How to sell more (AppSec use cases)

BARTOSZ CHMIELEWSKI
Senior Sales Engineer - AppSec Specialization
(CEE, BeNeLux, Nordics)

www.thalesgroup.com

THALES
Building a future we can all trust

Bartosz Chmielewski

Senior Sales Engineer –
AppSec Specialization
(CEE, BeNeLux, Nordics)

Agenda

1 Common Problems we are solving in AppSec

2 Typical Use-Cases

3 Best practices for pre-sales

Common problem we are solving in AppSec

Vulnerability to DDoS attacks.

Use of cheap and low-quality WAF/WAAP Protection.

Manageability challenges = high TCO.

Increasing dependency on CSP, CDN or ADC environments.

High rate of False-Positives.

Insufficient advanced capabilities.

No control over APIs

Lack of a unified API inventory

Lack of API-focused risk assessment tools

Lack of Data Classification.

THALES
Building a future we can all trust

Partner CONNECT

Common problem we are solving in AppSec

Dependence on US-based tech stack.

Bot activity negatively impacting business operations.

Lack of deployment flexibility.

Identity thefts and account abuse affecting company reputation.

Customer's SOC lacks understanding of web-related attacks.

USE-CASES

Use-Case 1

The Customer

Mid-size fintech in Belgium

Current environment

Business-critical apps are deployed primarily on Azure. Advanced DevOps processes are in-place. Apps need to be secured effectively. Needs to align to numerous regulations. Introducing Multi-Cloud approach.

The problem

Manageability challenges with Azure WAF. CSP lock-in. Lack of advanced capabilities like Client-Side Protection.

The solution

Imperva WAF provides cloud-agnostic WAF product with advanced capabilities (like Client-Side Protection). The enterprise-grade management console can significantly reduce the TCO. Additionaly, the CDN layer will reduce the data transferred from/to Azure Environment.

Use-Case 2

The Customer

A well-established, major car parts retailer in Estonia.

Current environment

Hybrid environment. A significant amount of proprietary data is shared on the public websites (SKUs, parts compatibility, schemas). Applications are currently protected with open-source tools maintained in-house.

The problem

Competitors are using bots to scrape the website to steal the proprietary information and product prices. As a result, they can deliver similar value at the lower price. The revenue is severely impacted.

The solution

Imperva Advanced Bot Protection can precisely differentiate between bots and humans and stop scrapers from stealing the intellectual property and scraping the prices. The SAS team can maintain the bot policy to ensure high ROI.

Use-Case 3

The Customer

Major bank in Romania

Current environment

On-prem DCs with a very limited adoption of public cloud services. The availability of their business-critical app depends entirely on their DCs. Regulatory requirements prevent decrypting any traffic in the cloud.

The problem

Due to tense political situation, the bank experienced a successful attack this year. An internal risk-assessment revealed the need for a premium DDoS protection service to reduce the likelihood of future incidents. Low latency, low TCO and SLA are crucial.

The solution

Imperva DDoS Protection for Networks provides On-Demand protection without the need to configure static rules or perform ongoing maintenance. Latency remains unaffected during normal operations.

THALES
Building a future we can all trust

Partner CONNECT

Use-Case 4

The Customer

University in BeNeLux

Current environment

On-prem environment with F5 LTM deployment. The applications are behind the LTM and the WAF protection is applied (F5 AWAF).

The problem

While the customer is satisfied with the ADC provided by F5 LTM, the WAF is creating operational challenges. In consistently generates a high volume of False Positivies despite their best efforts to optimize it. They need 0,5 to 1 FTE to handle.

The solution

With its advanced correlation engines, the Imperva WAF Gateway (or eWAF) reduces false positives to nearly zero. This allows customers to implement high-quality WAF protection without the typical operational overhead.

Use-Case 5

The Customer

Mid-Size bank in Poland

Current environment

The bank operates a large, purely on-prem environment but is actively transitioning to the cloud-native model, with a substantial Kubernetes deployment of over 200 hosts (on-prem). They are operating WAF Gateways.

The problem

Unable to provide WAF Protection for some subset of applications deployed on Kubertnetes environment due to architecture constrains.
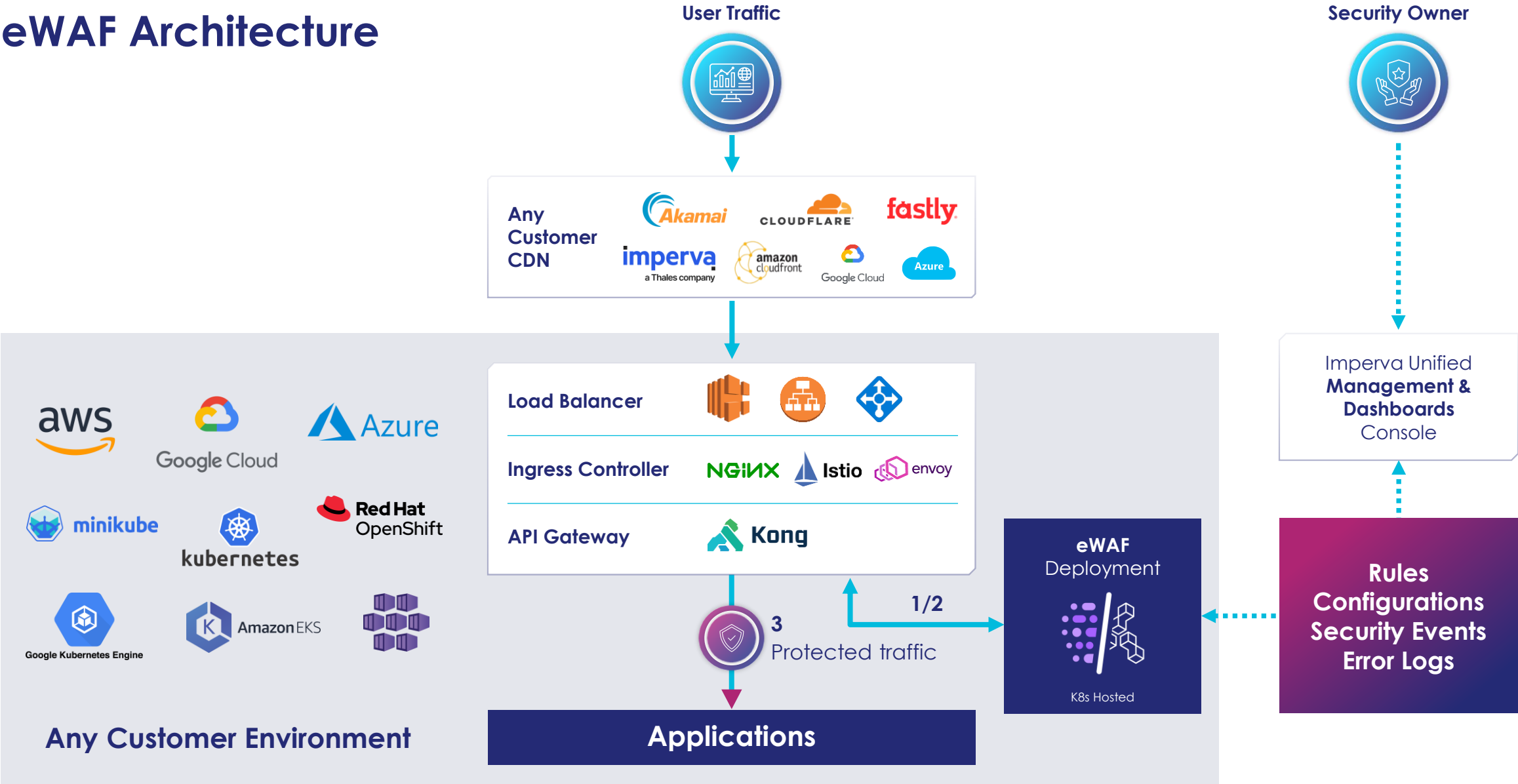
The solution

Deploying Elastic WAF, which is integrated with the Kubernetes platform, offers a seamless experience for DevOps teams. This integration ensures all workloads are properly secure and that security incidents can be effectively reviewed.

Imperva AppSec WAF Options Comparison

	Customer Use-Case	Deployment Method	Deployment Location	Deployment Responsibility	Management
Cloud WAF	Easy to implement and operate solution (low TCO) without on-prem footprint. L7 DDoS, APISec, CDN, Advanced Bot Protection, ATO protection, CSP protection.	Multi-tenant SaaS	Imperva Global POP Network	Imperva	Imperva Cloud Console
Elastic WAF	Easy to operate solution (low TCO) behind existing CDN. Need for locally deployed data plane. K8s environments available.	Cloud Native (K8s) application.	K8s on-prem or in the Cloud (via ingress plugin)	Customer	Imperva Cloud Console
WAF Gateway	Need to a local data and management plane (compliance). Positive sec. model. Advanced customizations and logging.	HW or VMs. (Transparent) Reverse Proxy, Bridge.	On-Prem or in CSP as IaaS	Customer	Local Console

eWAF Architecture

User Traffic

Security Owner

Any Customer CDN
- Akamai
- CLOUDFLARE
- fastly
- imperva a Thales company
- amazon cloudfront
- Google Cloud
- Azure

Any Customer Environment
- aws
- Google Cloud
- Azure
- minikube
- kubernetes
- Red Hat OpenShift
- Google Kubernetes Engine
- Amazon EKS

Load Balancer

Ingress Controller — NGINX, Istio, envoy

API Gateway — Kong

3 Protected traffic

1/2

eWAF Deployment
K8s Hosted

Applications

Imperva Unified **Management & Dashboards** Console

Rules Configurations Security Events Error Logs

Best practices for pre-sales…

Understand customer's problem (or make the customer understand his problem)

Be a trusted advisor (not a seller). Fell fee to talk about upsides and downsides of proposed solution

Propose a solution (instead of talking about products)

Be focused on building a solid business case

Be in customer's mindset regarding the competitive landscape

Minimalize sales cycle length