Application Security

SHAILES NANDA
Principal SE for EMEA

www.thalesgroup.com

Shailes Nanda

Principal SE

EMEA

Applications have rapidly evolved

Mass adoption of cloud service providers

AWS, Azure, and GCP achieved 63% share of total enterprise spending on cloud infrastructure in Q1 2025

+17.5 billon USD spent on cloud service providers from Q1 2024

Dev teams prefer to use cloud native tools

Over 200 products and services offered via cloud service providers

Faster development cycles, improved scalability and flexibility

Application security is shared responsibility in the cloud

Application security offered by the cloud providers are not good enough

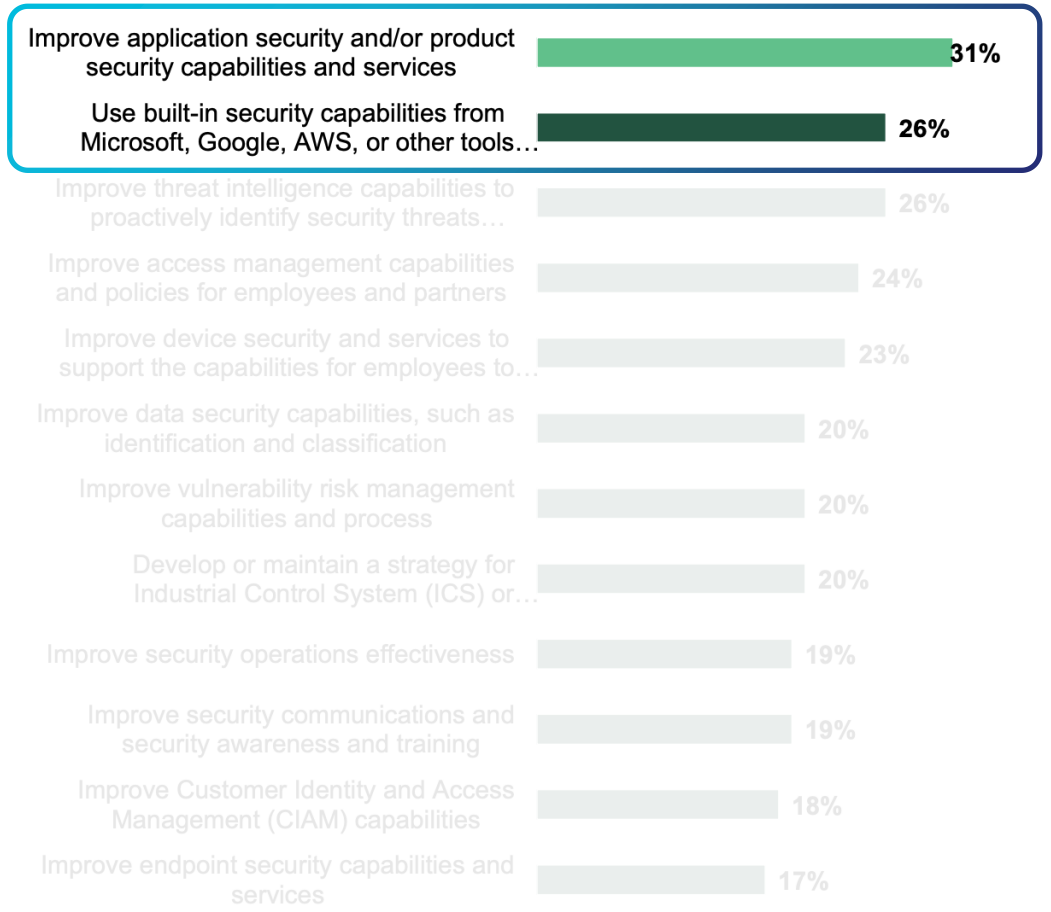
"Classic" WAFs are not a fit to respond to the rapidly evolving threat landscape and pace of business

https://www.crn.com/news/cloud/2025/cloud-market-share-q1-2025-aws-dips-microsoft-and-google-show-growth

Application security is a priority & needed where apps are built

"Which of the following initiatives are likely to be your organization's top tactical information/ IT security priorities over the next 12 months?"

(Multiple responses accepted)



Base: 2,801 Security decision-makers | Source: Forrester's Security Survey, 2024

State of application security market in EMEA

Our chance to catch the wave

14.1%

DDoS market growth

16%

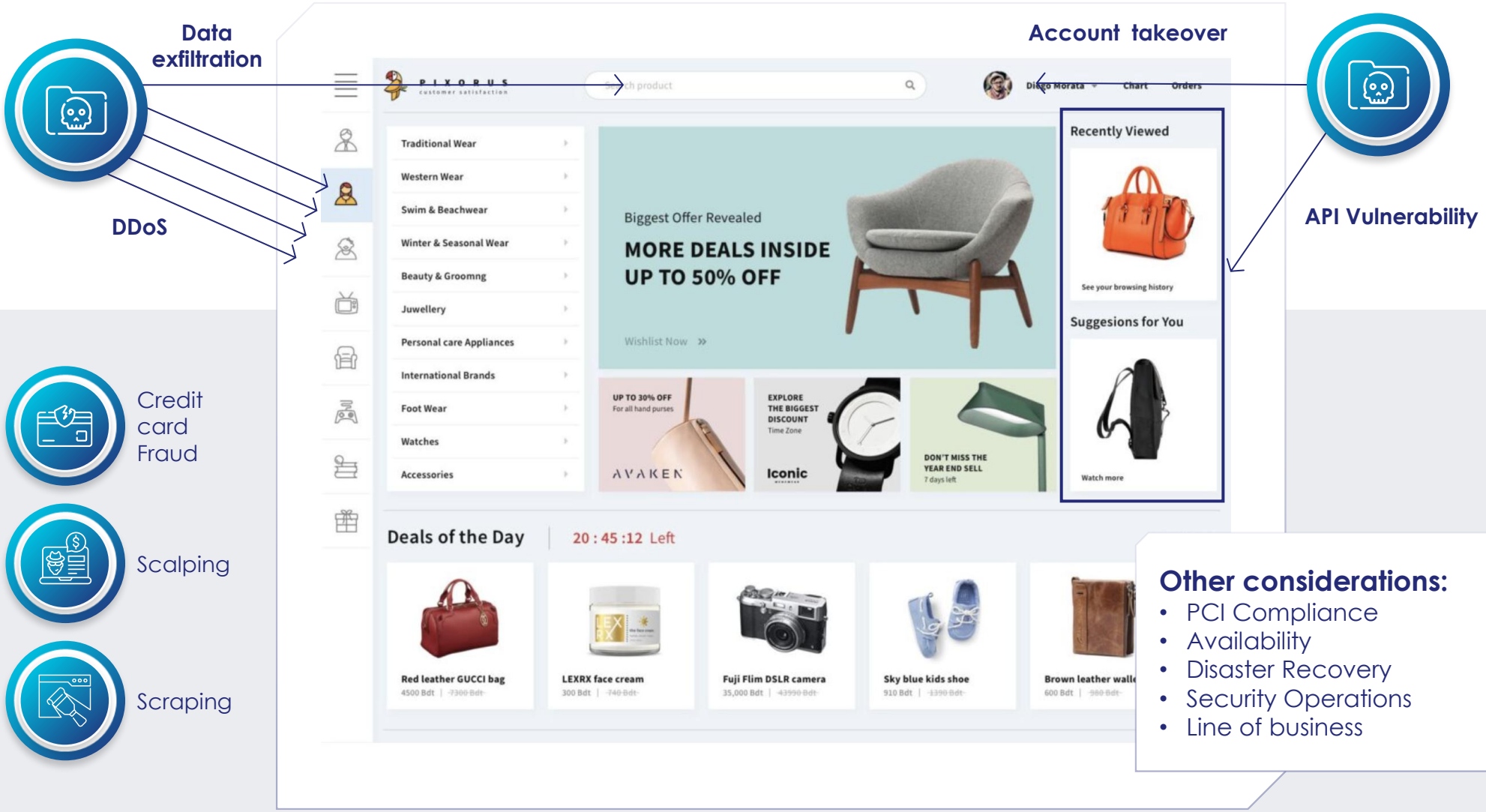
WAF market growth

20%

Bot protection market growth

31.5%

API security growth



Other considerations:

- PCI Compliance
- Availability
- Disaster Recovery
- Security Operations
- Line of business

Key Use Cases:

- Secure Apps & APIs
- Stop bad bots
- Protect from DDoS
- PCI Compliance
- Accelerate app security & delivery

Outcomes delivered

96.6%

of all policies in use are default policies with no changes

95%

of customers have sites with at least one rule in blocking mode

87%

of customers have sites with all rules in blocking mode

20%

Reduction in time spent investigating security events

Making an impact for our customers

Problem

A sophisticated bot attack was targeting Lucky Strike's age registration pages, creating fake accounts and costing the organization **$25–30K daily**

Solution

Expand Cloud WAF deployment by onboarding registration path to Advanced bot protection

Imperva stopped the attack, **saving $200K in 1 week**

Prevented **$8–10M** in annual losses

Won $2.8M deal to become a strategic partner for British American Tobacco

Imperva difference

In-depth visibility into requests hitting the registration page validated that the requests were malicious and gave the customer confidence to mitigate

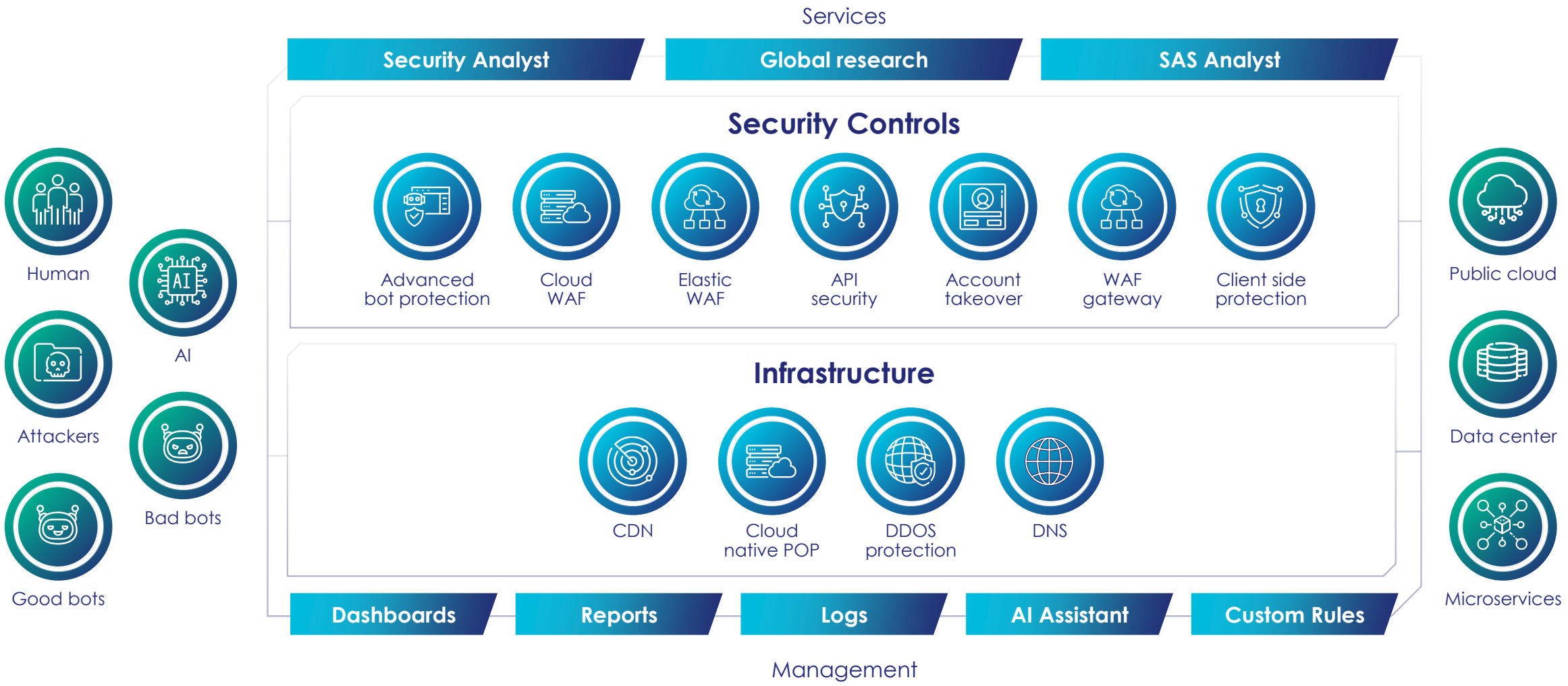
What happens when you amplify good security with automation?

127 A record of active websites onboarded **within an hour**

820 A record of active websites onboarded **within 48 hours**

6000 A record of websites onboarded by **a single customer**

Imperva application security platform



Why are we excited to partner together

Platform strength

Growing market with industry leading platform

$$$

Solve new problems

Address new business problems and emerging use cases

$$$

Strategic services

Enhance your portfolio and introduce new strategic services

$$$

PLATFORM STRENGTH

Why Customers Choose Imperva

Efficacy

Fully managed rule creation and testing to ensure zero false positives frees up resources dedicated to writing custom rules

Efficiency

Automation and streamlining of day-to-day and repetitive tasks to reduce resource consumption

Security Anywhere

Security policy and management that seamlessly follows applications wherever they are deployed

Platform comparisons

	Other vendors	Imperva
Efficacy	Extensive tuning due to open source or cheap technology	Lowest false positive rate
Efficiency	Weeks to months to block attacks	Blocks attacks out of the box
Dependencies	Bundle app security with CDN or load balancer	App sec can be deployed anywhere apps are built
Business outcomes	Higher complexity, cost & reduced efficacy	Effective & efficient security that works out of the box

Shifting gears on the competition

Manual work , Specialty Skills, Cost & complexity

Fully automatic, for anyone, it just works

A global network purpose-built for security

2,000+
Cloud sensor instances

1.5 Trillion
Requests analyzed / month

63 Billion
Attacks blocked / month

<0.01%
False Positive Rate

<3 second DDoS
Mitigation SLA, powered by AI and automation

10
Integrated and unified WAAP products

16Tbps+
DDoS Resilient Datacenters

5,000+
Network adjacencies

99.999%+
Uptime

60+ distributed POPs
Single-stacked solution PoPs

Imperva for Google Cloud - currently in beta

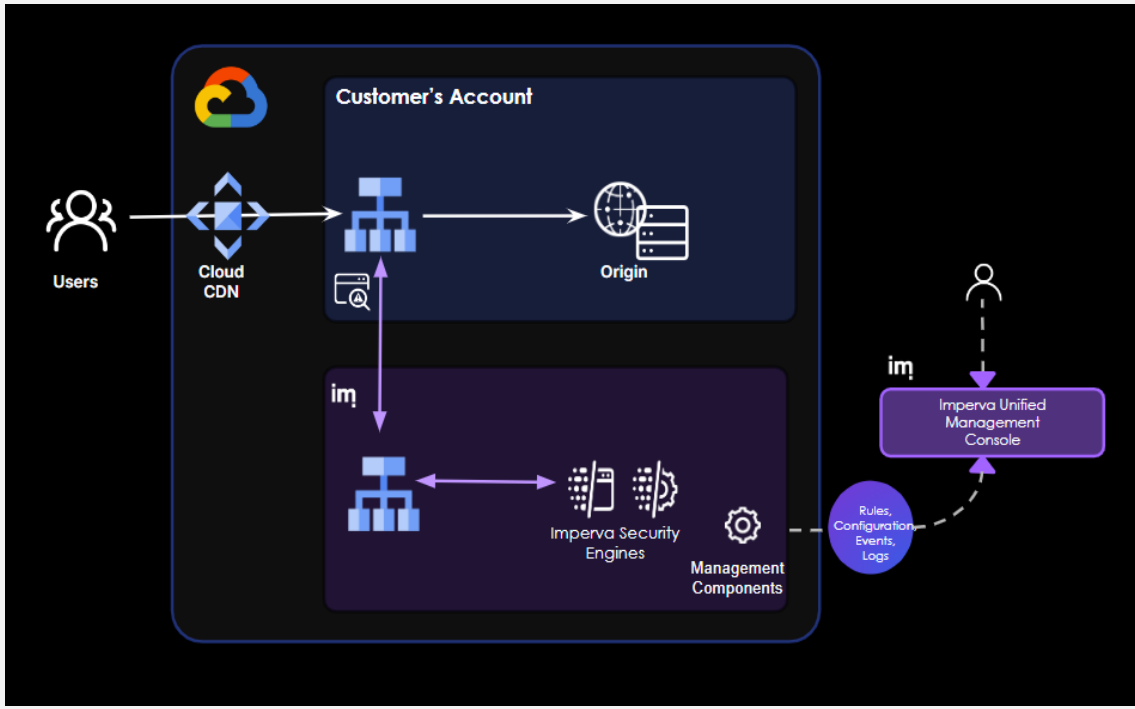
Best-of-breed security without serializing CDNs

Leverage Google Cloud CDN and Edge Compute

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

Easy purchase through Google Cloud that retires commits

Recruiting design partners to onboard and shape the solution



SOLVING NEW PROBLEMS

Emerging threats

API Security:

Blocking BOLA

Advanced Bot Protection:

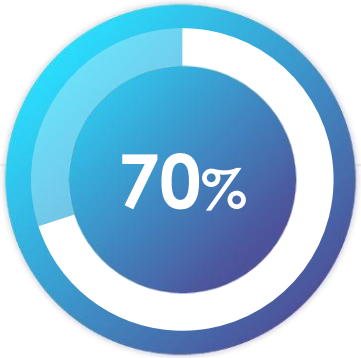
Polymorphic bots

Securing AI:

AI firewall

APIs are on the rise and abused

Annual losses globally from **API insecurity**



of all web traffic is **API based**

Three Steps to API protection

Discovery, assessment, mitigation

Discover all APIs

Always up-to-date inventory, including unspecified APIs

Data classification to identify sensitive APIs

Risk assessment

Automatic risk assessments to identify high risk APIs (including OWASP API Security Top 10 risks)

Visibility to assist security admins to focus their mitigation efforts

Static + runtime mitigations

Static mitigations:

Schema enforcement

Monitor and enforcement of security best practices: API access control posture improvement, schema assessment and security testing

Runtime mitigations:

Prevention of bad bot reconnaissance scan

Policy based runtime Detection and Response (DR)

Imperva bad bot report

Bad bot vs good bot vs human traffic

37% Bad Bot

14% Good Bot

49% Human

Bad Bots	**37%**	+5%	**More automated traffic than human**
Good Bots	**14%**	-3%	
Human	**49%**	-1%	**First time in 10 years**

Impact of bad bots

- **Account takeover**
- **DDoS attacks**
- **Credential stuffing**
- **Commit fraud**
- **Web scraping for AI and LLMs**
- **Disrupt business**
- **Inventory hoarding**
- **Target APIs**

Keep the bots guessing

Simplified and automatic mitigation selection to confuse attackers

Rollout strategy

Enables customers to gradually move from mitigating **1%** to **100%** of traffic

Time-based strategy

Mitigate only at specific times so attackers can't learn how to evade detections

Random mitigation strategy

Allow predefined segment of traffic at specific times so attackers believe their bots are working until its too late

Mitigation stack strategy

Force attackers through computationally intensive challenges like captcha and proof of work before blocking or tarpitting them

SECURING AI

Strengthen your AI security posture with enhanced visibility, control and protection against threats to data, models and applications

SECURE AI DATA

Protect sensitive data and comply with regulations in AI initiatives

ENSURE INTEGRITY OF AI

Protect AI applications and models from corruption, misuse or theft

PROTECT AGAINST AI ATTACKS

Monitor continuously for risks and threats from AI and to AI

Secure the AI lifecycle with Thales

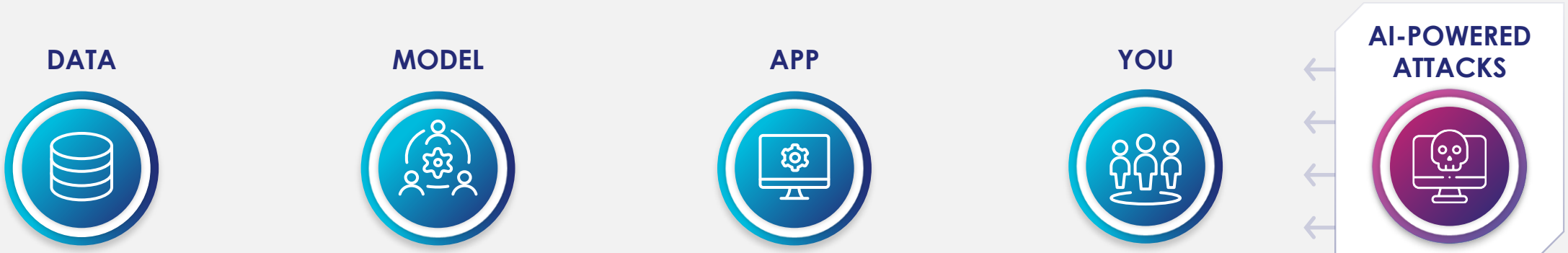
Thales helps organizations protect the AI lifecycle from model development and training to deployment and usage

DATA SECURITY: CipherTrust Platform, HSMs

APPLICATION SECURITY: WAF, Bot Protection, API Security

Protect sensitive data and AI model

Protect AI application & stop ai-powered bots



Data Collection | **Training** | **Deployment** | **Inference/RAG**

Protect and monetize AI model & application

Protect from ai-powered attacks

SOFTWARE MONETIZATION: Sentinel

IDENTITY & ACCESS MANAGEMENT: Workforce IAM

Protect AI application & stop AI-powered bots

Customer challenges

API abuse in AI applications
Vulnerable APIs in AI applications can be exploited to bypass security measures

Prompt injection
Attackers prompt LLMs to perform unintended actions and reveal confidential information

Business logic abuse
Attackers leverage APIs to exploit business logic by identifying and manipulating workflows

Advanced AI-powered bot attacks
ML-powered Bots can mimic human behavior to manipulate AI systems

Benefits/capabilities

Prevent data extraction and business logic abuse
Detect, classify, and protect vulnerable APIs

Mitigate API abuse
Monitor and protect API traffic in real-time

Prevent malicious AI-powered bot attacks
Detect and prevent malicious Bot attacks on AI model, data or applications

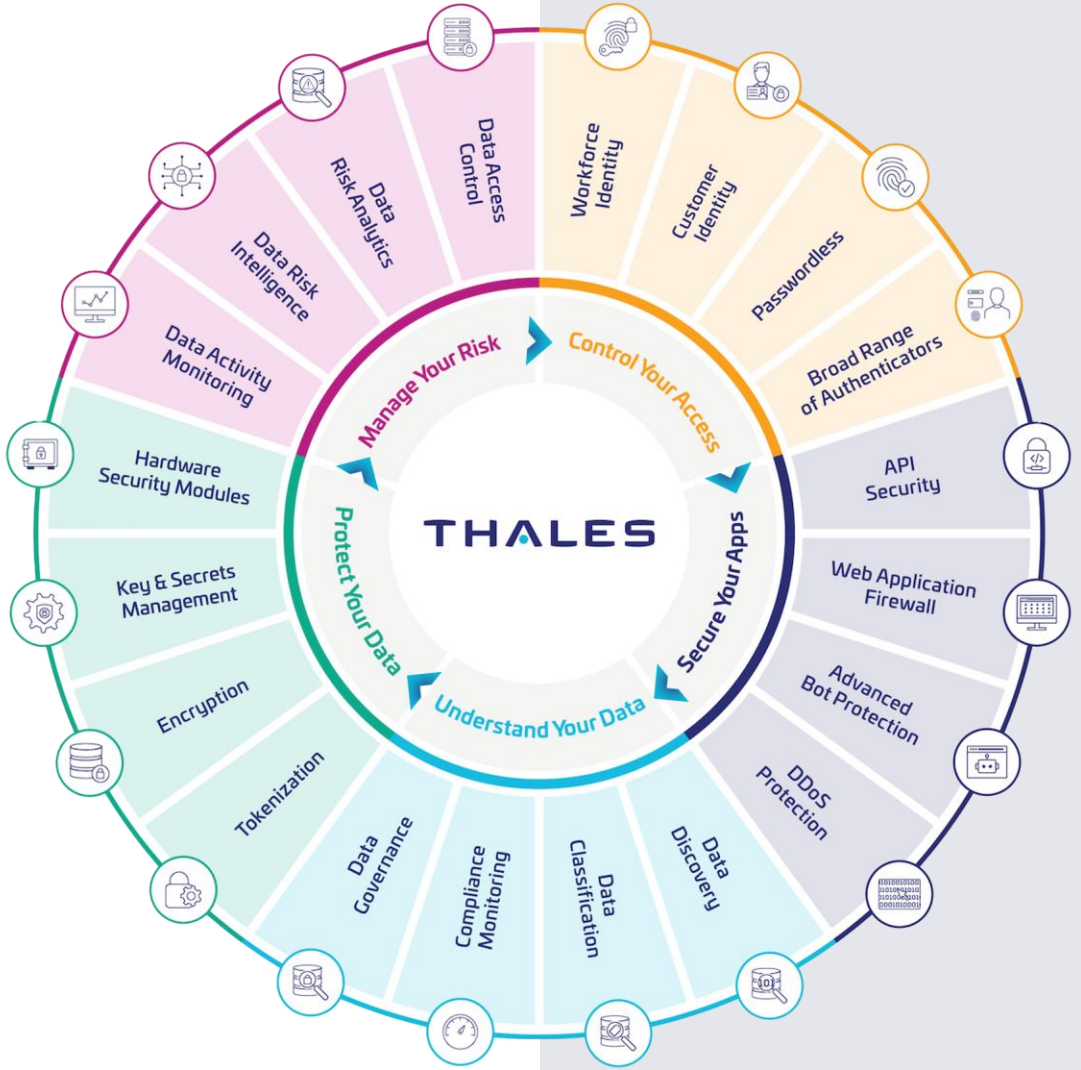
Control bot access and secure APIs
Prevent data scrapping, model manipulation, and comply with regulations

Application Security Solutions

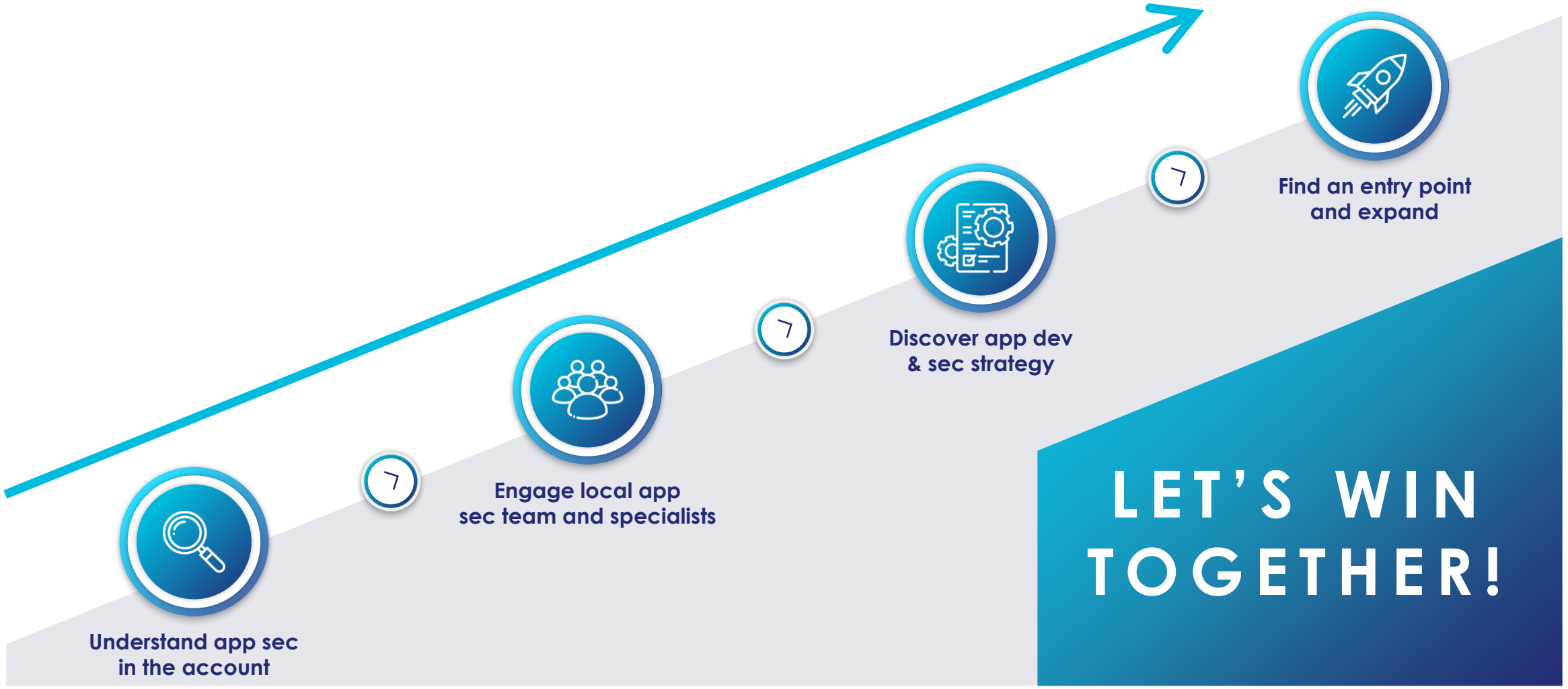
API security **Bot protection**

THALES CYBERSECURITY PRODUCTS

Pivoting services
around the portfolio



Closing thoughts:
How we will grow together




THALES
Building a future we can all trust
Thank you
www.thalesgroup.com