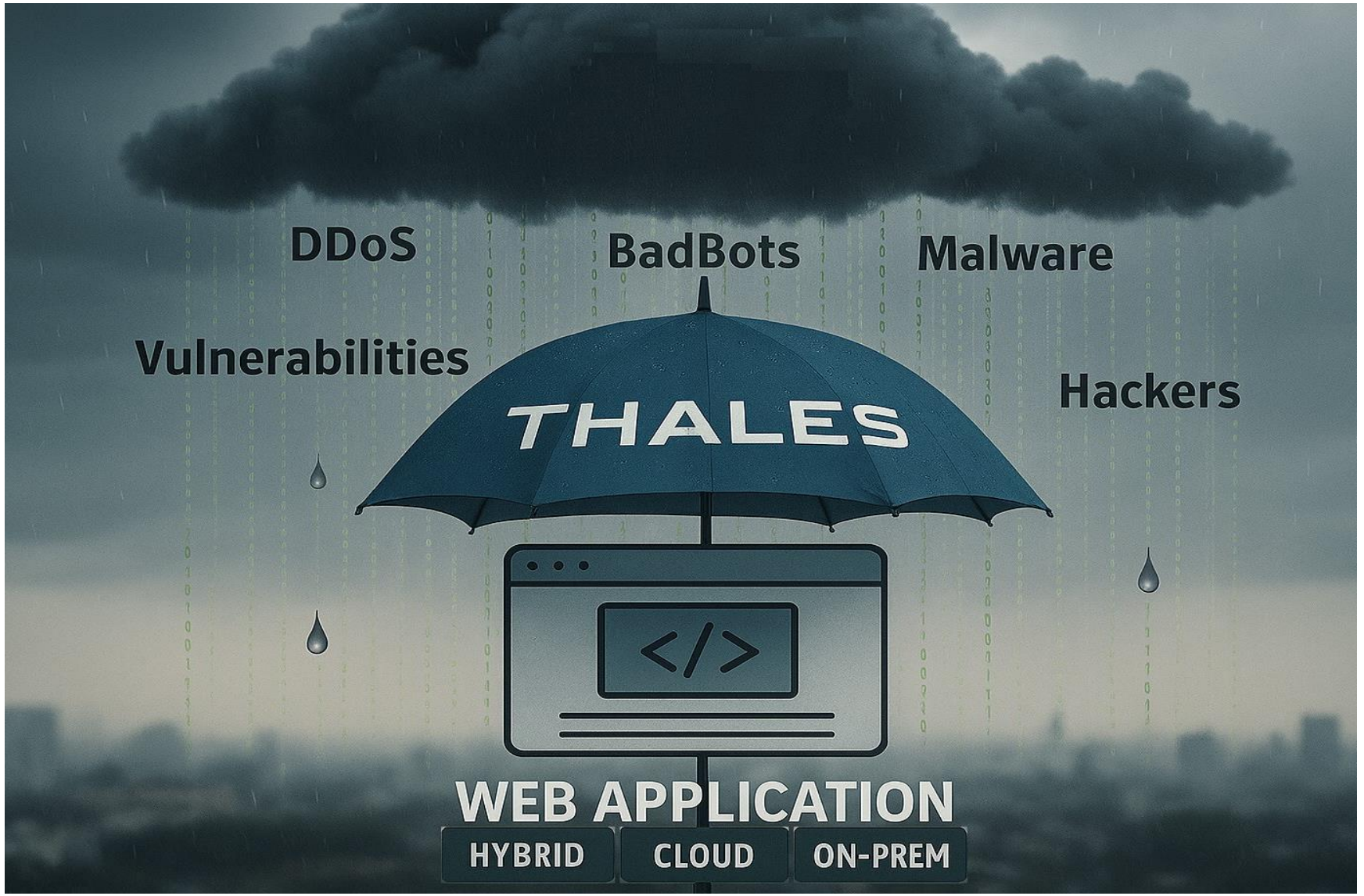
THALES
Building a future we can all trust

Partner CONNECT

Der Schutschirm – Application Security

Stephan Dykgers
Regional Sales Director
Entrprise

www.thalesgroup.com


DDoS
BadBots
Malware
Vulnerabilities
Hackers
THALES
WEB APPLICATION
HYBRID
CLOUD
ON-PREM

Thales Bad Bot Report 04/2025

Bad Bot v Good Bot v Human Traffic 2024

37%
Bad bot

14%
Good Bot

49%
Human

Percentage change from the previous year

Bad Bots	37%	+15,6%
Good Bots	14%	-20,5%
Human	49%	-2.8%

Impact of Bad Bots

- Account Takeover
- DDoS Attacks
- Credential Stuffing
- Commit Fraud
- Web Scraping for AI and LLMs
- Disrupt Business
- Inventory Hoarding
- Target APIs

Quelle: The State of API Security, imperva.com

Key Findings

51% AMOUNT OF AUTOMATED INTERNET TRAFFIC

AMOUNT OF INTERNET TRAFFIC MADE UP OF BAD BOTS **37%**

14% AMOUNT OF INTERNET TRAFFIC MADE UP OF GOOD BOTS

55% PROPORTION OF ADVANCED OR MODERATE BOT ATTACKS IN 2024

45% PROPORTION OF SIMPLE BOT ATTACKS IN 2024

44% PERCENTAGE OF ADVANCED BOT ATTACKS TARGETING APIS

55%  SURGE IN API DATA LEAKAGE & API VIOLATIONS IN 2024

25% PERCENTAGE OF BOT ATTACKS TARGETING BUSINESS

19% PERCENTAGE OF ACCOUNT TAKEOVER ATTACKS TARGETING APIS

6


2025 Imperva Bad Bot Report
#2025BadBotReport
46%
PERCENTAGE OF BOT ATTACKS USING CHROME TO APPEAR AS LEGITIMATE TRAFFIC
14%
****
PERCENTAGE OF ALL LOGINS THAT WERE ACCOUNT TAKEOVER ATTEMPTS
31%
PERCENTAGE OF ATTACKS THAT WERE OWASP AUTOMATED THREATS
AI
2 MILLION
DAILY AVERAGE NUMBER OF AI-ENABLED ATTACKS
27%
PERCENTAGE OF BOT ATTACKS TARGETING THE TRAVEL INDUSTRY IN 2024
13 TRILLION
NUMBER OF BOT REQUESTS BLOCKED BY IMPERVA IN 2024
40%
PERCENTAGE GROWTH OF ACCOUNT TAKEOVER ATTACKS IN 2024
7

Erhebliche geschäftliche Auswirkungen durch Bot-Traffic

Betrügerische Aktivitäten

- Diebstahl sensibler Daten
- Markenschaden (IP)
- Umsatzverlust

Wettbewerbsnachteile

- Umsatzverlust an die Konkurrenz
- Verfügbarkeits-Targeting, Unterbieten von Preisen und Werbeaktionen
- Niedrigere Suchmaschinen-Rankings

Dienstunterbrechungen

- Anwendungs-Verlangsamungen und hohe Ausfallzeiten
- Schlechte Kundenerfahrung (Reputation)
- Markenschaden und Kundenabwanderung

Betriebsüberwachung und Abweichungen

- Bots verfälschen Key Performance Indicators (KPIs)
- Blindflug – man kann nicht verwalten, was man nicht sieht
- Fehlgeleitete Geschäftsentscheidungen und schlecht zugewiesene Budgets

Thales CSP - Application Security Services

Umfassender, zentral verwalteter Schutz, egal wo die Anwendung läuft.

DDoS

Maximieren Sie die Netzwerk- und Anwendungsverfügbarkeit mit einer schnellen Reaktion auf Netzwerk- und L7-DDoS-Angriffe.

WAF

Schützt Anwendungen direkt einsatzbereit mit nahezu null Fehlalarmen.

Client-Side Protection

Verhindern Sie Datendiebstahl durch clientseitige Angriffe wie Formjacking, digitales Skimming und Magecart.

Secure CDN

Content-Caching, Lastenausgleich und Failover zur sicheren Bereitstellung von Anwendungen weltweit.

API Security

Runtime Protection

Ständige Zero-Trust-Sicherheit für Anwendungen.

Secure DNS

DNS-Management und DNS-Schutz für die DNS-Zonen der Kunden. Bereitstellung erweiterter Funktionen wie GLB und Geofencing.

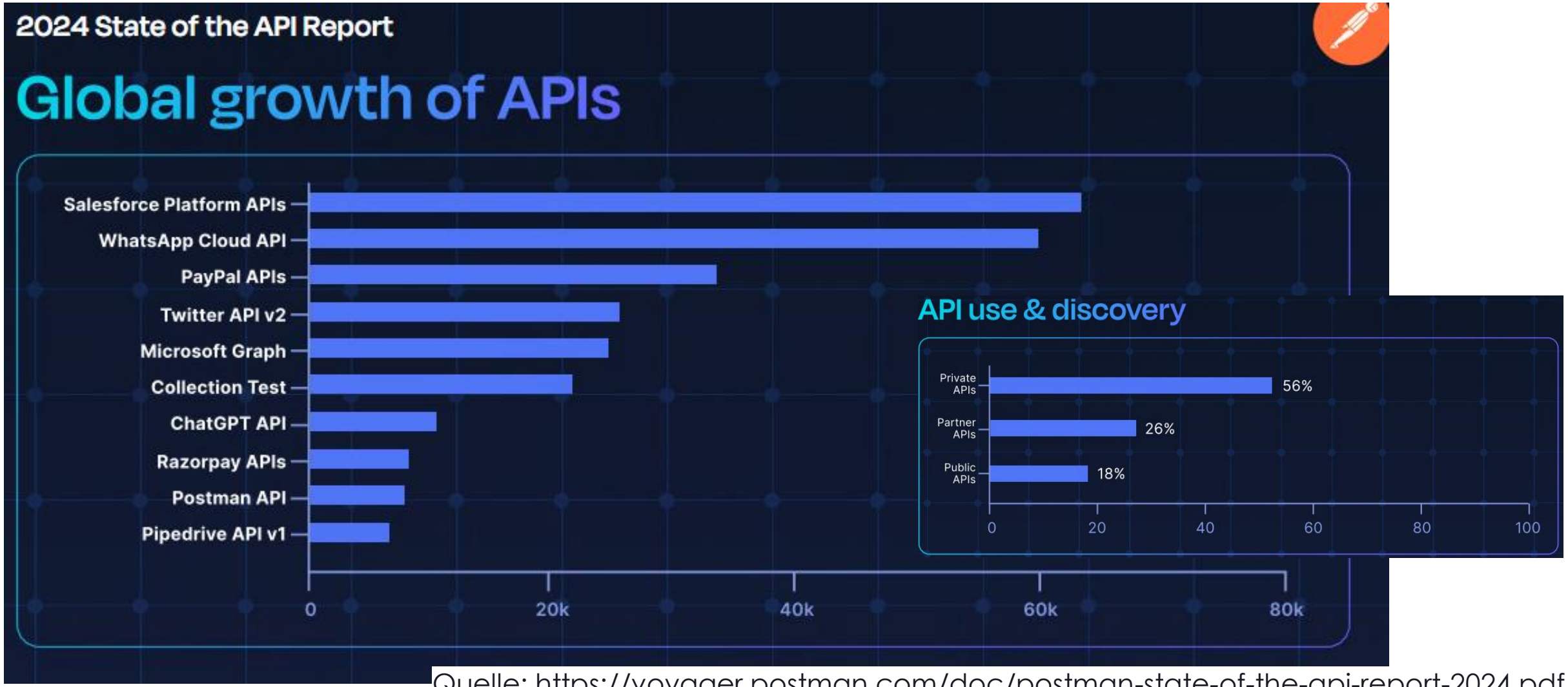
Bot Protection

Schützen Sie Websites, mobile Apps und APIs vor automatisierten Angriffen.

Account Takeover

Schützt vor automatisiertem Kontoübernahmebetrug.

Es gibt immer mehr APIs: Postman State of the API Report



Quelle: https://voyager.postman.com/doc/postman-state-of-the-api-report-2024.pdf

API Security Challenges

Lack of Visibility

Unreliable API Inventory

New & Changing APIs

Sensitive Data Loss

Bad Bots are Coming for APIs

Highly lucrative targets

API requests do not go through the traditional route of browsers or native app agents, providing direct access to the backend, including resources and functionalities.

Exposed business logic

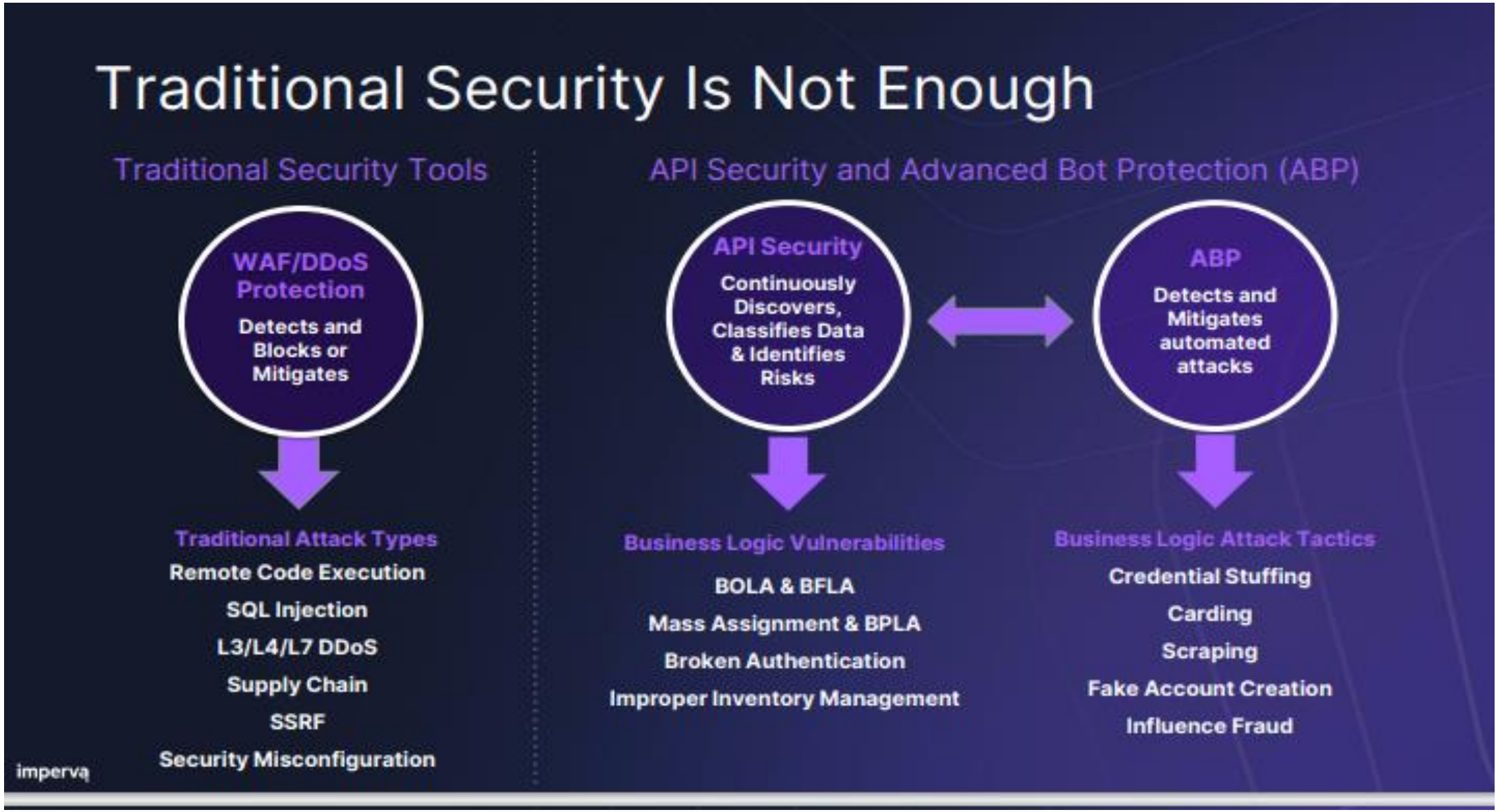
Developers use generic rulesets for APIs without keeping the business logic in mind, opening their APIs to business logic vulnerabilities that are often exploited using bots.

Lack visibility into bots

APIs handle a large volume of requests but lack built-in defense mechanisms, making it difficult to detect and block malicious bot traffic.

This enables attackers to use automation more freely without the risk of raising any alarms. The process of attacking is also easier, because APIs do not require browser automation software.


Bad Bots are Coming for APIs
Account Takeover
Data scraping
Credit card fraud
Vulnerability scanning
API

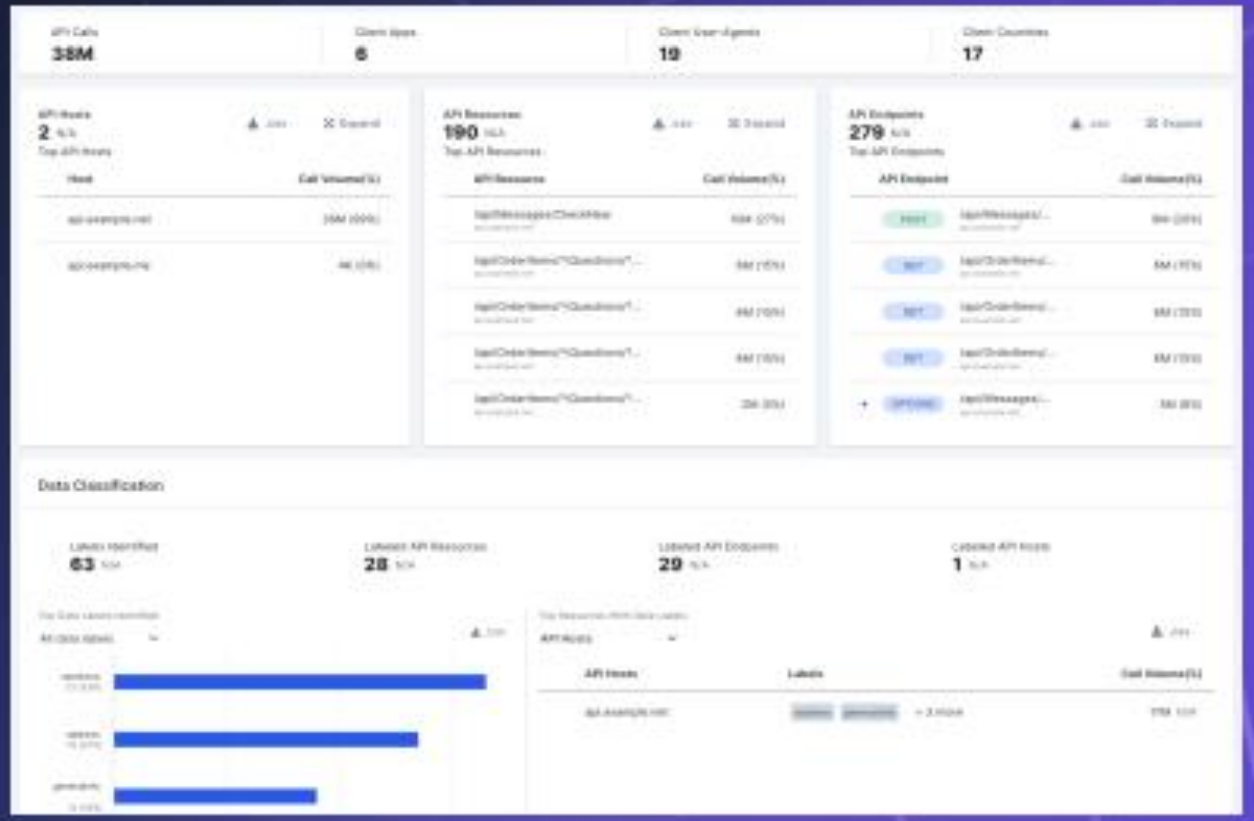

Traditional Security Is Not Enough
Traditional Security Tools
API Security and Advanced Bot Protection (ABP)
WAF/DDoS Protection
Detects and Blocks or Mitigates
API Security
Continuously Discovers, Classifies Data & Identifies Risks
ABP
Detects and Mitigates automated attacks
Traditional Attack Types
Remote Code Execution
SQL Injection
L3/L4/L7 DDoS
Supply Chain
SSRF
Security Misconfiguration
Business Logic Vulnerabilities
BOLA & BFLA
Mass Assignment & BPLA
Broken Authentication
Improper Inventory Management
Business Logic Attack Tactics
Credential Stuffing
Carding
Scraping
Fake Account Creation
Influence Fraud
imperva

API Security Starts with Discovery

Know where every API is in your infrastructure

API Discovery and Classification

1. Automatically discovers all API endpoints
2. Classifies APIs by sensitive data
3. Baseline acceptable API use

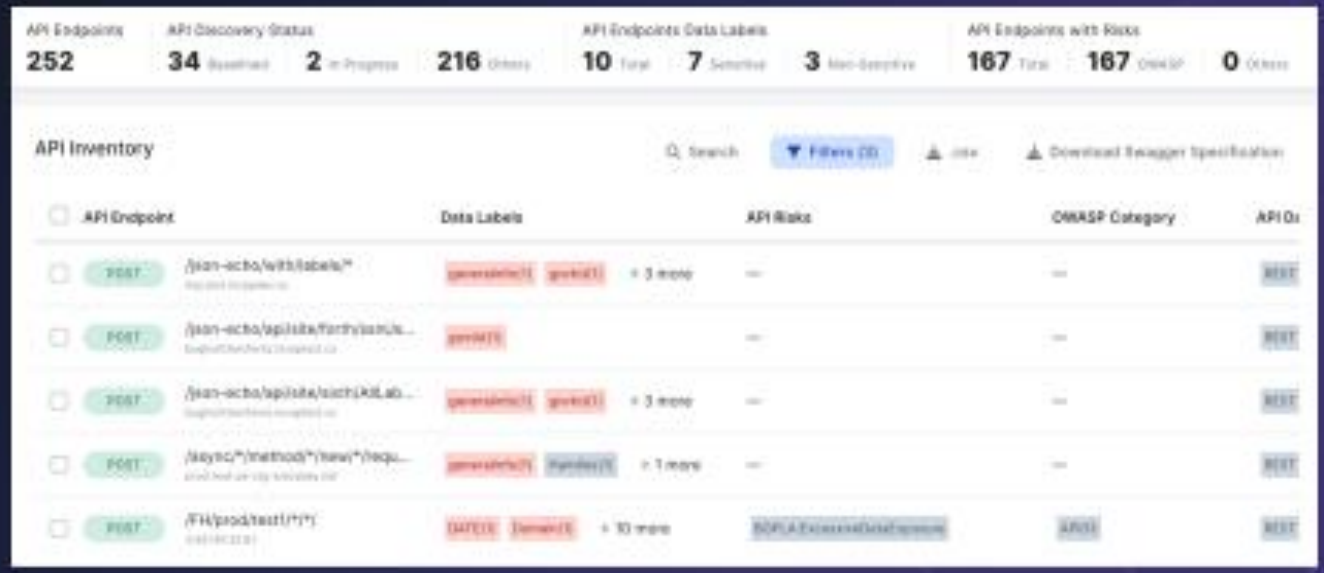


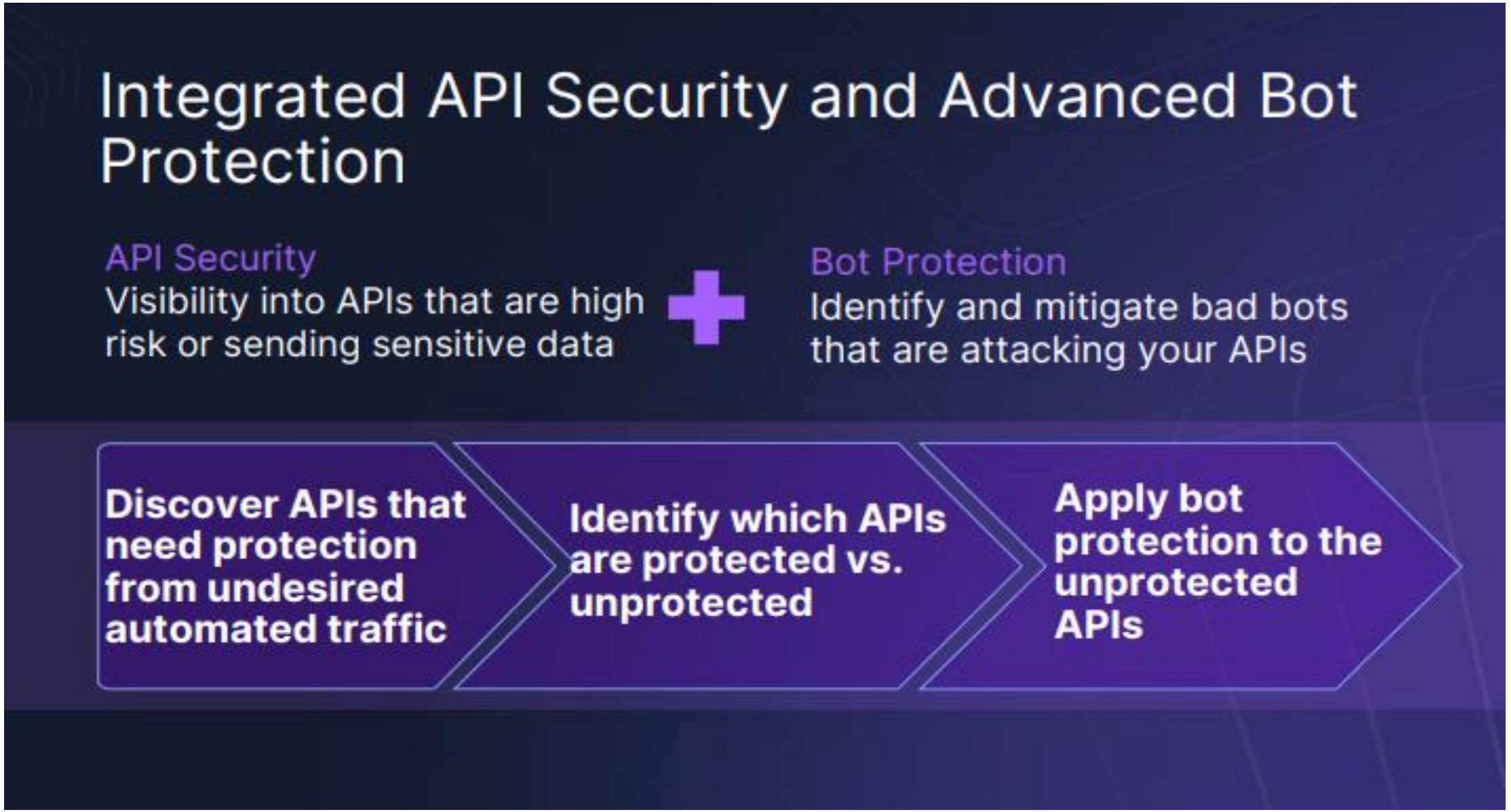
Identify API Vulnerabilities

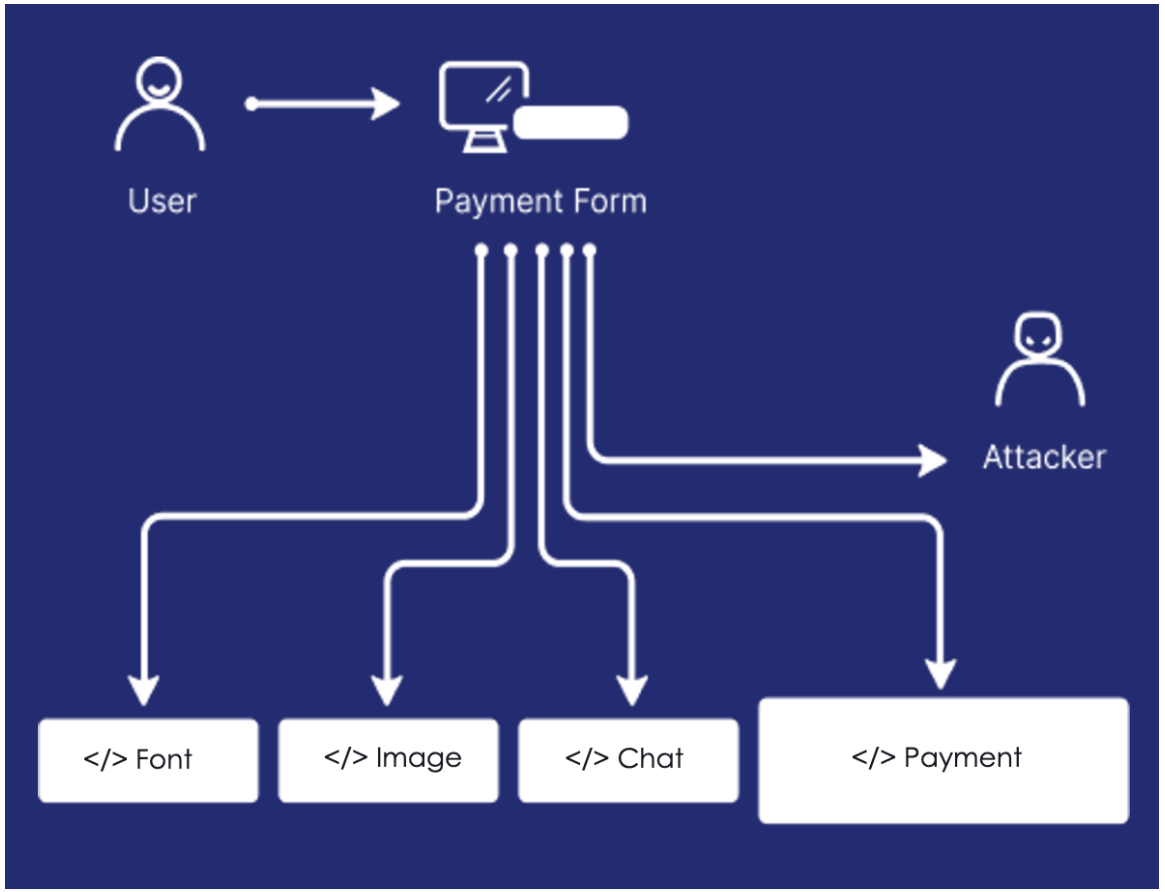
Uncovering design and implementation flaws

Detecting weaknesses that could expose APIs to abuse

1. Automatically detects and uncovers API design flaws
2. Continuous Baseline of Normal versus Abnormal patterns




Integrated API Security and Advanced Bot Protection
API Security
Visibility into APIs that are high risk or sending sensitive data
Bot Protection
Identify and mitigate bad bots that are attacking your APIs
Discover APIs that need protection from undesired automated traffic
Identify which APIs are protected vs. unprotected
Apply bot protection to the unprotected APIs



Client Side Protection

Ziel:
Schutz vor Bedrohungen, die im Browser des Benutzers stattfinden, vor allem durch JavaScript-Supply-Chain-Angriffe (z. B. Magecart, Formjacking)

Eingesetzt:
Während die Webanwendung im Browser läuft – besonders wenn sie Drittanbieter-Skripte verwendet (z. B. Zahlungsdienste, Analyse, Chat-Widgets).

Funktion:

- **Überwacht alle clientseitig eingebundenen JavaScript-Dateien**
- **Warnt bei Änderungen an Skripten oder verdächtigem Verhalten**
- **Bietet Sichtbarkeit, wer welche Daten im Browser verarbeitet**

Beispiel:
Ein eingebettetes Drittanbieter-Skript wird kompromittiert und versucht, Kreditkartendaten beim Checkout zu stehlen → Imperva erkennt den Vorfall, alarmiert und kann die Ausführung unterbinden.

THALES
Building a future we can all trust

Thank you

cpl.thalesgroup.com

THALES
Building a future we can all trust

Partner
CONNECT

Cloud-WAF als Basis für Cross- und Upselling – Teil 1

Kattia Wiemann
EAM Application Security

Kurzprofil des Kunden

> Kurze Kundenbeschreibung

- **Handelsunternehmen aus NRW.**
- Geschäftsfelder: Energie, Agrarerzeugnisse, Tierhaltung und Pflanzenzucht
- über **83 Millionen Kunden** in mehr als **70 Ländern**

> Kennzahlen

- 7000 Mitarbeiter
- 10 Haupstandorte, 400 Niederlassungen
- ca. **8.5 Milliarden** EUR Jahresumsatz

Kundenprojekt in Kurzform

> Digitale Transformation

- **Modernisierung** der Applikationslandschaft
- **Cloud 1st**

> Herausforderung

- **Einarbeitung** in neue Funktionen der CWAF
- **Verständnis** der erweiterten Sichtbarkeit
- **Überwachung** von Sicherheitsereignissen
- **Umsetzung** gezielter Sicherheitsmaßnahmen

- **Ziel: optimaler Nutzen der neuen Lösung!**

Herangehensweise

> Wie sind wir ins Projekt eingestiegen

- **Begleitung** bei der **Migration**
- **Einführung** in neue Sicherheitsfunktionen
- **Health-Check** und **Review**: **Anstieg des API-Traffics!**
- **→POV für API-Security**

> Warum hat der Kunde uns ausgewählt?

- **Nahtlose CWAF-Integration** in die bestehende on-prem WAF
- **Vertraute Tools & Workflows**
- **Integrierte Plattform –** (WAF, DDoS-, **API-,** Client-Side- sowie Advanced Bot-Protection)
- **Modular und skalierbar**
- **Zukunftssicherheit -** kontinuierliche Innovation

Lösung und Kundennutzen

> Welches AppSec-Portfolio kam zum Einsatz

- **CWAF-Bundle** (App Protect Professional) **+ API Security Modul**
- Gesamtvolumen: **300K**

> Kundennutzen

- **Flexible Skalierung** ohne zusätzliche Hardware
- **weniger Verwaltungsaufwand**
- **Moderne Schutzfunktionen**: API-Schutz, Client-side Protection, Bot- & KI-basierte Bedrohungserkennung
- **Globale Performance:** Weniger Latenz durch weltweit verteilte Rechenzentren

> Zusätzlicher Nutzen

- IT-Security erhält **volle Visibilität im API-Verkehr**
- → **heute Zusammenarbeit mit API-Team** zur Einhaltung von Sicherheitsstandards

THALES
Building a future we can all trust

Partner CONNECT

Reifegraderhöhung in der Informationssicherheit

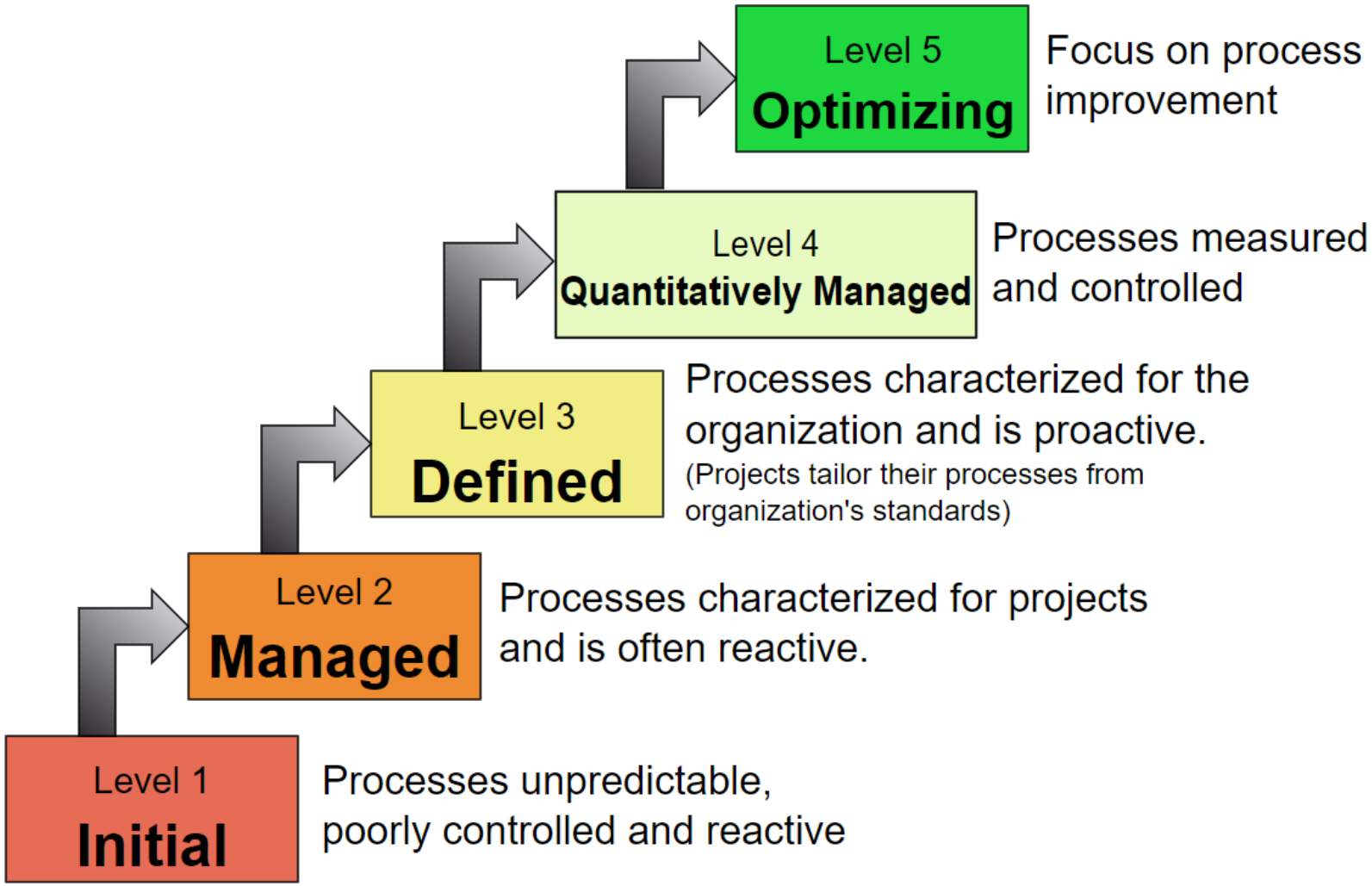
Martin Gegenleitner
PreSales Consultant,
DataSec

www.thalesgroup.com

WARUM SPRECHEN WIR ÜBER REIFEGRADE?

Weil wir keine “Low-Hanging-Fruits”, sondern eine Steigerung der Resilienz adressieren.

Theorie zum Reifegrad nach CMMI



Beispiele für zu bewertende Prozesse

Schwachstellen-Management

* Security Posture Management

Strategie & Richtlinien

Kryptographie

Log-Management & Monitoring

Physical Security (& Safety)

JEDER PROZESS HAT SEINE RISIKEN

Wir sind in den meisten Fällen die “Second Line of Defence”.
Hat deshalb ein Prozess noch keine Grundreife,
sind wir wahrscheinlich noch zu früh dran.

Risiko-Management-Prozess

1

Zusammenhänge definieren

Abgrenzung/Scoping (Standorte, System, Geschäftsprozesse)

Rahmenbedingungen (technisch, finanziell, gesetzlich, kulturell, …)

Tragbare/untragbare Risikoen

2

Risiken identifizieren

Werte (Assets)

Bedrohungen (Threats)

Schwachstellen (Vulnerabilities)

3

Risiken abschätzen

Qualitativ

Quantitativ

Risiko-Management-Prozess

4

Risiken bewerten

Soll ein Risiko behandelt werden?

Prioritäten setzen

5

Risiken behandeln

Risikovermeidung

Risikoverminderung

Risikotransfer

Risikoakzeptanz

6

Risiken akzeptieren

Risiko liegt unter gegebenem Wert

ODER

Behandlung nicht möglich/sinnvoll

Managemententscheidung

Beispiel Post-Quanten-Kryptographie

> Welche Unternehmen nehmen das Thema als zu behandelndes Risiko wahr?

- Großindustrie?
- Startups?
- KMUs?
- Behörden und andere Gov-Orgas?

> Warum kann es ein Thema sein?

- Regulative Anforderungen an Vertraulichkeit von Informationen (DSGVO)
- Schutz von Intellectual Property vor Wirtschaftsspionage
- Langlebige OT/IoT-Geräte im Feld (Satelliten, Offshore-Windkraft, …)

Beispiel Souveränität

> Welche Organisationen müssen darauf achten?

- Staatliche Einrichtungen
- Startups?
- Industrie?

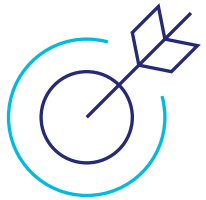
> Warum sollte darauf geachtet werden?

- Reduktion von externen Abhängigkeiten zur Erbringung meiner Geschäftsprozesse!
- Kernfrage: Wem kann ich vertrauen?

Gemeinsamkeit der Beispiele: ähnliche Risikobewertung

Threat

Impact



Likelihood

WIE WIRD DAS THEMA POLITISCH THEMATISIERT?

NIS-2, DORA & CRA

TEASER

Wir konkretisieren das gleich nach der Pause

anhand des Beispiels DevSecOps!

THALES
Building a future we can all trust

Martin Gegenleitner

Presales Consultant

+43 660 82 62 166

martin.gegenleitner@thalesgroup.com

THALES
Building a future we can all trust

Partner
CONNECT

DevSecOps-Relevanz nimmt massiv zu. Was kann man tun?

Martin Gegenleitner
Julian Iavarione
Senior Sales Engineer AppSec
www.thalesgroup.com

„Sicherheitsrisiken verlangsamen Innovation und verlängern die Time-to-Market.

„Sicherheitsengpässe in CI/CD-Pipelines **verlangsamen die Bereitstellung** und beeinträchtigen die Entwicklungsagilität.“

„Die Skalierung der Sicherheit für APIs und Microservices ist komplex und schränkt die Fähigkeit ein, mit schnellem Wachstum Schritt zu halten.“

„Abstimmung zentraler Sicherheitsanforderungen mit den Unternehmenszielen“

Resiliente Sicherheit

- **Governance** stärken, um Resilienz aufzubauen – ohne Tempoverlust
- Sicherheit nahtlos in Entwicklungsprozesse integrieren, um Agilität zu steigern

Schnelle Entwicklung

- Beschleunigte Entwicklung durch eine **optimierte, automatisierte Web Application Firewall (WAF)**
- DevOps befähigen, sichere und hochwertige Anwendungen **ohne Engpässe** bereitzustellen

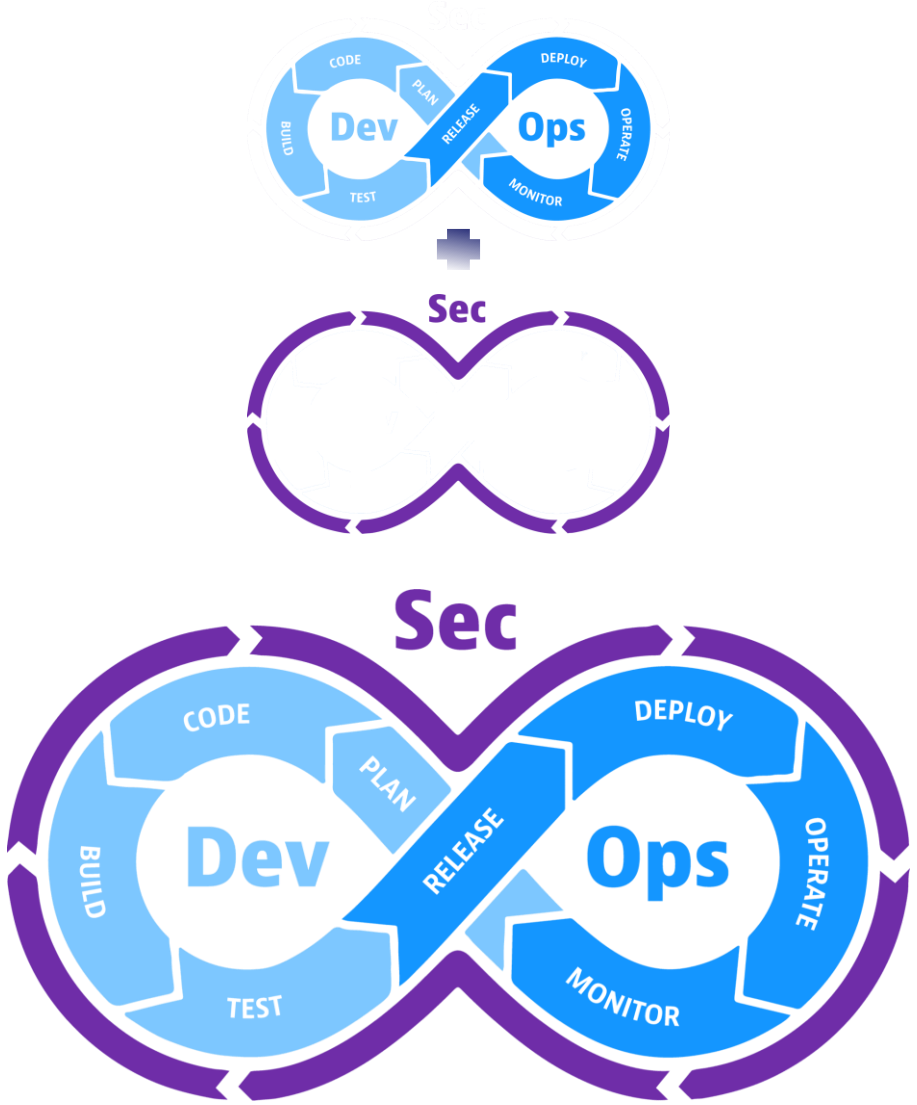
Was bedeutet DevSecOps?

> Sichere Weiterentwicklung und Bereitstellung von Anwendungen

- Secure Software Design
- Secure Coding
- Software Engineering
- Software Testing
- …

> Personas aus unterschiedlichen Disziplienen

- **Devs:** APIs, Features, Sprints
- **Ops:** Ansible, Kubernetes
- **Sec:** Risiken, Angriffsvektoren, Resilienz
- **Produkt-Owner**: Budgets, Resourcen

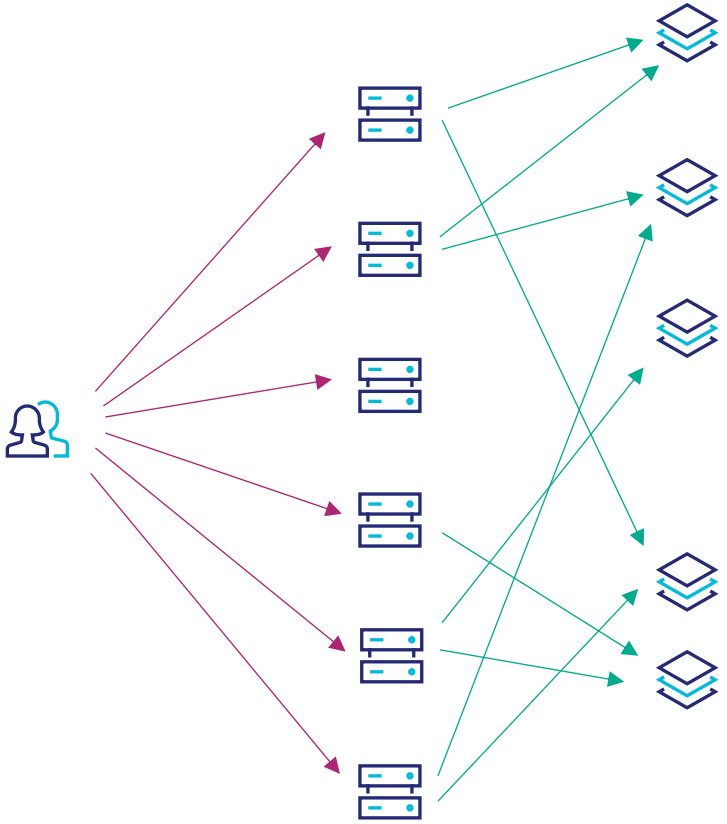


WIE KÖNNEN WIR DEVSECOPS-TEAMS UNTERSTÜTZEN?

Bei einer Make-or-Buy-Entscheidung muss unsere Buy-Option besser sein – also schneller, effektiver, günstiger!

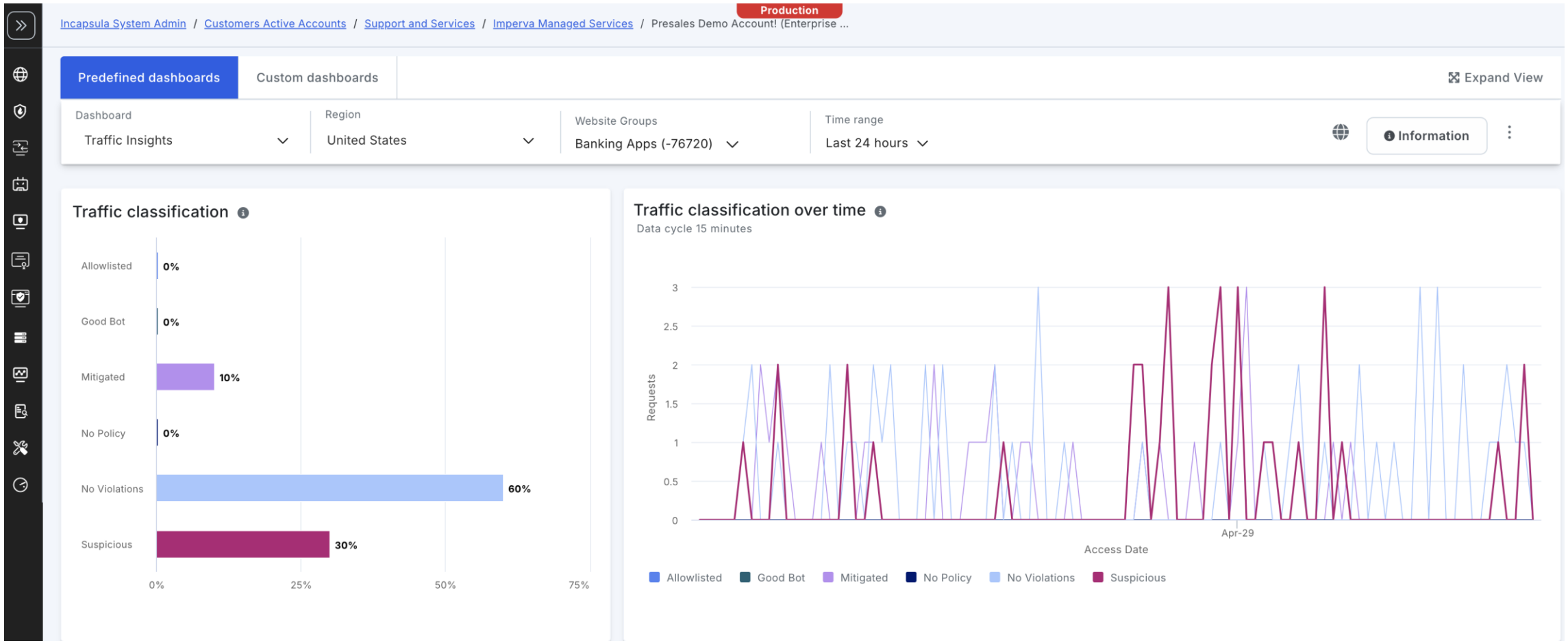
Wir treten als Enabler auf!

Evolution von Applikationen



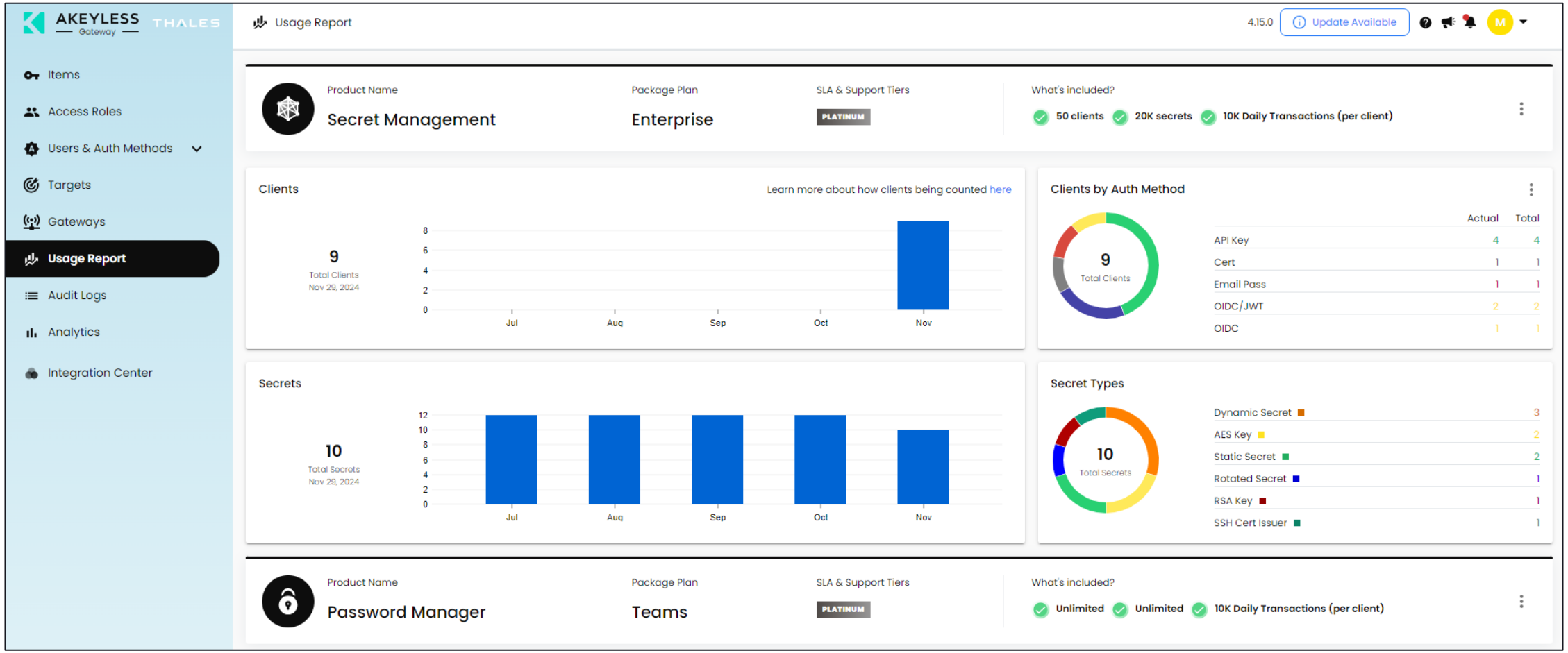
Beispiel KI-verstärkte Bots

> Will ich Anti-Bot-Maßnahmen selber bauen oder lass ich den Datentraffic extern vorfiltern?



Beispiel Automatisierung und dynamische Umgebungen

> Kann ich mir es leisten Zugangsdaten/Secrets/Credentials/Token/Zertifikate noch manuell zu verwalten?



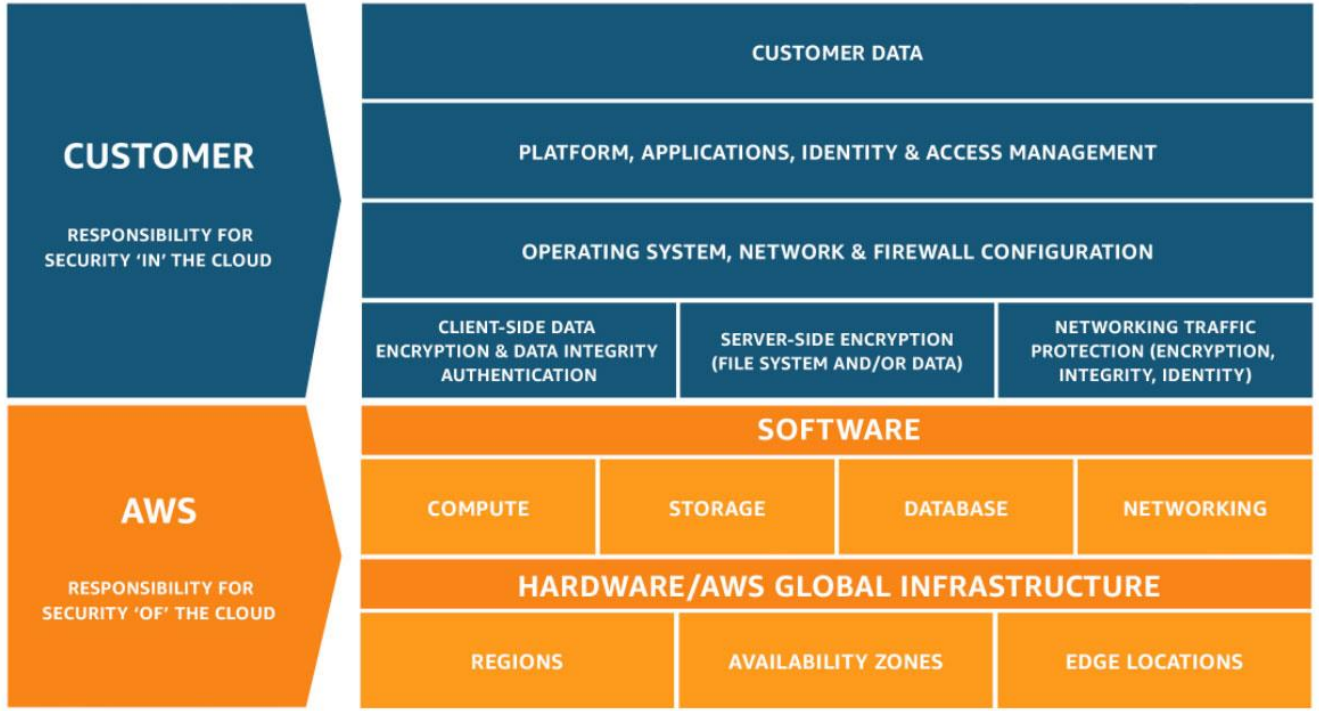
Beispiel Datenhoheit in Multi-Cloud-Umgebungen

> Will/Darf ich mich auf Cloud-Provider verlassen?

> Will ich mich um die Verschlüsselung und deren zusätzliche Risiken selbst kümmern?

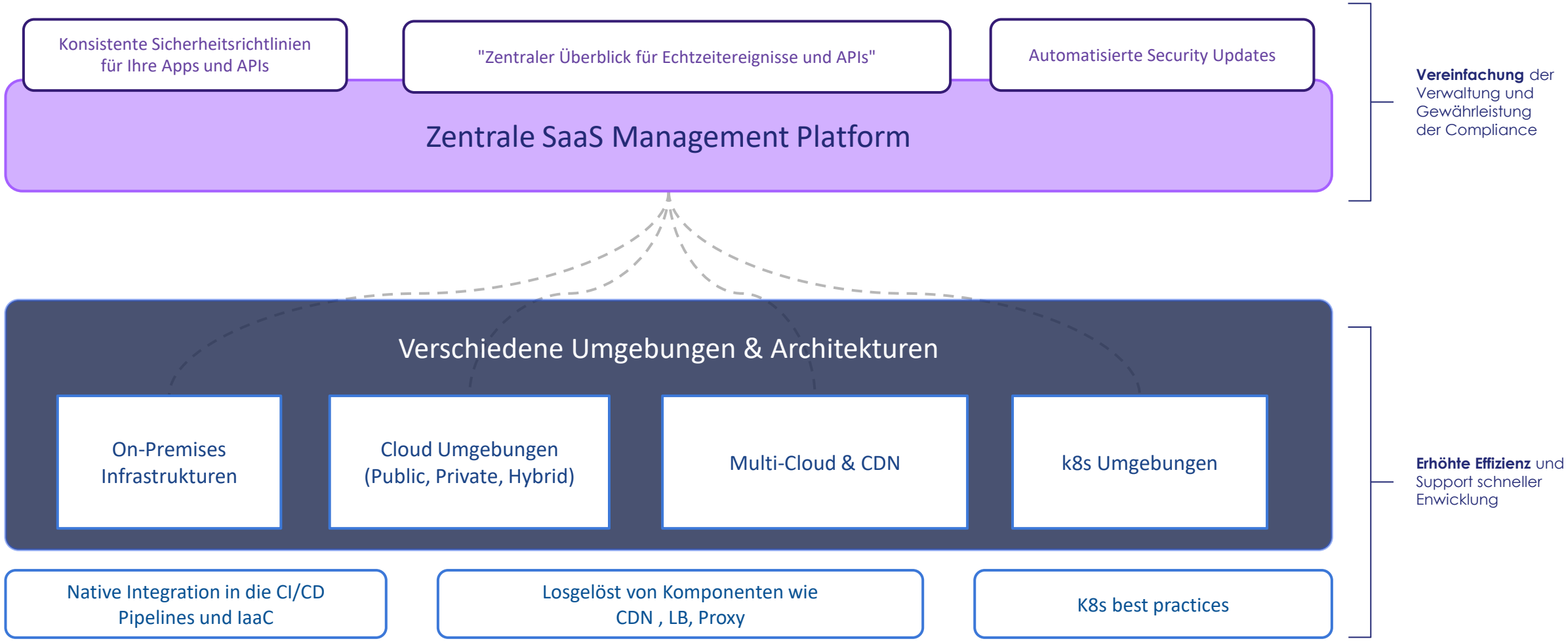
- Key-Rotation
- Integration
- Desaster-Recovery-Prozeduren
- Zukunftssicherheit

> Will ich selbst die Datenzugriffe automatisiert erfassen und interpretieren?



Beispiel MultiCloud-Kontrolle

> Wie viel ist es wert auf einen Blick alle Risiken aller Umgebungen auf einem Dashboard zu haben?



GEMEINSAMKEIT ALLER BEISPIELE

Es handelt sich nicht um Einsteigerthemen!

THALES
Building a future we can all trust

Contact

Julian Iavarone

Senior Sales Engineer

Phone number

julian.iavarone@thalesgroup.com

Martin Gegenleitner

Presales Consultant DACH

+43 660 82 62 166

martin.gegenleitner@thalesgroup.com

THALES
Building a future we can all trust

Partner CONNECT

Cloud-WAF als Basis für Cross- und Upselling – Teil 2

Kattia Wiemann
EAM Application Security

Kurzprofil des Kunden

> Kurze Kundenbeschreibung

- **Handelsunternehmen**
- Geschäftsfelder: Energie, Agrarerzeugnisse, Tierhaltung und Pflanzenzucht
- über **83 Millionen Kunden** in mehr als **70 Ländern**

> Kennzahlen

- 7000 Mitarbeiter
- 10 Haupstandorte, 400 Niederlassungen
- ca. **8.5 Milliarden** EUR Jahresumsatz

Kundenprojekt in Kurzform

> Digitale Transformation

- **Cloud 1st**

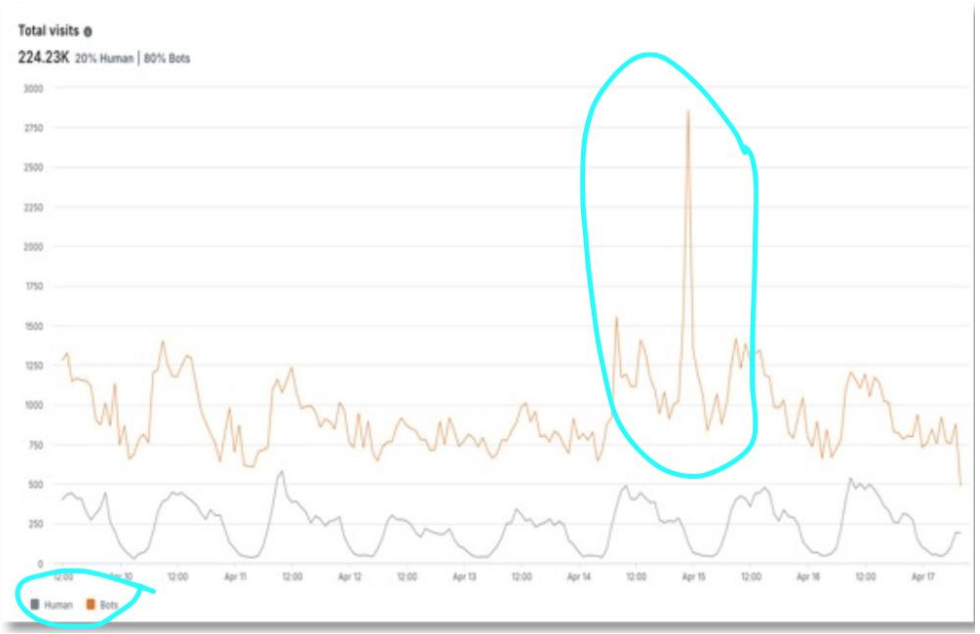
> Herausforderung

- **„Sichtbarkeit bedeutet Handlungsfähigkeit – und Verantwortung.“**
- **Ziel:** Eine **schnelle, gezielte** Reaktion auf Vorfälle.

Herangehensweise

> Wie sind wir ins Projekt eingestiegen

- **Kontinuierliche Zusammenarbeit**: vierteljährliche Reviews
- **Anomalie** : **Massiver Anstieg des Bot-Traffics**
- **Vermutung**: Mögliche gezielte Attacke
- **Maßnahme**: Proof of Value (POV) für Advanced Bot Protection



> Warum hat der Kunde uns ausgewählt?

- **Integrierte Sicherheitsplattform -** (WAF, DDoS-, API-, Client-Side- sowie **Advanced Bot Protection**)
- **Modular und skalierbar**
- **Zukunftssicher -** Kontinuierliche Innovation

Lösung und Kundennutzen

> Welches AppSec-Portfolio kam zum Einsatz

- **Advanced Bot Protection Modul**

> Kundennutzen

- **Aktiver Schutz vor hochentwickelten Bots**, die herkömmliche Schutzmaßnahmen traditioneller WAFs umgehen
- **Adaptive Verteidigung -** Passt sich dynamisch an neue Bedrohungen und Tarntechniken an
- **Echtzeit-Erkennung -** Identifiziert und blockiert fortschrittliche Bot-Angriffe sofort bei der Anfrage

> Zusätzlicher Nutzen

- **Verbesserte System-Performance** durch geringere Infrastrukturbelastung

THALES
Building a future we can all trust

Partner
CONNECT

Double Key Encrypion Use Case

Sascha Pdadenhauer
Major Account Manager
Martin Gegenleitner
www.thalesgroup.com

Kurzprofil des Kunden

> Kurze Kundenbeschreibung

- Global agierender Finanzdienstleister eines führenden Automobil Konzerns
- Bietet Mobilitäts- und Finanzlösungen wie Leasing, Finanzierung, Versicherung und Flottenmanagement für Privat- und Geschäftskunden
- Weltweit 28.5 Mio Verträge (Stand 2024)

> Ein paar Kennzahlen, z.B.

- 11.500 Mitarbeiter
- 47 Länder mit Zahlreichen Niederlassungen aktiv
- 50.8 Mrd. € Umsatz (2023)/+15.5% zum Vorjahr

Cyber Security Improvement Program

> Double Key Encryption (DKE)

- Einführung M365
- Souveränität der Daten gegenüber Service Provider

> Herausforderung

- Sensible Daten werden über M365 verarbeitet
- Schnelle Umsetzung von Board Level CIO gefordert
- Wenig Resourcen im Team

Herangehensweise

> Wie sind wir ins Projekt eingestiegen

- Wir sind schon 2023 mit dem Kunden zu DKE eingestiegen
- Bestehender Kunde im Umfeld PKI (HSM)
- Wir haben den Partner nach erfolgreichen POC eingebunden
- Die Cloud basierende Lösung CDSPaaS hat den Kunden überzeugt

> Warum hat der Kunde uns ausgewählt?

- Kunde kennt uns aus dem HSM Umfeld
- Gute bestehende Relationship
- Aufbau einer Encryption Plattform

Lösung und Kundennutzen

> Welche Lösung kam zum Einsatz

- 1x CTM aaS mit DPoD als Root of Trust mit 2x CCKM für DKE
- Produktvolumen, z.B. 180k€ Produkte für 3 Service

> Kundennutzen

- Regulatorische Anforderungen
- Sicherheit, Kontrolle Souveräntität gegenüber dem Cloud Service Provider

> Zusätzlicher Nutzen

- gestärkte Kundenbeziehung, Plattform für Ausbau weiterer Use-Cases

Balancing M365 E5 Functionality and Sovereignty Controls

Azure Native Keys

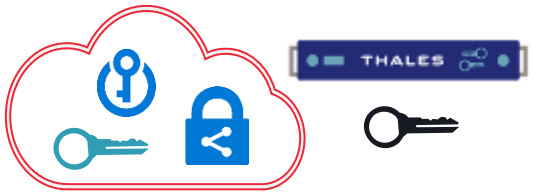
Preventing Microsoft Accessing Your Data
NO

	MS365 Functionality
Available	Search and Index
	Co-authoring
	Co-pilot
	DLP Inspection
	Delve
	eDiscovery

MPIP + BYOK/CDSP

Preventing Microsoft Accessing Your Data
Partial

	MS365 Functionality
Available	Search and Index
	Co-authoring
	Co-pilot
	DLP Inspection
	Delve
	eDiscovery

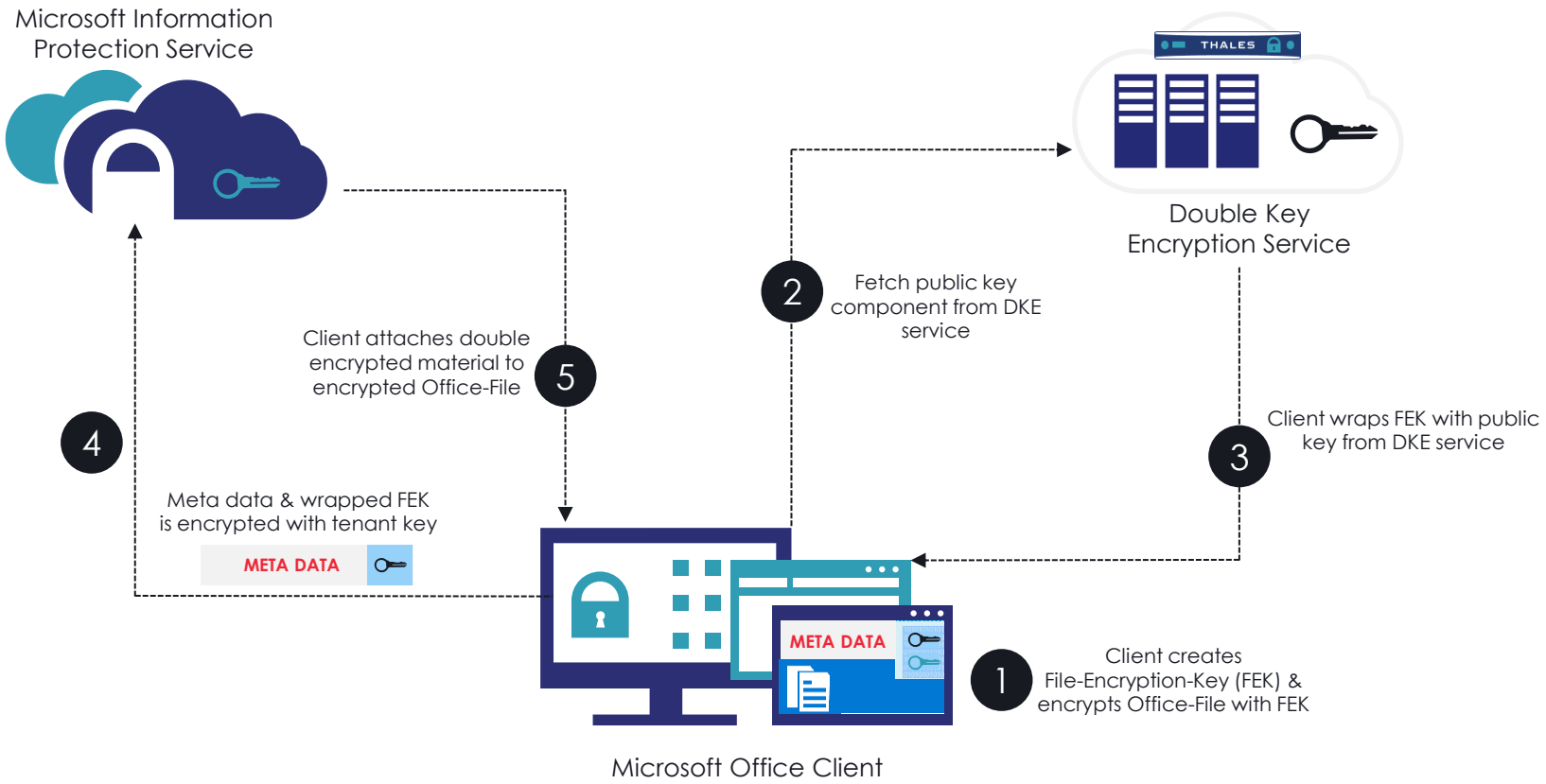


MPIP + DKE/CDSP

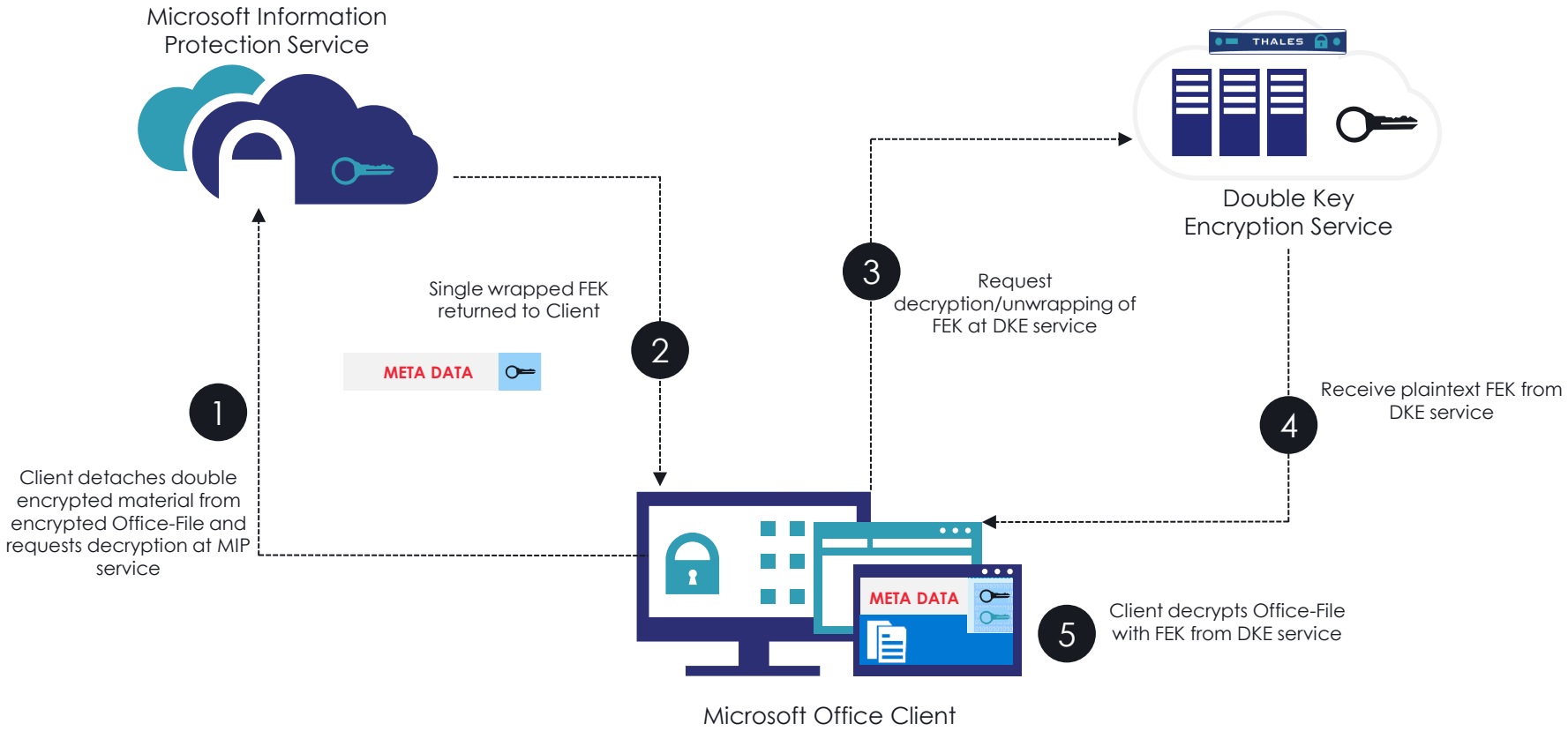
Preventing Microsoft Accessing Your Data
YES

	MS365 Functionality
Intentionally Denied	Search and Index
	Co-authoring
	Co-pilot
	DLP Inspection
	Delve
	eDiscovery

DKE Encryption Flow

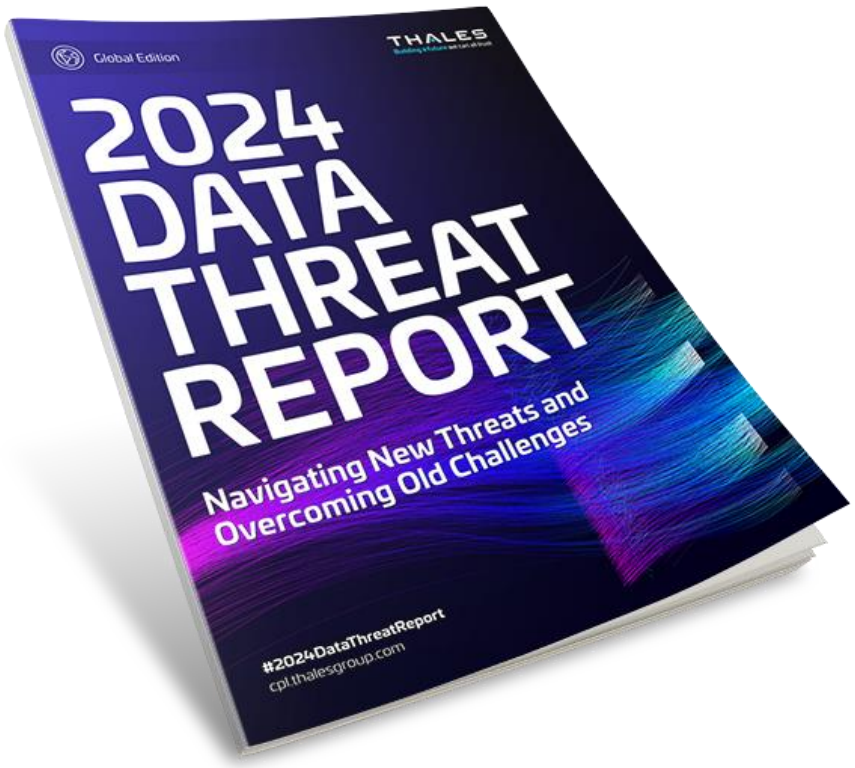


DKE Decryption Flow




THALES
Building a future we can all trust
Partner
CONNECT
The Future of Thales
Security Products
Tim Ayling
VP EMEA Cyber Specialists
www.thalesgroup.com

Compliance plays a key role in security and mitigating risk

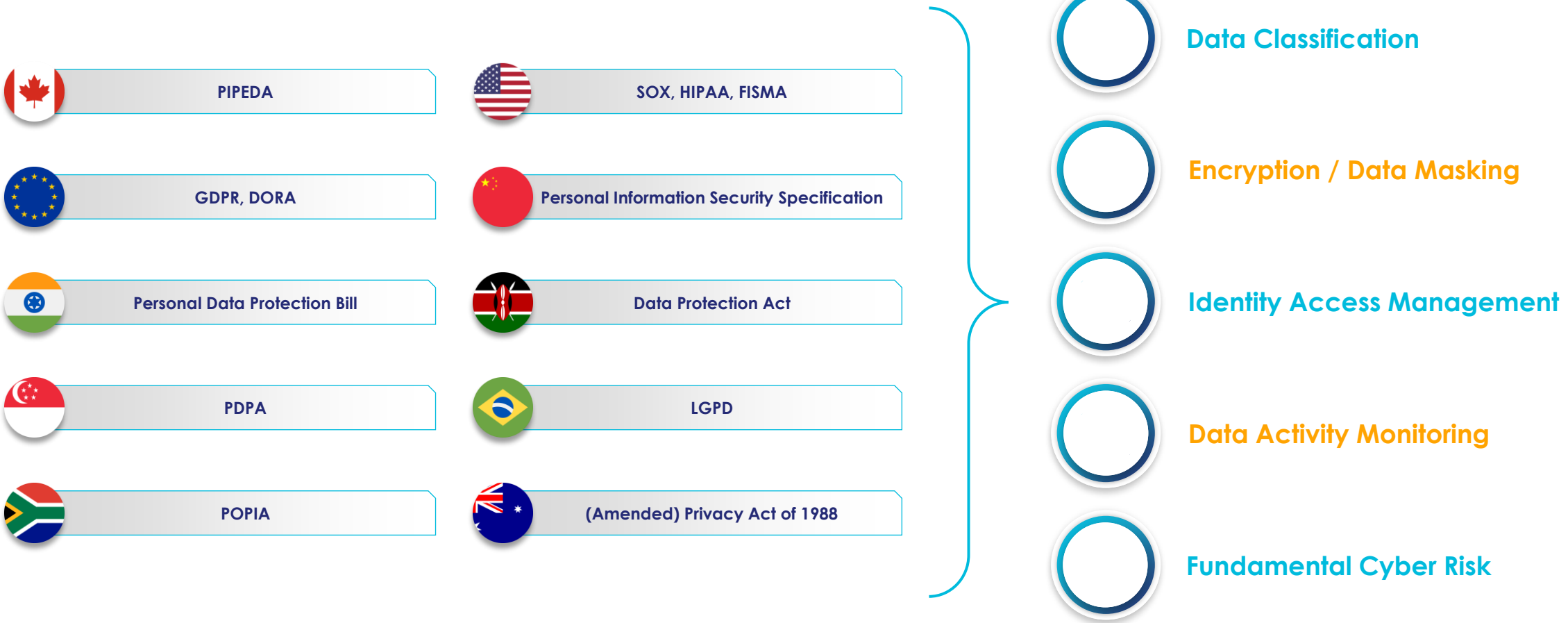


Thales 2024 Data Threat Report

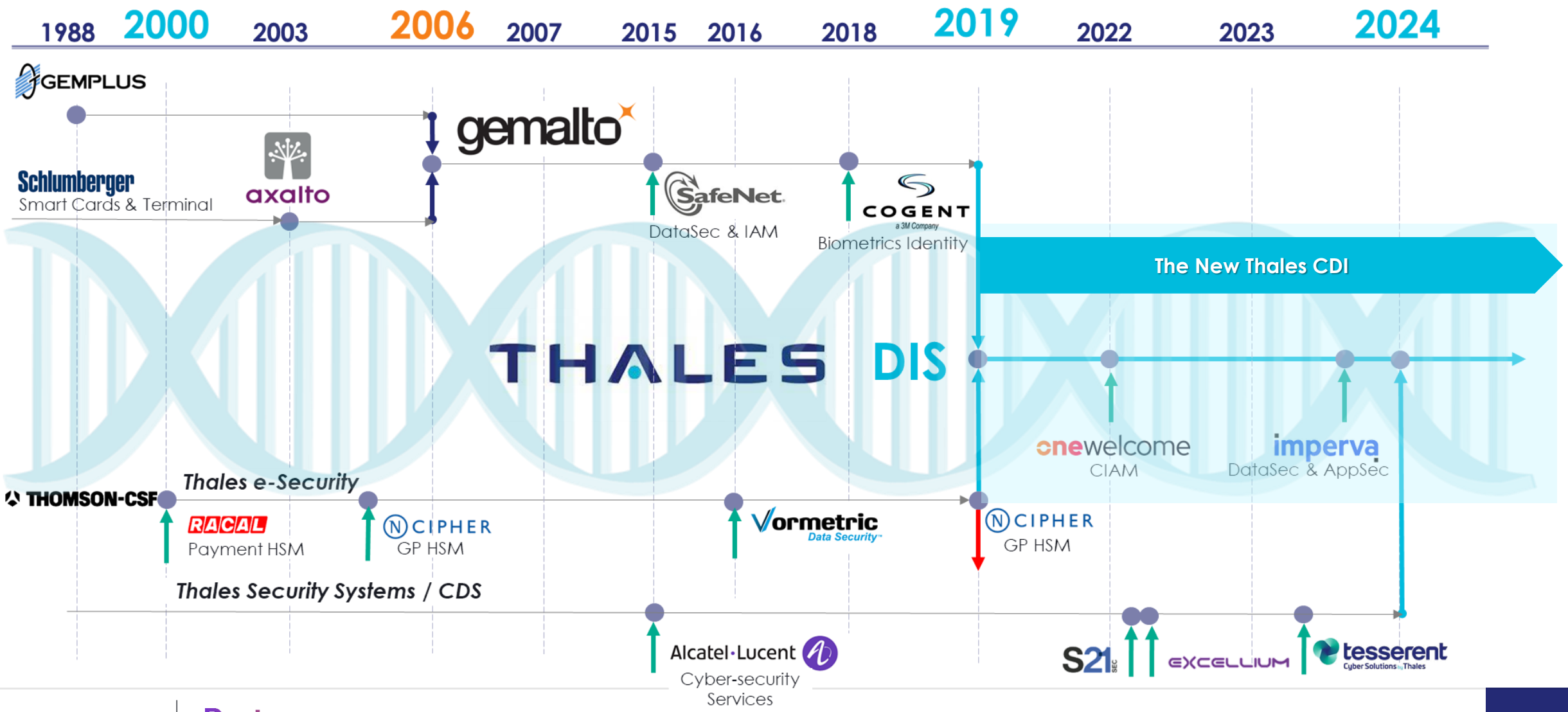
- The research found that over two-fifths **(43%)** of enterprises failed a compliance audit in the past twelve months – with the report highlighting a very clear correlation between compliance and data security
- Of those who had failed a compliance audit in the past 12 months, **31% had experienced a breach** that very same year
- This compares to just **3% of those who had passed** compliance audits

Explosion of global regulations increasing complexity of managing cyber risk and compliance

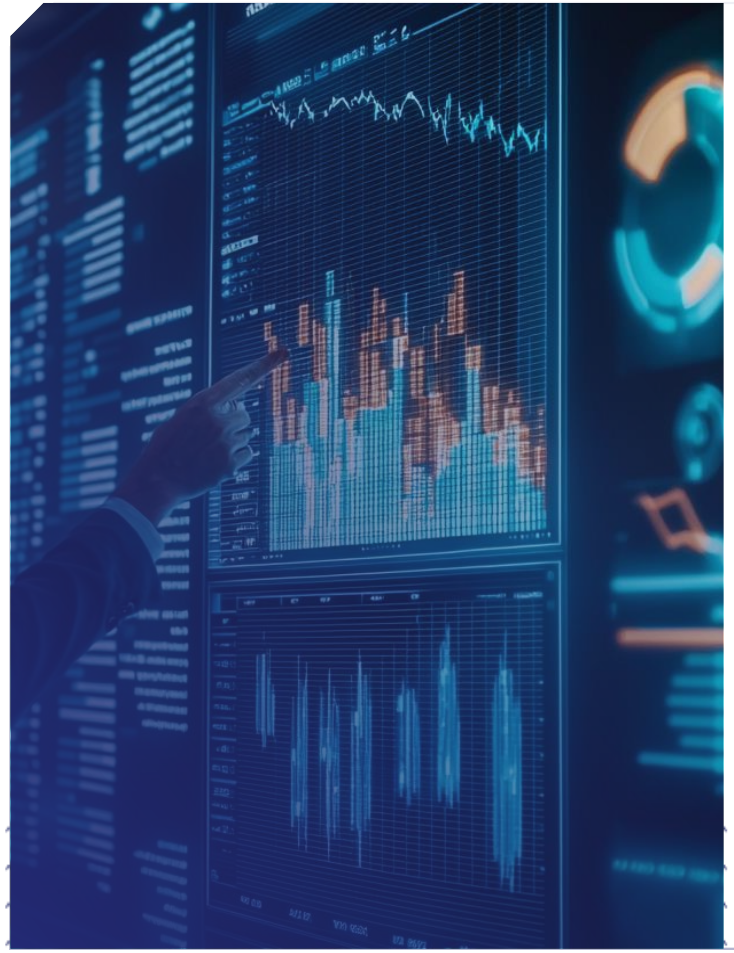
Global data regulation common denominators

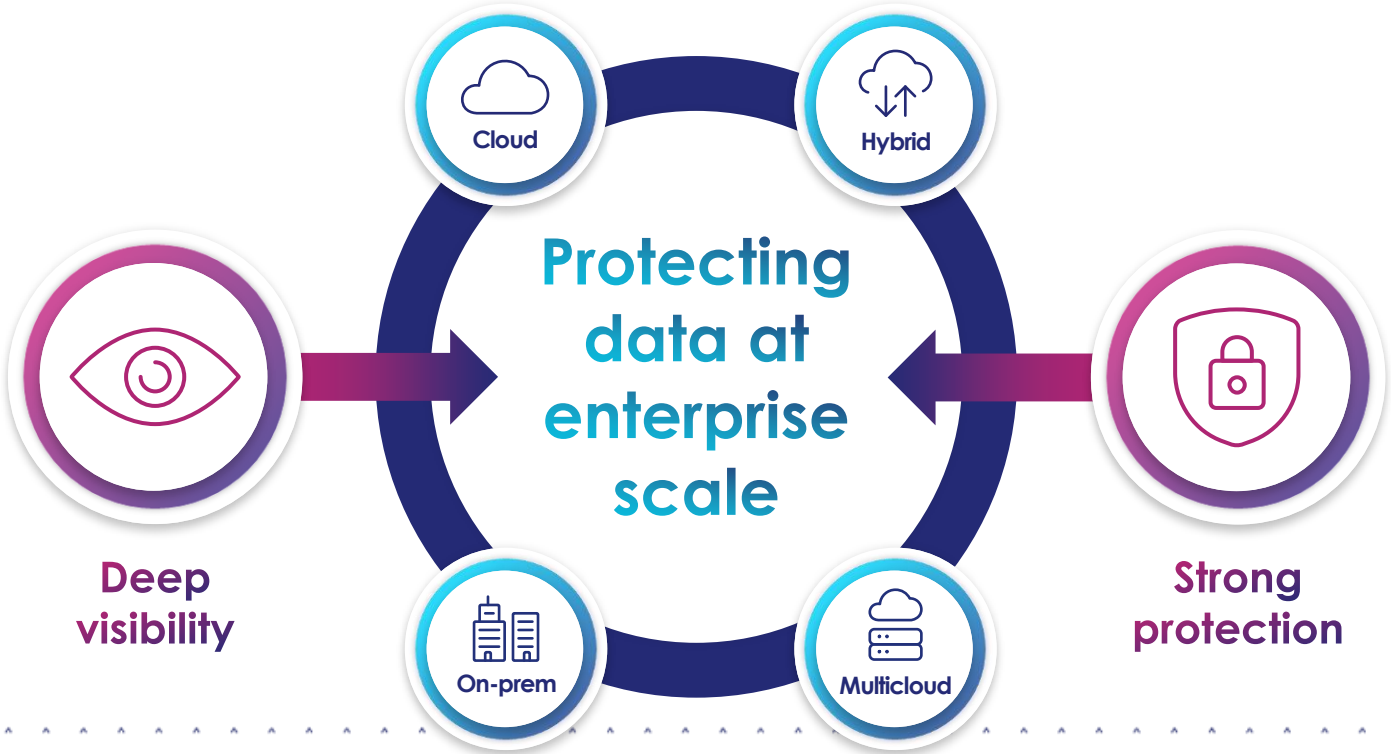


Thales has steadily invested and assembled and industry leading cybersecurity business that is stronger together

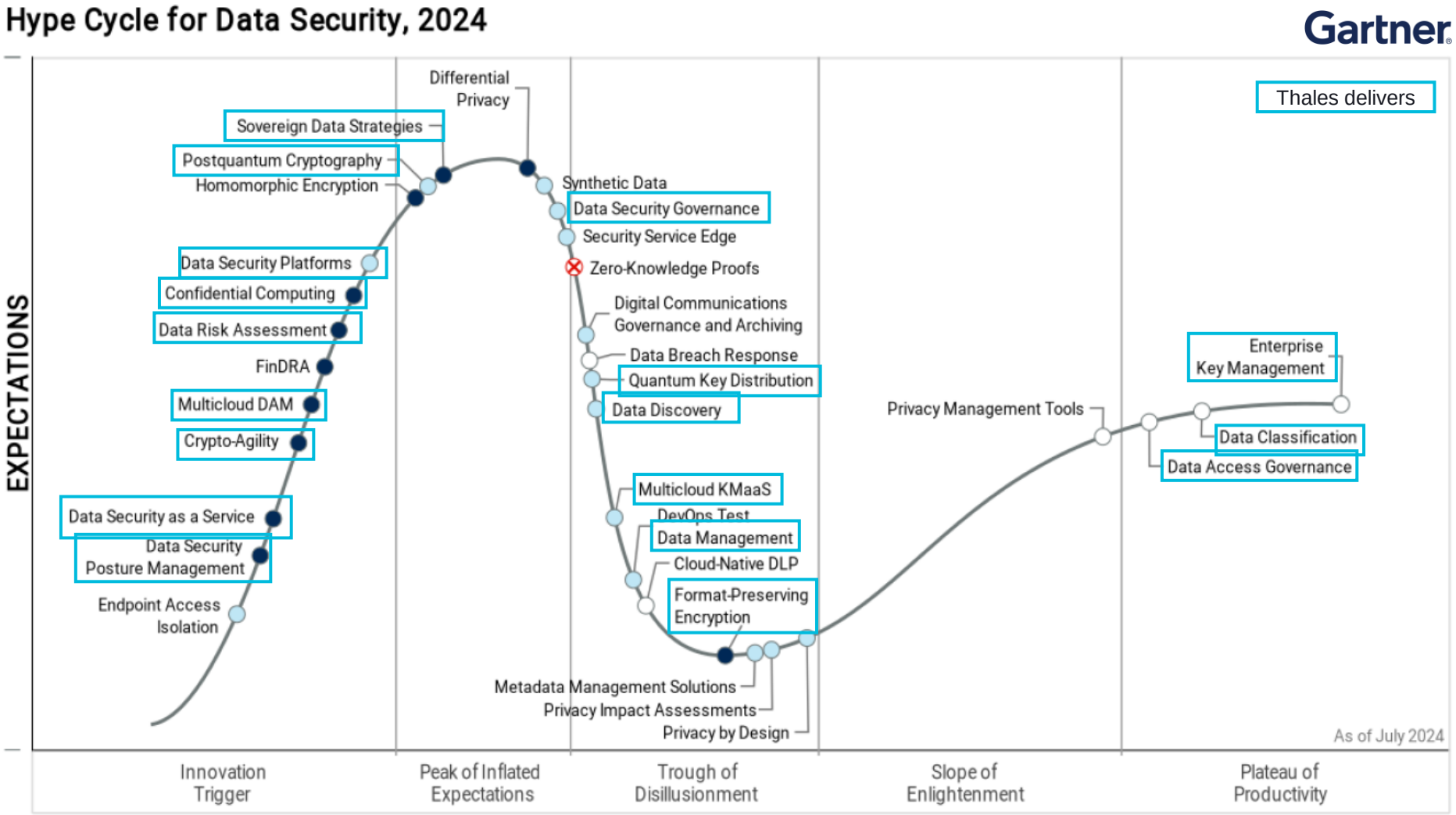


The Thales Data Security platform addresses and reduces both **compliance and breach risks**



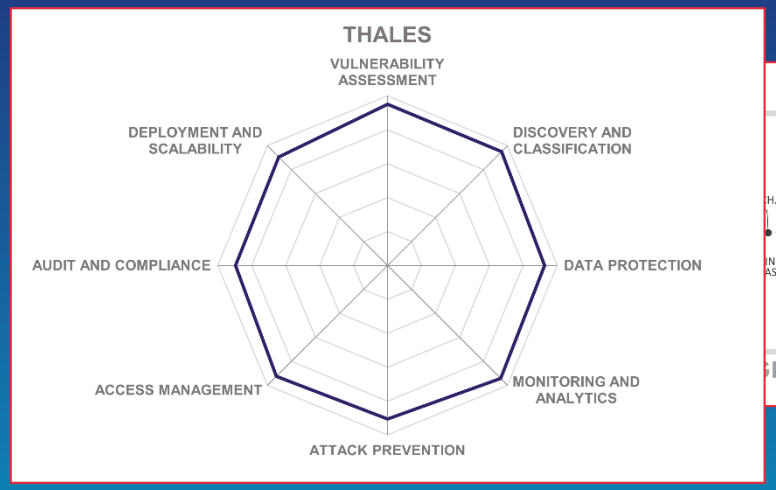


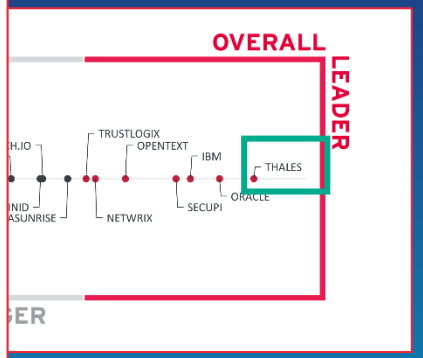
Thales leadership in Data Security

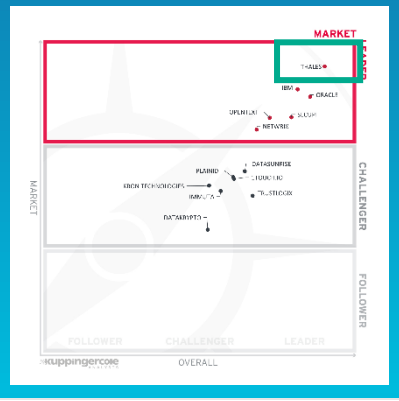


Thales Market Leadership

> KuppingerCole Data Sec Platform







Data Security Platform

> Thales Strengths

- "A comprehensive data security portfolio addressing **all aspects of data security**
- Broad coverage of databases and cloud data platforms
- Strong multi-cloud and hybrid cloud support, ensuring consistent security policies across distributed environments.
- **Advanced threat detection and automated remediation capabilities**
- Compliance-centric design, facilitating regulatory adherence for enterprises."

Source: *KuppingerCole*

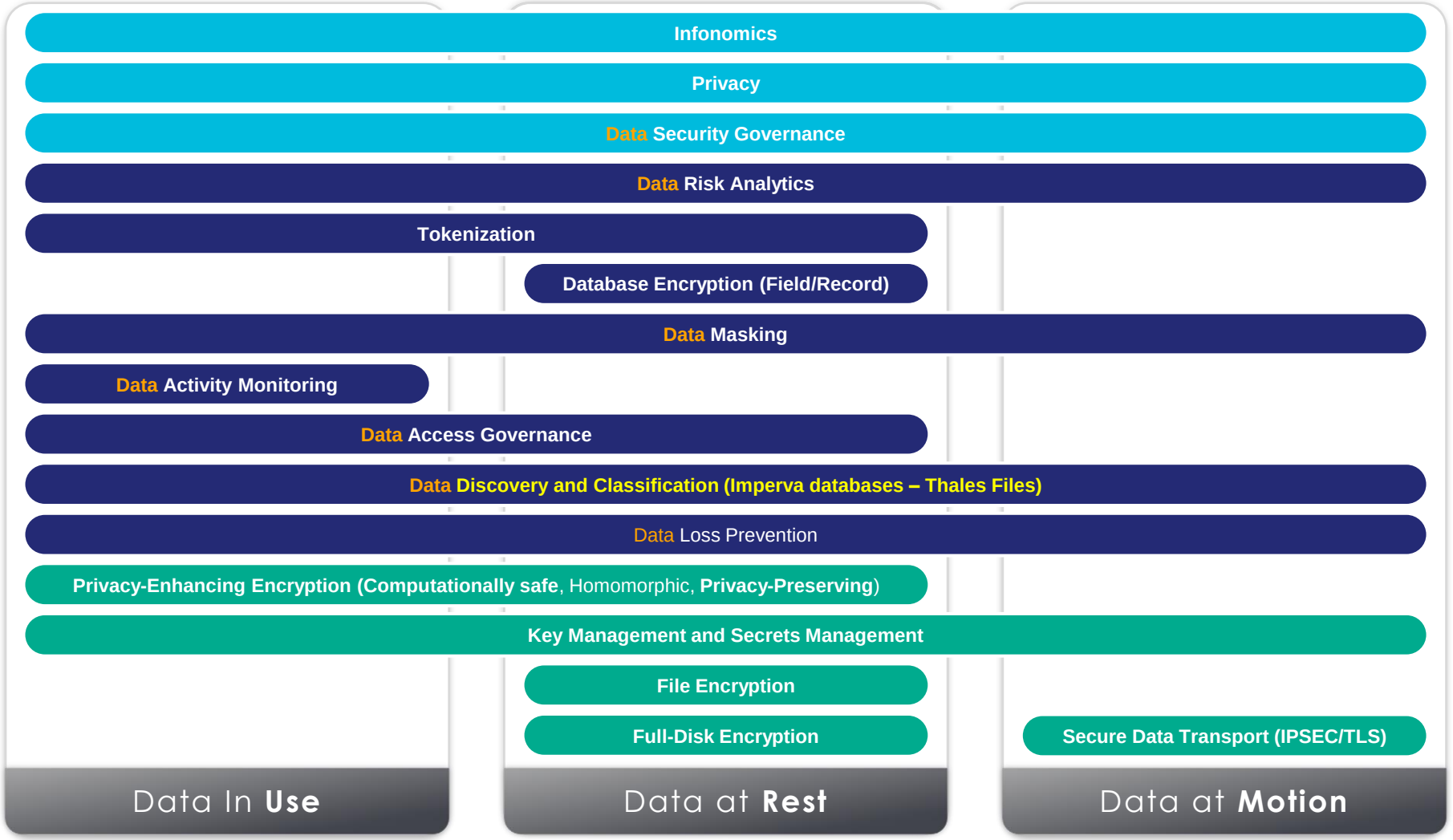
Final capability covered together – File activity monitoring and security

People and Process

Data Security Platform (DSP)

Adjunct Data Security Infrastructure

Data Types



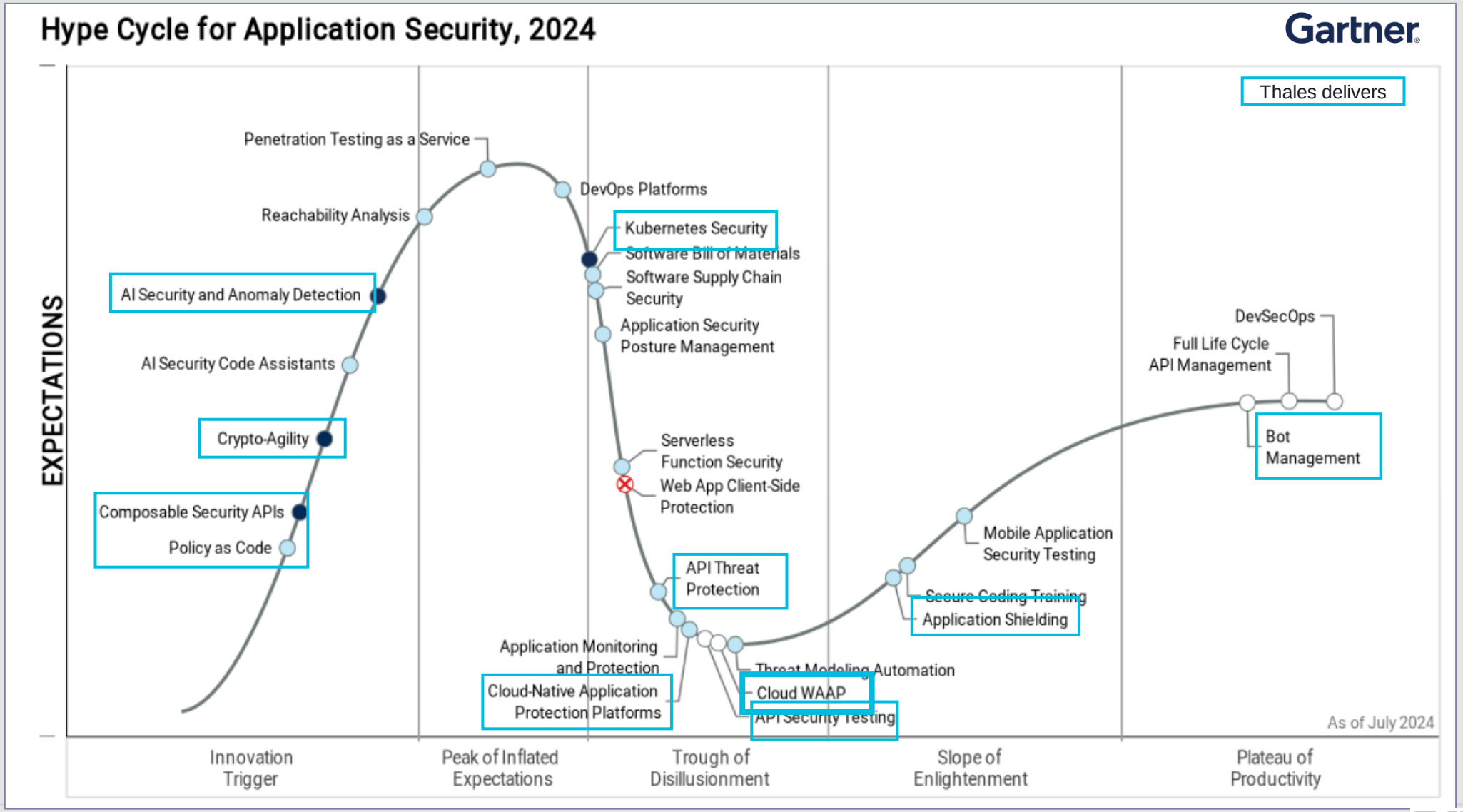
Industry Analyst Assessment

THE FORRESTER WAVE™ Data Security Platforms

Q12023

Q12025

Thales leadership in App Security



Thales Market Leadership

> Forrester

WAAP

> Thales Strengths

- "Imperva has a **solid offering across the board**, but the company **stands out for its layer 7 DDoS**, which includes adaptive protection and relevant out-of-the-box reports. On the product security front, Imperva not only has signed the **CISA Secure by Design Pledge** but also **provides customers with security assessment reports to improve WAF configuration** and application coverage.
- Imperva's reference customers praised the **quality of detection** and were **bullish on customer service**"

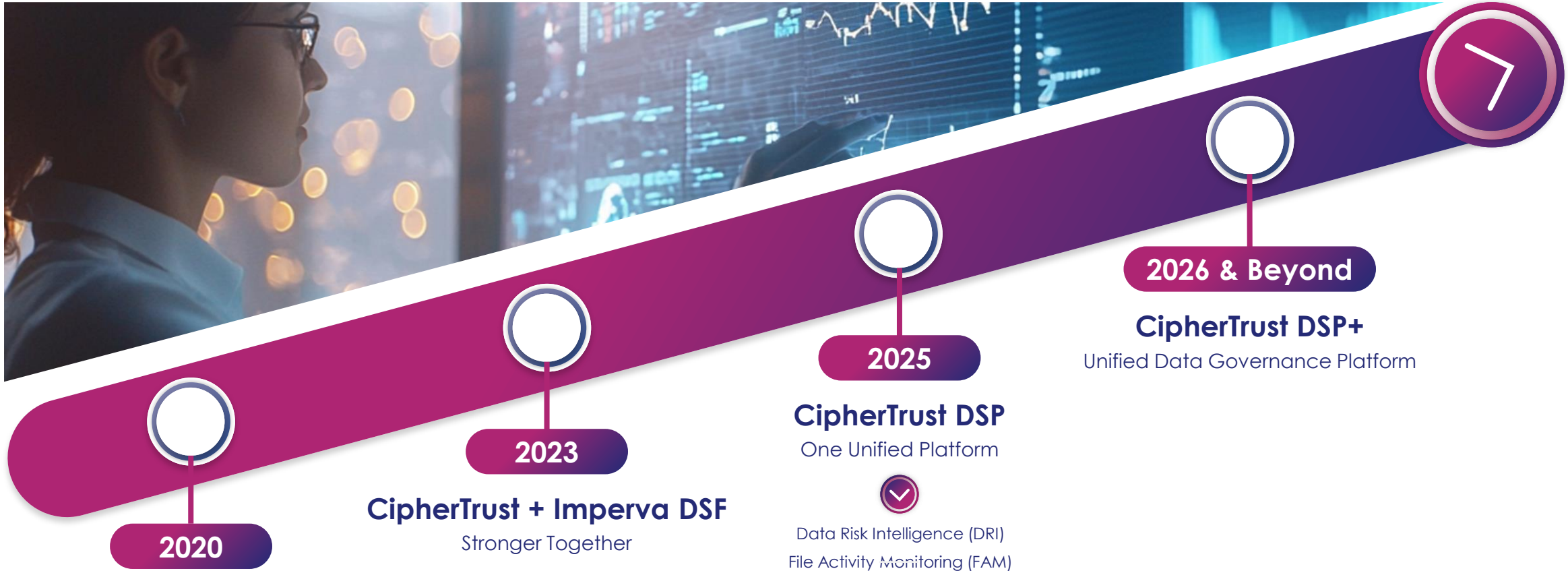
Source: *Forrester*

What's coming in Data Security

THALES
Building a future we can all trust

Partner CONNECT

Data Security Platform Evolution



2020

CipherTrust is born!

Best of Both (KeySecure + DSM)

2023

CipherTrust + Imperva DSF

Stronger Together

2025

CipherTrust DSP

One Unified Platform

Data Risk Intelligence (DRI)

File Activity Monitoring (FAM)

AI Chatbot for Data Security

Post Quantum Readiness

Converged UI/UX

As a service expansion

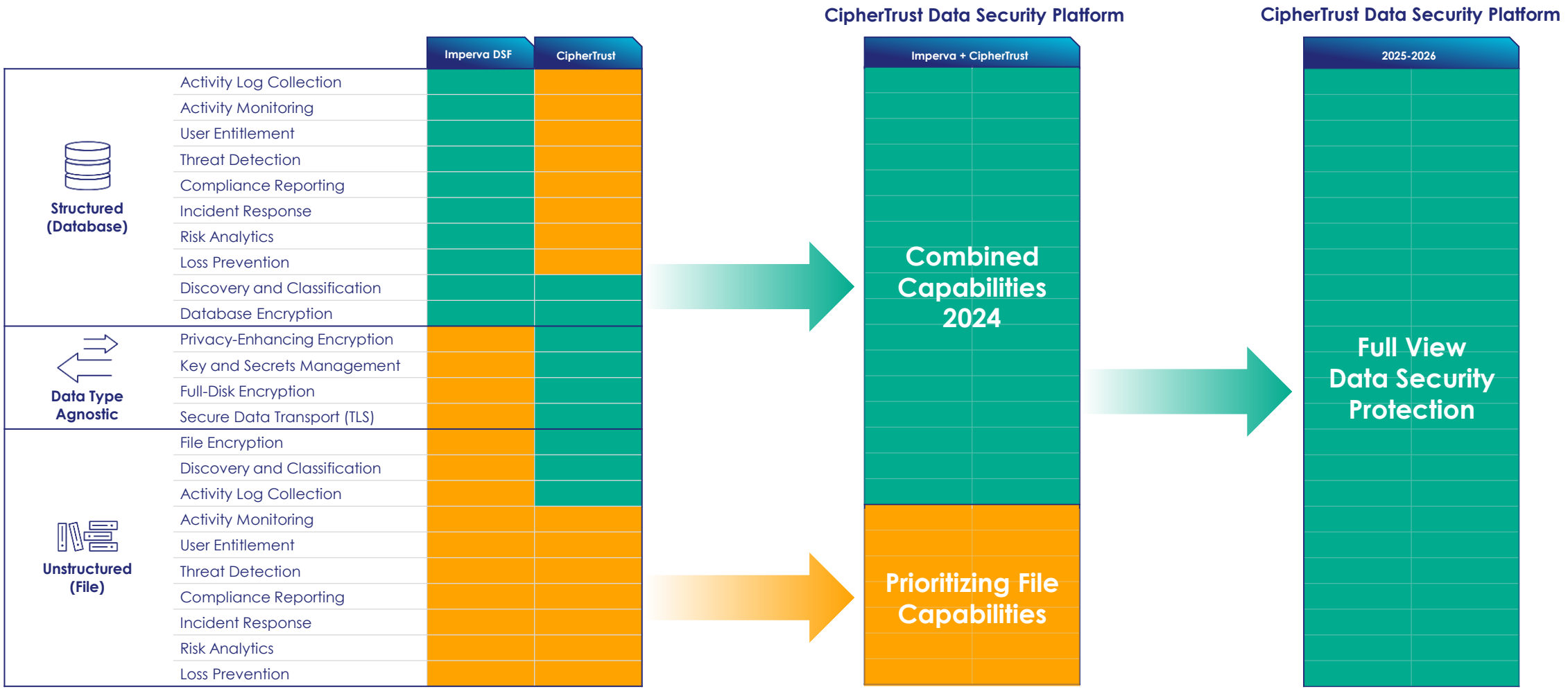
GTM expansion with GCP-DSPM

2026 & Beyond

CipherTrust DSP+

Unified Data Governance Platform

Combine coverage, capability, and scale to complete the platform



Our Focus on Data Security and Key Investment Areas

CipherTrust Data Security Platform – Protecting your data and all paths to it

DEEP VISIBILITY

- Structured Classification and Activity Monitoring
- Unstructured (File) Classification and Activity Monitoring

RISK PRIORITIZATION

- Risk Scoring (Using posture, behavior, and encryption assessments)
- Crypto and Encryption Key Assessment

PROTECT

- Confidential Computing
- Agentless Blocking

CONTROL

- Crypto Agility
- Post-quantum Readiness

2025 Key Data Security Product Releases

Thales + Imperva

Data Risk Intelligence with Encryption

Provide a central data risk application for the organization, including an organization-wide risk score and well prioritized tasks to help reduce the risk in the organization

Q1 GA

FAM – Secure Unstructured Data

Provide compliance and security for unstructured data stores, wherever they reside, to complement the structured data security abilities in DSF

Q2 GA

CT- DSPM with DDC-aaS

Leverage our CipherTrust capabilities to map against the market definition of DSPM. Highlight our new data discovery and classification service and add additional capabillities

Q3 GA

KMIP/TDE-aaS

Give customers a choice, by offering KMIP and TDE as a service. Builds upon our successful launch of CDSP-aaS with CCKM and CTE last year

Q3 GA

NextGen HSM Alpha release

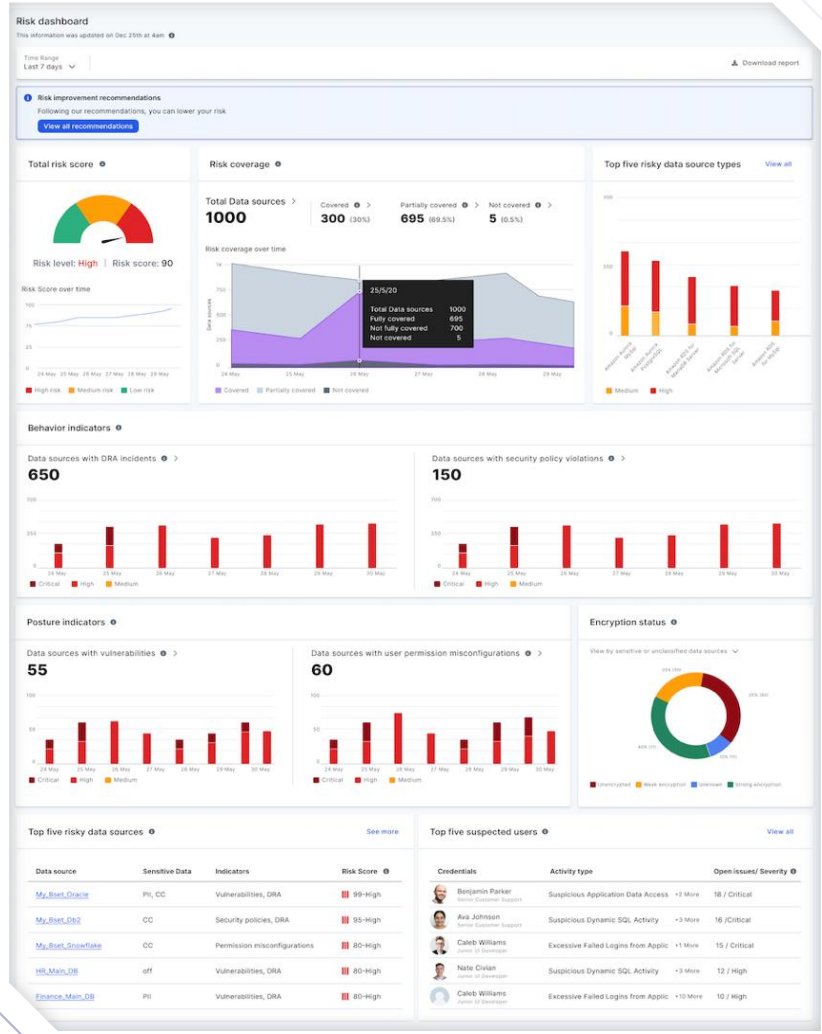
Tech preview and initial testing on our next generation payment and general purpose HSM

Q4 GA

DRI - Customize Risk Score According to Organization's Practice

POSTURE INDICATORS

- Vulnerabilities
- User Permissions Misconfigurations
- Coverage
- Sensitive Data
- Encryption



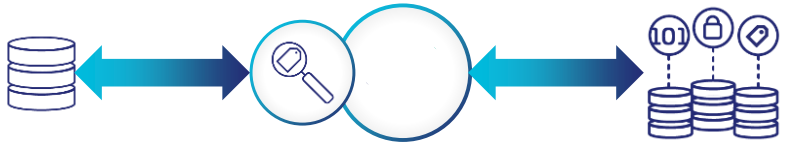
BEHAVIORAL INDICATORS

- Active Attacks on Databases
- Suspicious Scans
- Suspicious Logins
- Suspicious Command Execution
- Suspicious DB Access Scenarios

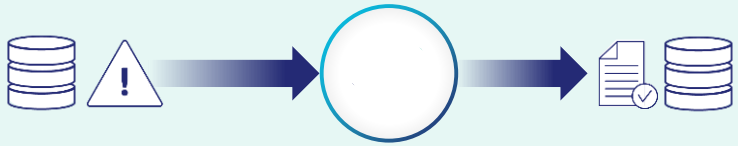
AI-Powered Security and Compliance Automation

1 **AI Assistant for Security and Compliance**: Automates responses to policy violations, audit findings, and data access queries

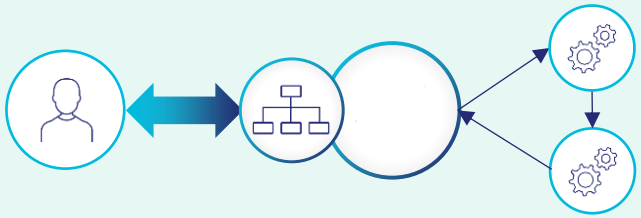
2 **Real-Time Data Classification:** Identifies and categorizes sensitive data using semantic search



Pre-Trained with Transformative Neural Network Architecture



3 **Policy Generation:** Generates policies based on risk incidents and AI-driven recommendations



4 **Automated Workflows:** Creates workflows for tasks like access requests or compliance approvals, allowing you to review and approve efficiently

☐ Roadmap investments

What's Coming in App Security

THALES
Building a future we can all trust

Partner CONNECT

Investment Areas

Security Efficacy

Multi-layer threat detection utilizing behavioral analysis and machine learning techniques while remaining transparent to legitimate human users

Operational Efficiency

ML-driven guidance, insight, recommendations and automated policy creation coupled with programmability to enable scale

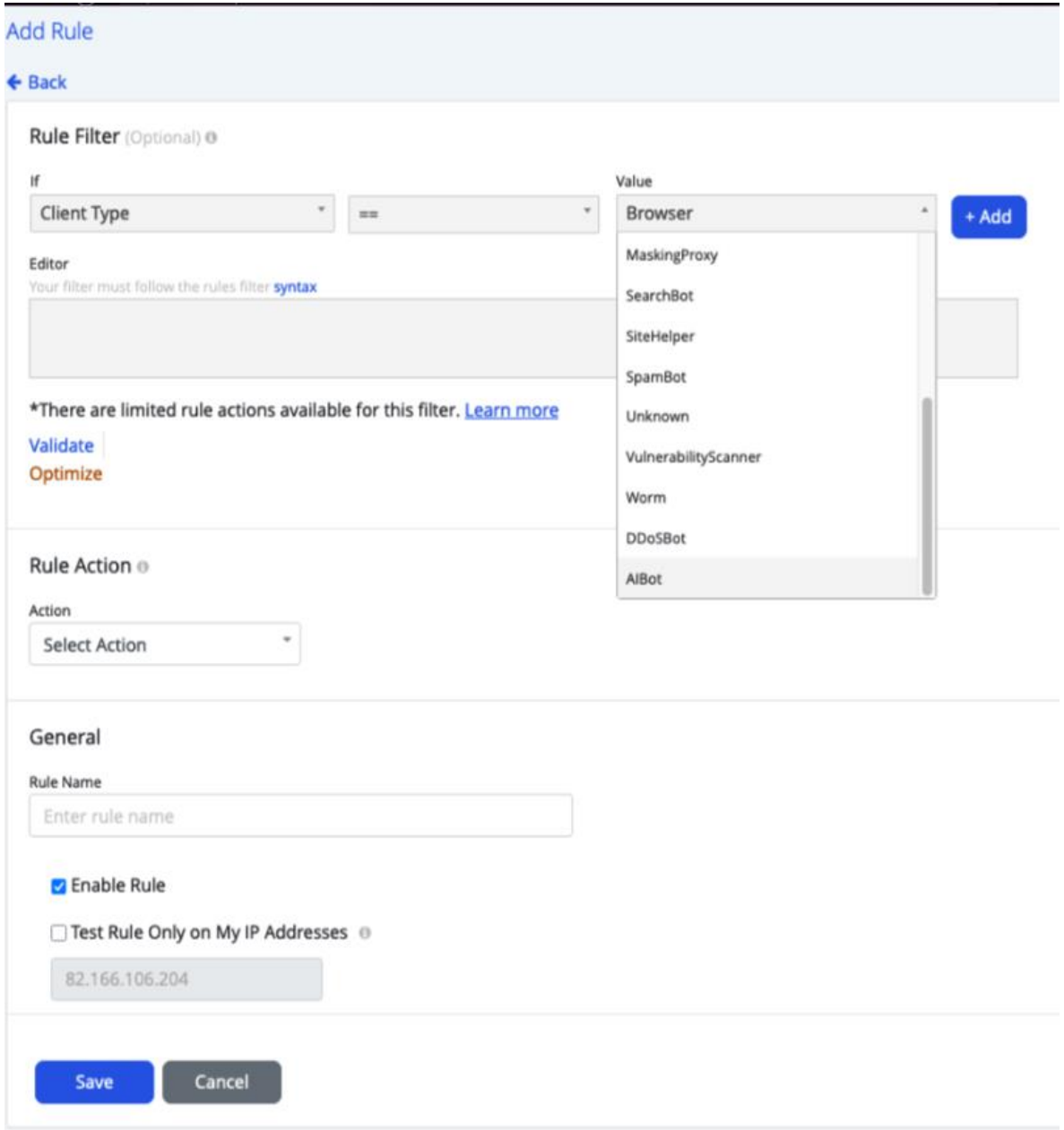
Security Anywhere

Advanced web, mobile, & API protection for apps delivered on-prem, in the cloud or in hybrid environments

Security Efficacy

Detect & Restrict AI Bots

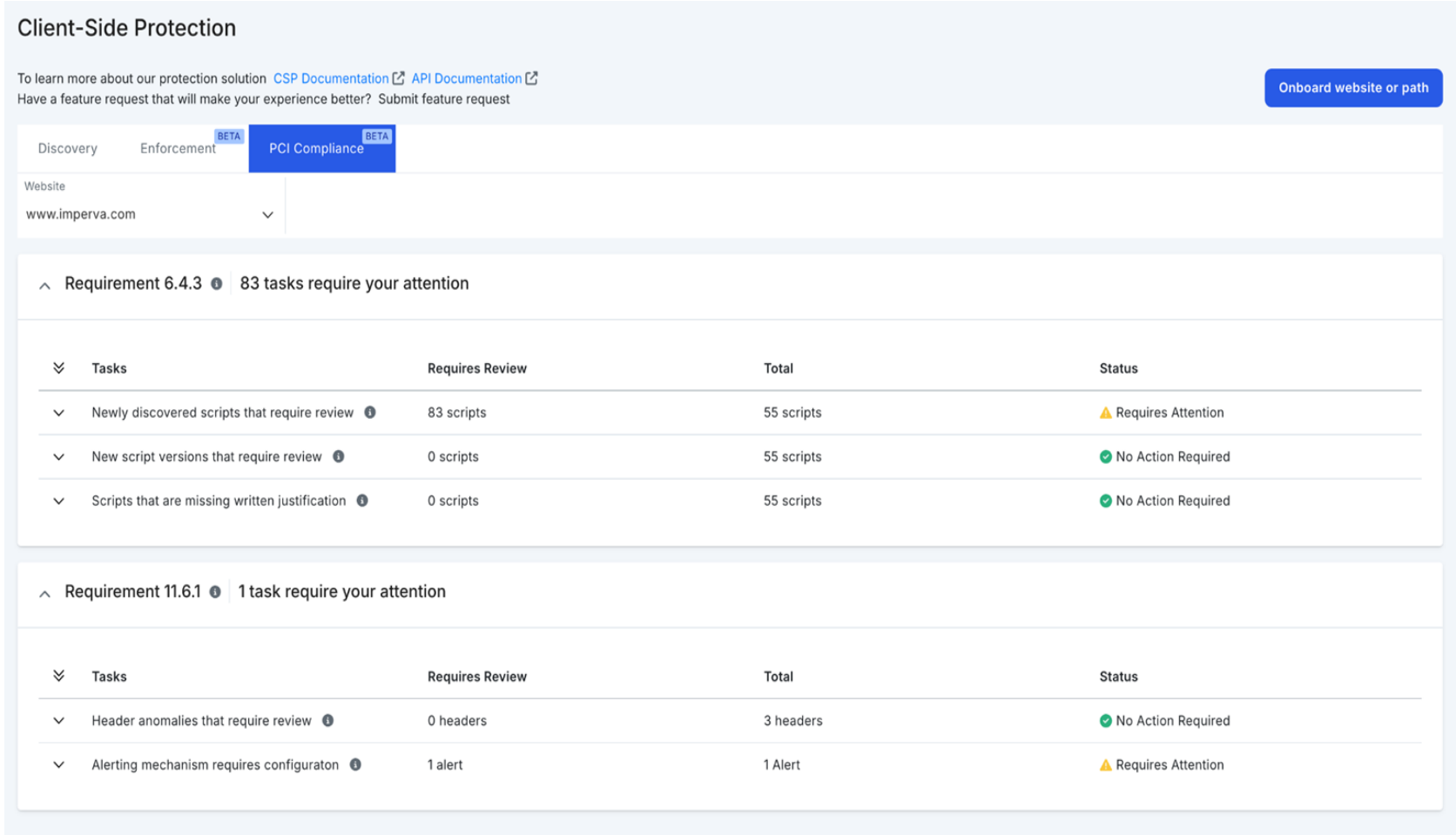
Categorize AI bots and and create custom rules to prevent harvesting of IP or excessive traffic costs



Security Efficacy

PCI DSS 4.0 Compliance Dashboard

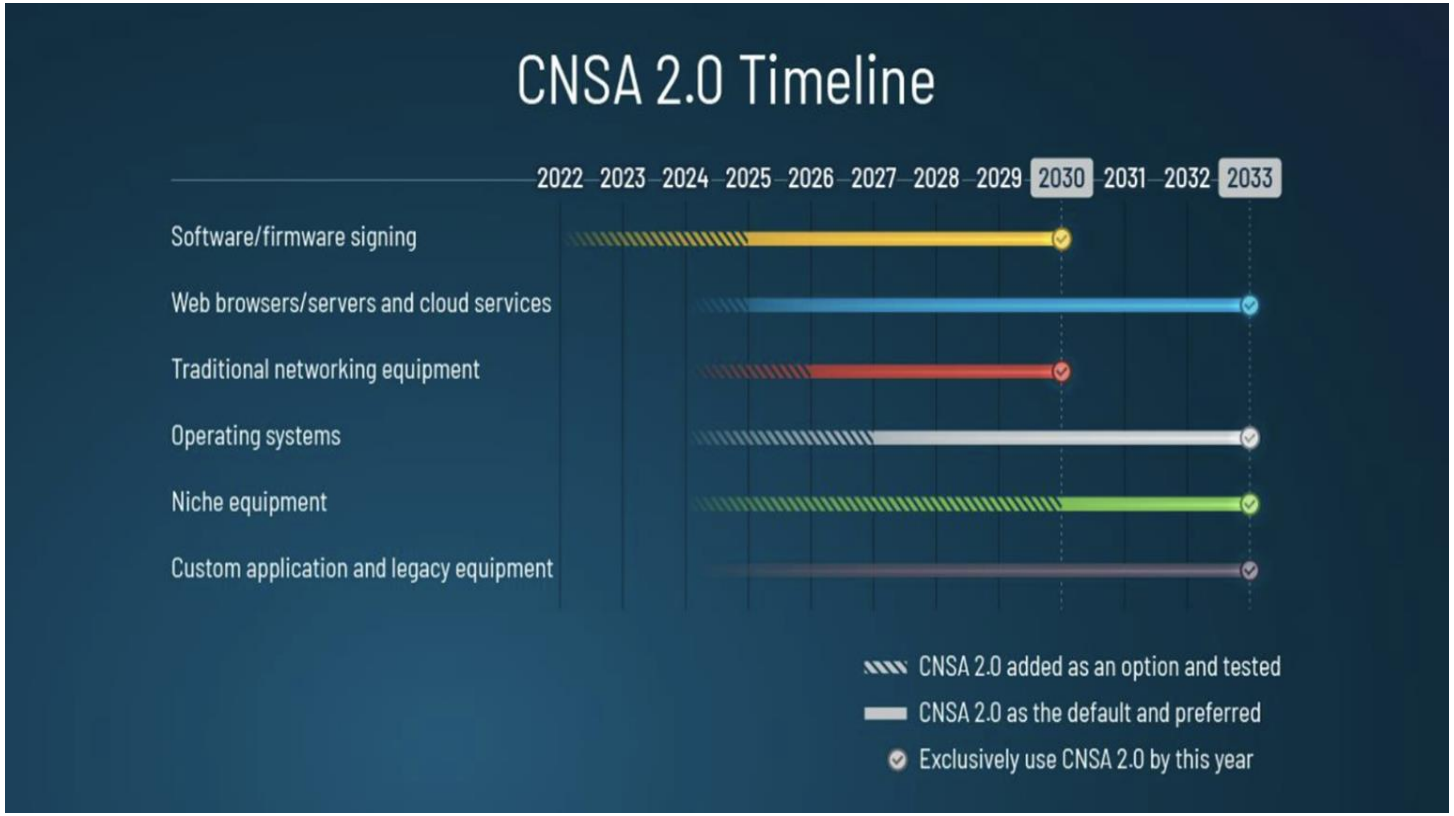
Simplify audit process with a dashboard that demonstrates compliance with 6.4.3 and 11.6.1 requirements



Security Efficacy

Post-Quantum Cryptography (PQC)

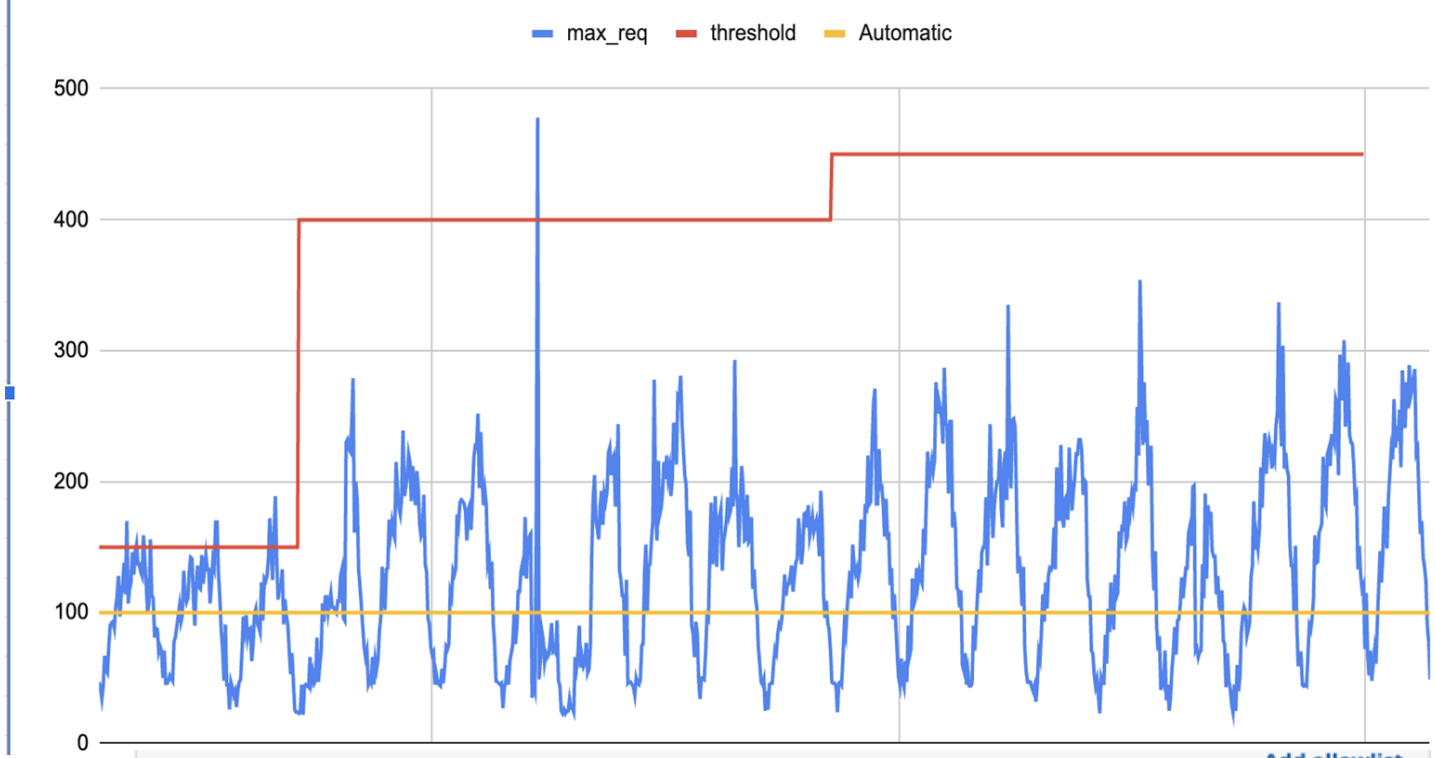
PQC protects data from future quantum computers that could break current encryption. Attackers can intercept and store encrypted data now, planning to decrypt it when quantum technology matures



Operational Efficiency

Adaptive Threshold for L7 DDoS Attacks

Automatically update DDoS thresholds based on historical traffic patterns



Add allowlist

DDoS

Detect and stop distributed denial of service attacks on your website.

Read more

Select a protection option and configure it in Mitigation settings.

- ○ **On**
  Activate mitigation rules for all traffic
- ◉ **Adaptive**
  Activate mitigation rules when request rate exceeds the Imperva threshold
  Current threshold: 500 RPS (last updated on: May 06 2023)
- ○ **Automatic**
  Activate mitigation rules when request rate exceeds your threshold setting
  Static threshold: 1000 RPS
- ○ **Off**
  Do not activate mitigation rules for any traffic or known DDoS attack patterns

Mitigation Settings Slow HTTP Add allowlist

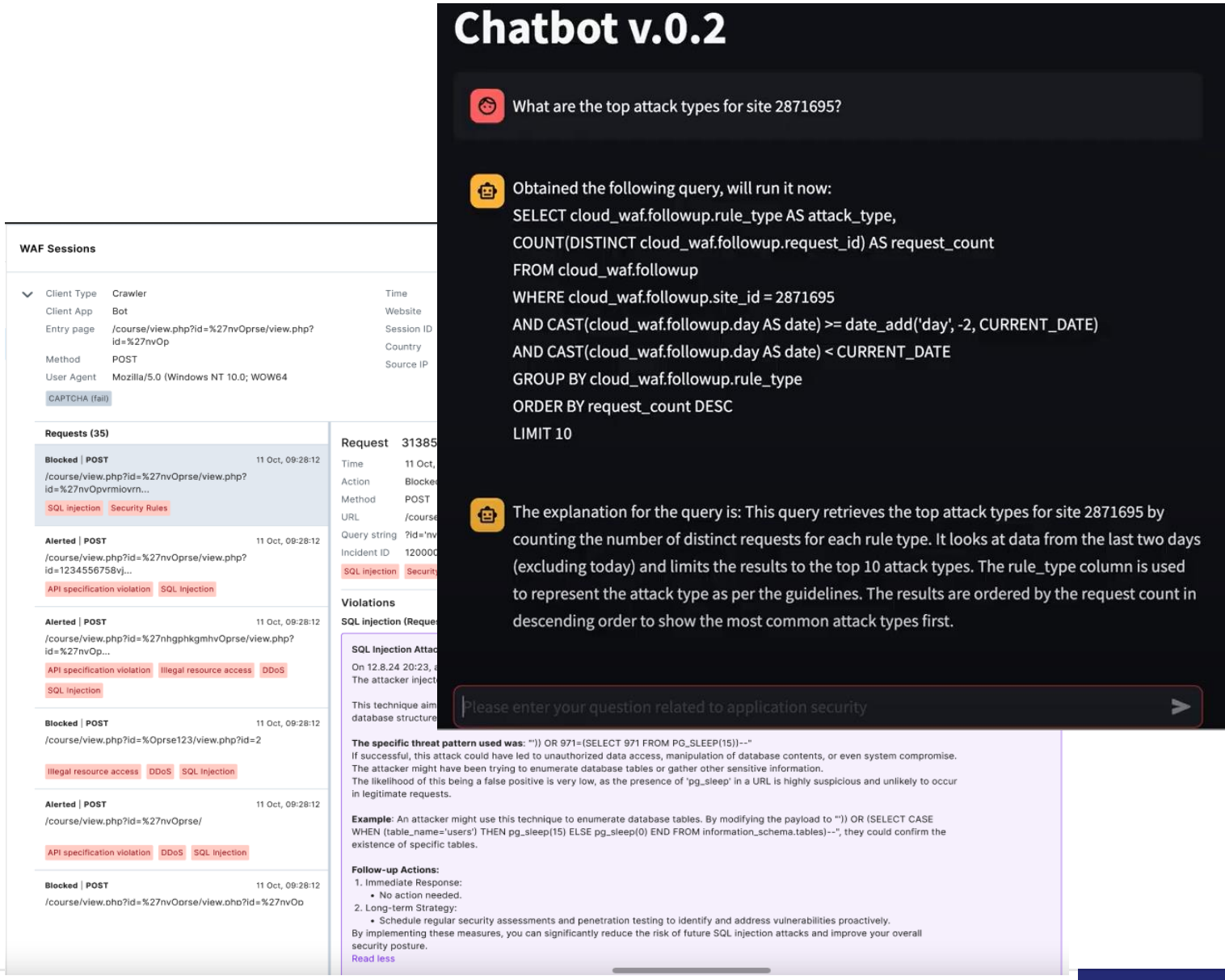
THALES
Building a future we can all trust

Partner CONNECT

Operational Efficiency

Application Security Co-Pilot

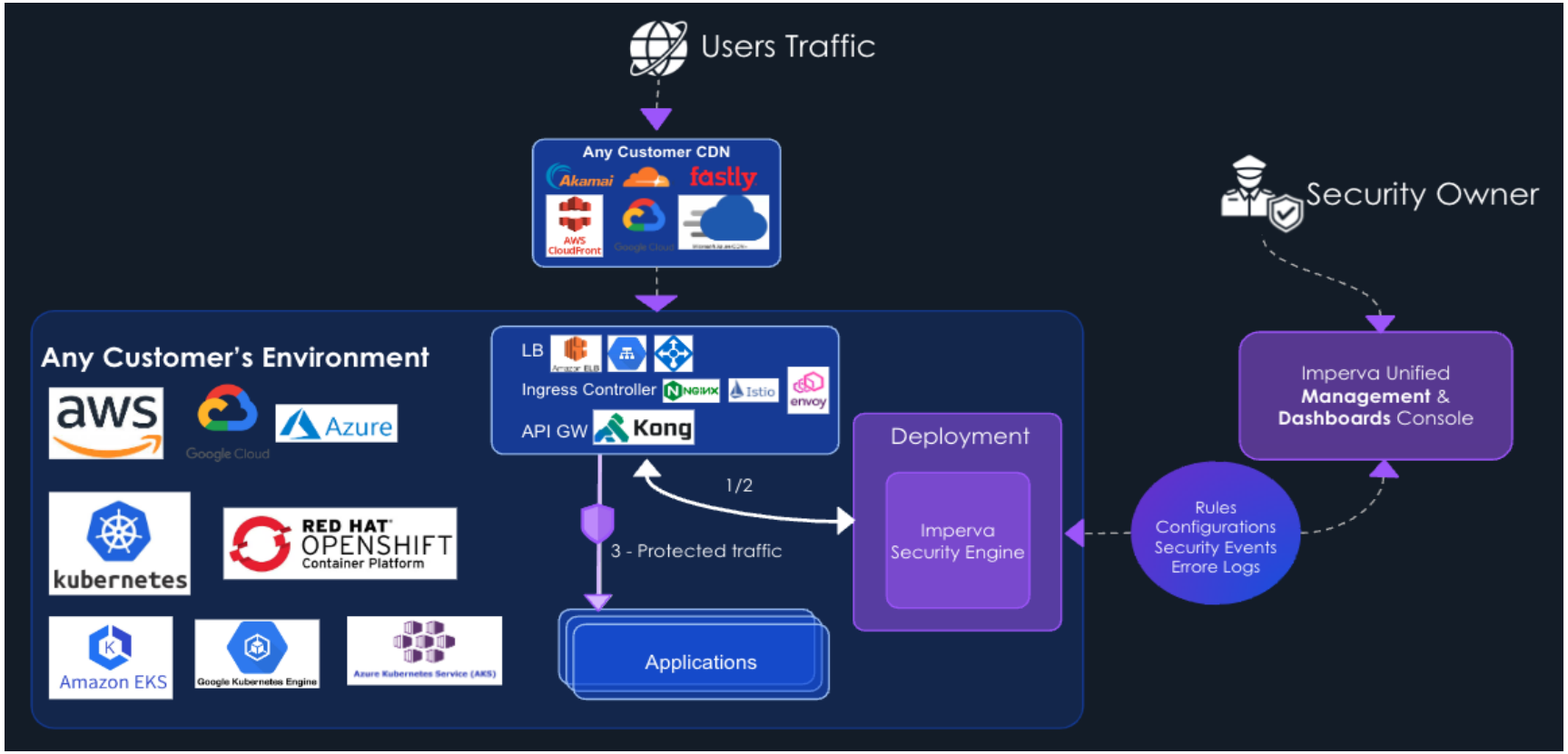
AI-enabled WAF Explain and Chatbot provide natural language context to understand incidents, help answer key questions for investigations and make policy recommendations



Security Anywhere

Elastic WAAP

Modernize WAAP with an on-prem, containerized WAF & API Security solution managed through Imperva Cloud Console and deployable behind any CDN on any Cloud Provider



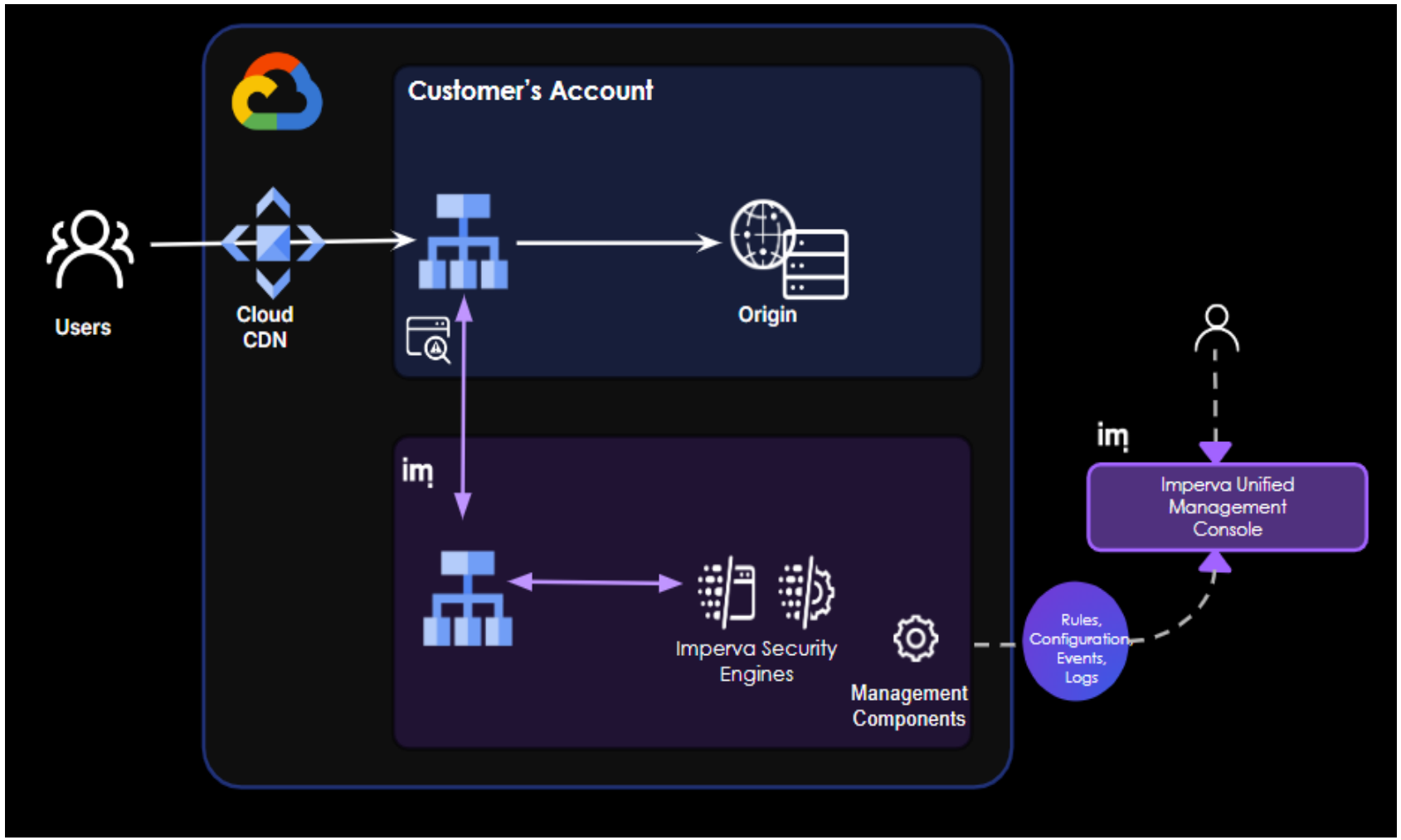
Security Anywhere

Google Cloud Virtual PoP

Best-of-breed security without serializing CDNs

Leverage Google Cloud CDN and Edge Compute

Traffic doesn't leave Google Cloud - lower latency and costs



Key Takeaways

One data security platform

Expand functionality through organic development, as well as with external partners

Compliance + security

Compliance is the foundation that we build upon. However, we do more than just compliance, we're a data security company, not all data is created equal

Future Proof

Security for AI, DSPM and PQC

Vendor consolidation

Get the full package with Thales… one vendor, one platform, one future together

THALES
Building a future we can all trust

Thank you

cpl.thalesgroup.com