Check Point
SOFTWARE TECHNOLOGIES LTD

PROTEÇÃO PARA APLICAÇÕES WEB E API

Henrique Moisés – Security Engineer

Irapuan Lima – Security Engineer

Segurança em Todo Lugar

CLOUD

- CloudGuard Dome9 — Cloud Posture Management
- CloudGuard LOG.IC — Network Traffic Analysis
- CloudGuard Workload — Runtime Workload Protection
- CloudGuard SaaS — SaaS, Email Security
- CloudGuard IaaS — Cloud Access Control, Prevention
- CloudGuard Edge / CloudGuard Connect — Branch Threat Prevention

Multi & Hybrid Cloud

SD-WAN

NETWORK

SandBlast NETWORK

Headquarters

- Access Control
- Data Protection
- Multi Layered Security
- Advanced Threat Prevention

Branch

- Access Control
- Multi Layered Security
- Advanced Threat Prevention
- Wi-Fi, DSL, PPoE Ready

CHECK POINT INFINITY NEXT

Threat Intelligence Compartilhada

THREATCLOUD

R80

Gerenciamento Segurança Consolidado

MOBILE

SandBlast MOBILE

- App Protection
- Network Protection
- Device Protection

- Capsule WorkSpace/Docs
- Remote Access
- Secure Business Data
- Protect Docs Everywhere

INTERNET of THINGS

Risk Analysis, Auto Segmentation, Threat Prevention

ENDPOINT

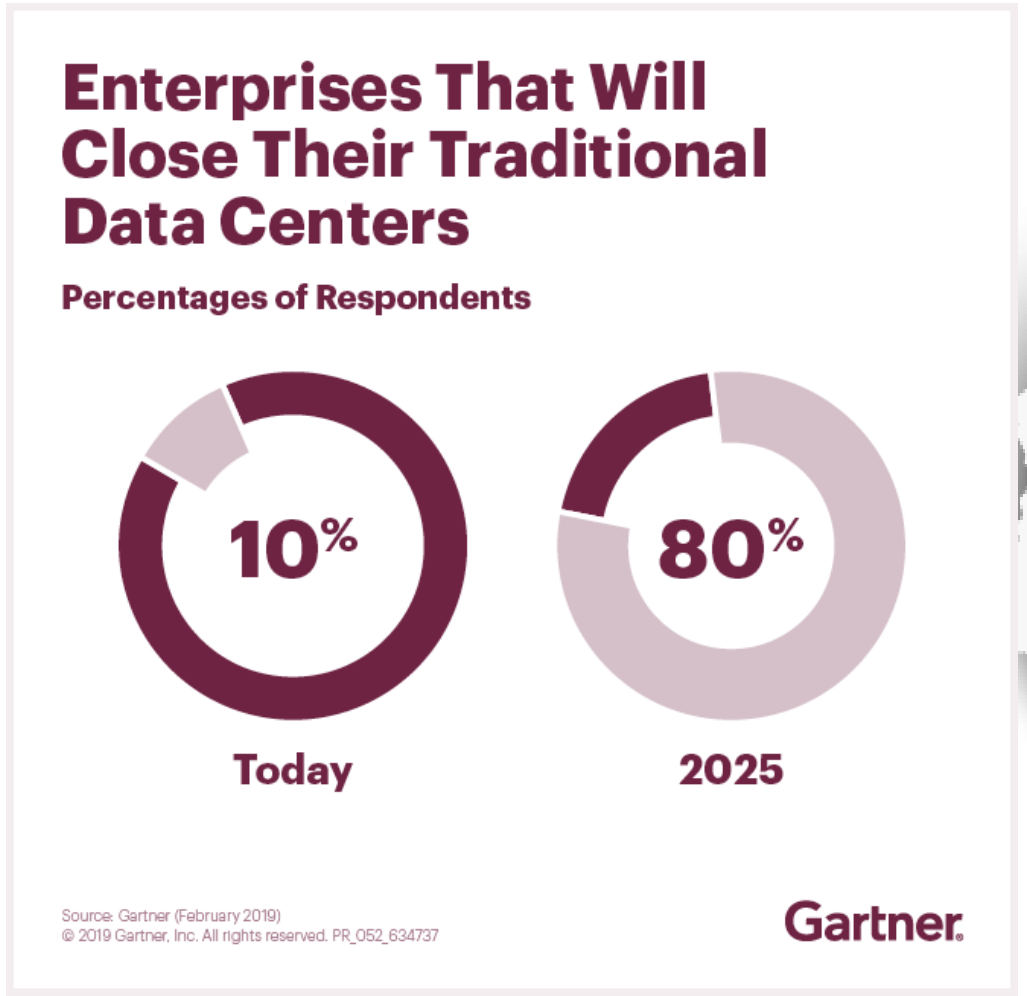
SandBlast AGENT

- Threat Prevention
- Anti-Ransomware
- Forensics

Access/Data Security

- Access Control
- Secure Media
- Secure Documents

O **Crescimento** Constante das **Aplicações** Web



PUFFIN SECURITY

Perda de **receita** ou até **interrupção** dos negócios

Penalidades juridicas (ex.: **LGPD**)

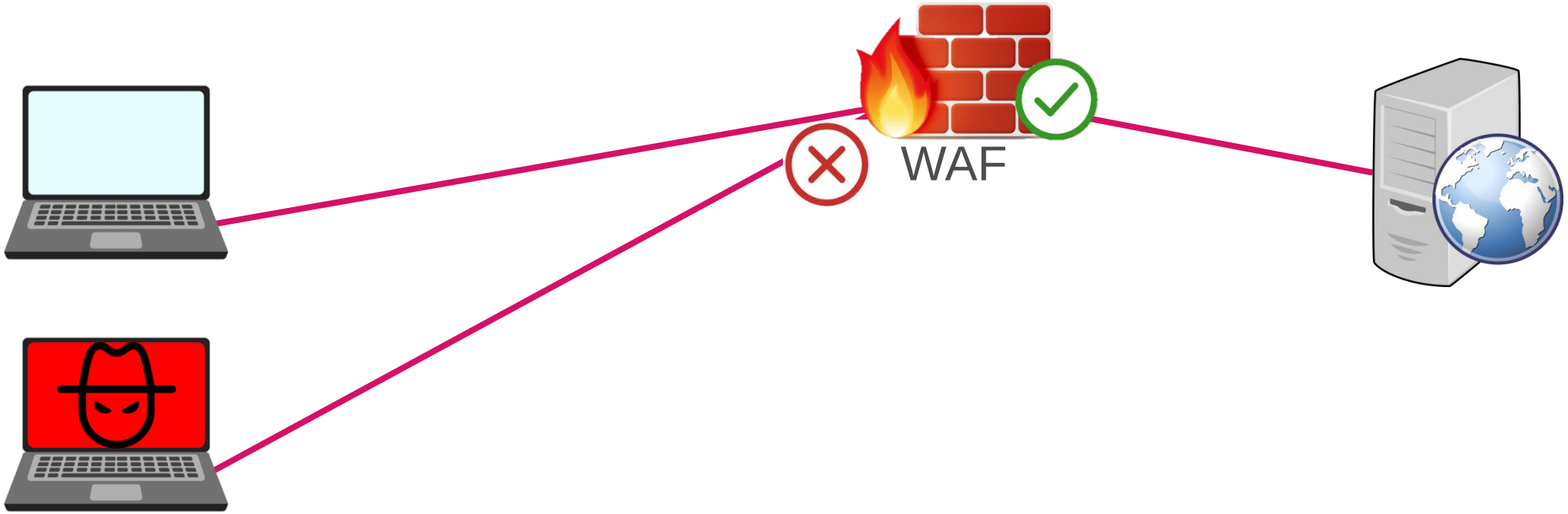
Dano à **reputação**

Problemas com métodos de **pagamento** online

Perda econômica por **fraude**

DEMO

Acesso à Aplicação Web



SEU DATACENTER & APLICAÇÕES AGORA ESTÃO *EM TODO LUGAR*

DE:

- DATACENTERS TRADICIONAIS
- ESCRITÓRIOS REMOTOS ADMINISTRADOS CENTRALMENTE
- APLICAÇÕES Tier 3 (Web, App, DB)
- DEMAIS APPS E SERVIÇOS LOCAIS

PARA:

- NUVEM HIBRIDA PÚBLICA + PRIVADA
- ESCRITÓRIOS REMOTOS CONECTADOS DIRETAMENTE À NUVEM
- CONTEINERS & MICROSSERVIÇOS
- APLICAÇÕES SaaS

Dificuldades de um WAF Tradicional

Resultado: Alto número de Falso Positivos

Desafios das Soluções WAF

Check Point
SOFTWARE TECHNOLOGIES LTD

*"Soluções WAF são **complexas**.* Com a escassez de profissionais qualificados e experientes, as empresas devem considerar o ***tempo*** e os ***recursos*** necessários para instalar, manter e ajustar a solução de maneira adequada. ***Não fazer*** isso pode resultar em produtos não atingirem seu potencial de ***segurança total***"

Web Application Firewall comparative analysis Total Cost of Ownership (TCO)
NSS Labs

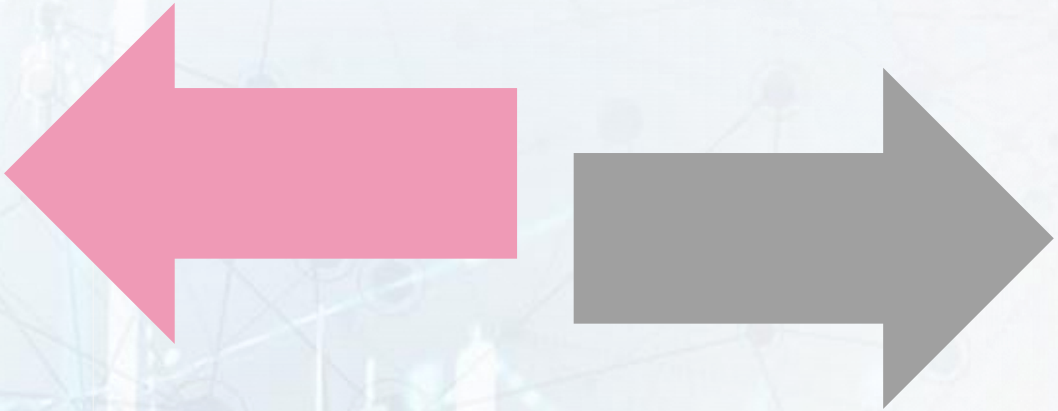
Realidade dos Falso Positivos

Check Point
SOFTWARE TECHNOLOGIES LTD

“Lidando com falsos positivos e recursos avançados

Estamos nos esforçando para reduzir o número de falsos positivos (falsos alertas) na instalação padrão. No entando, mais cedo ou mais tarde, você pode encontrar falsos positivos” https://modsecurity.org/crs

Duas Abordagens Opostas para Falsos Positivos



OWASP® Top 10 Web App Risks

1. Injection

2. Broken Authentication

3. Cross-Site Scripting (XSS)

WAAP - Proteção contra os Vetores de Ataque

OWASP top 10
e ataques avançados

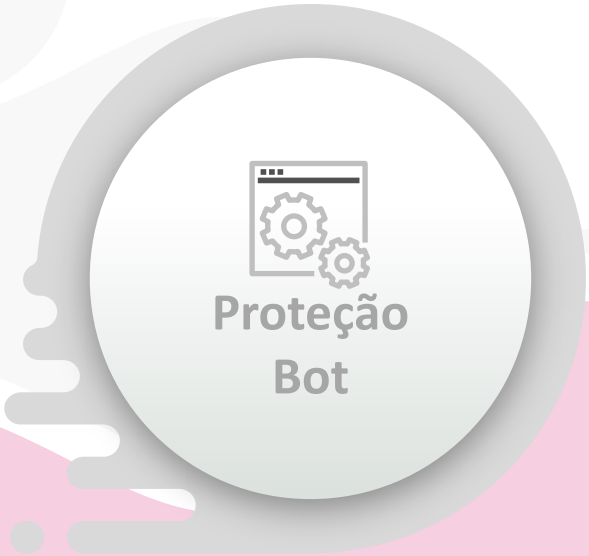
Validação
Template

Distinção entre
humanos e *Bots*

WAAP - Proteção contra os Vetores de Ataque

OWASP top 10
e ataques avançados

Validação
Template



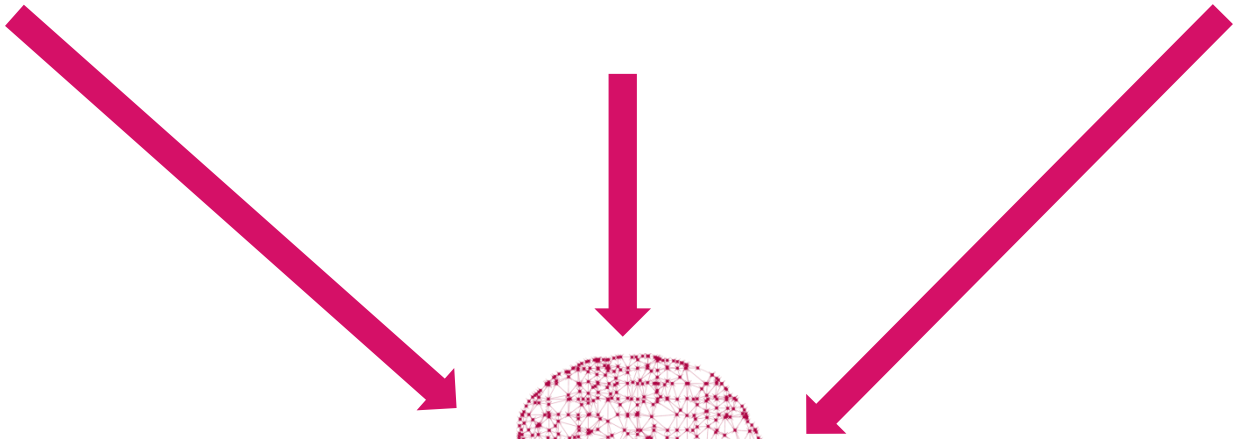
Distinção entre
humanos e *Bots*

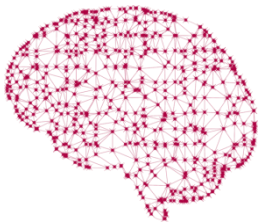
Inteligência Artificial - Análise

Pontuação para Indicadores

Reputação do Usuário

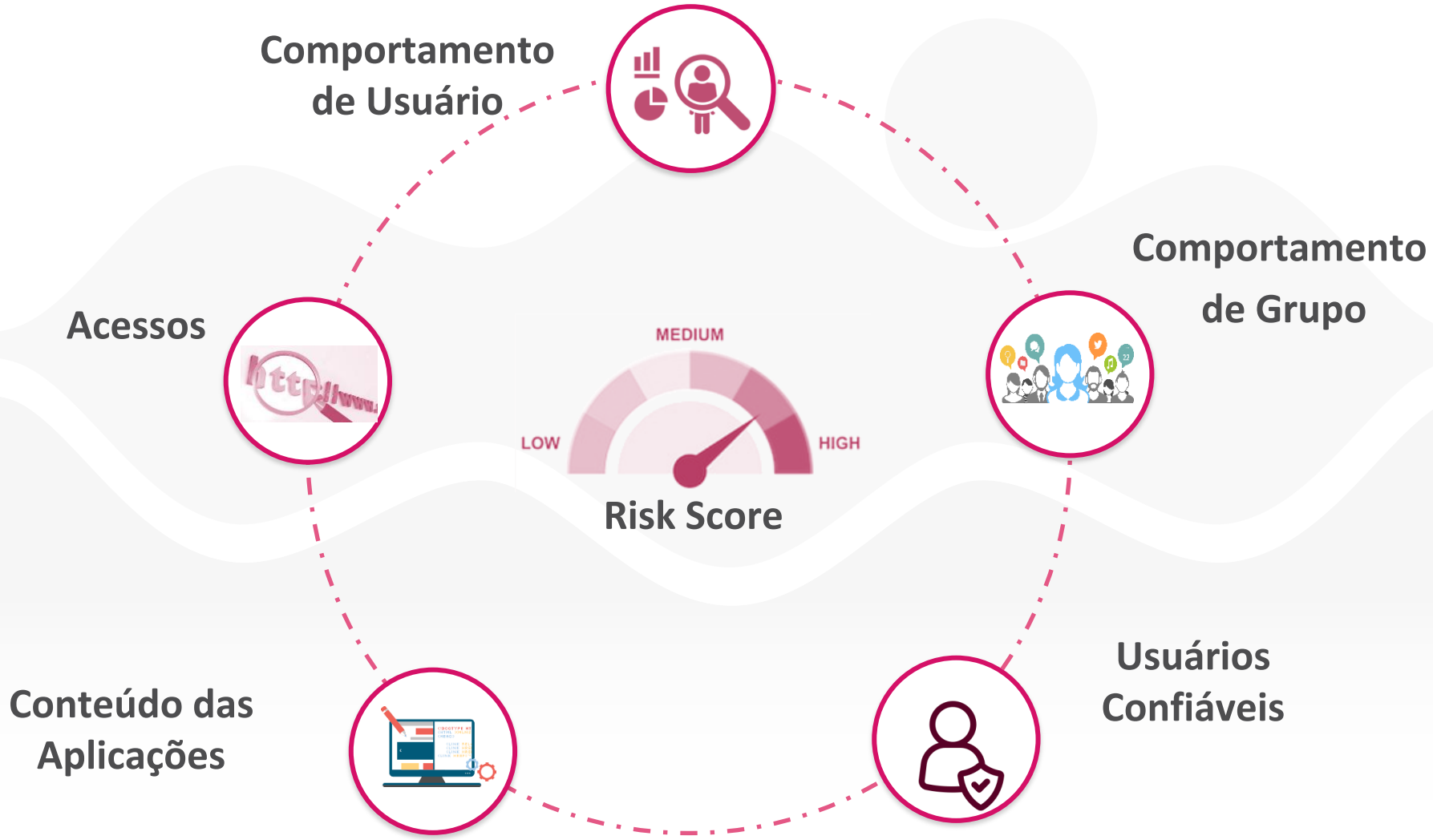
Reconhecimento das Aplicações



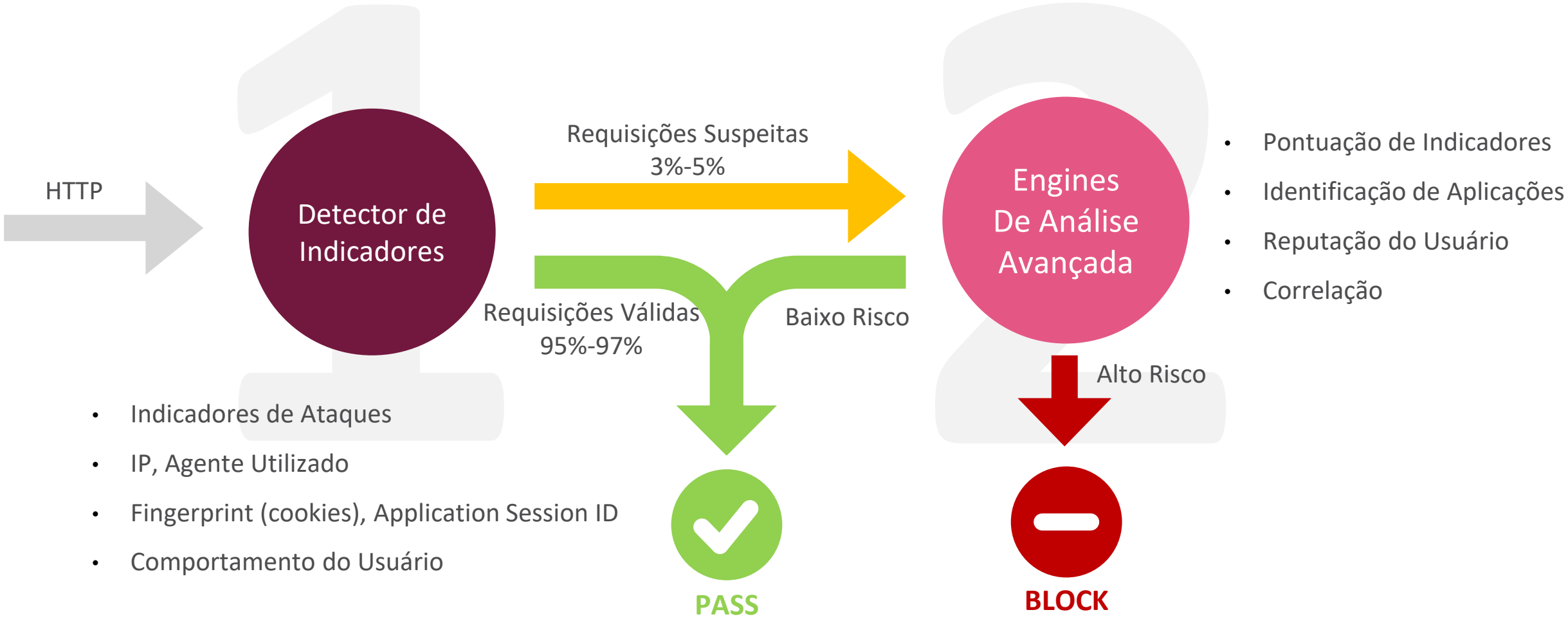


Avaliação Geral de Risco

Entrando em detalhes - Análise Contextual



Estágios da Análise – Machine Learning



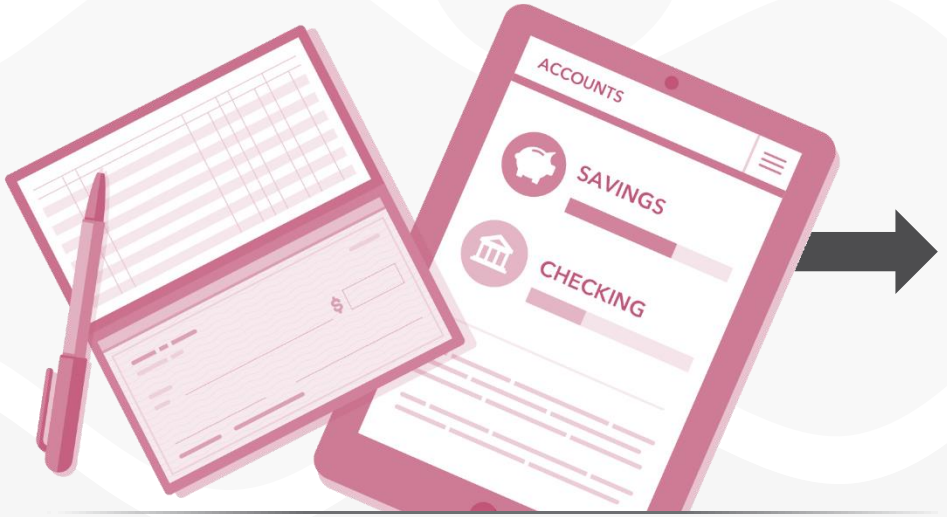
- Indicadores de Ataques
- IP, Agente Utilizado
- Fingerprint (cookies), Application Session ID
- Comportamento do Usuário

- Pontuação de Indicadores
- Identificação de Aplicações
- Reputação do Usuário
- Correlação

Exemplificando

George

John



Requisição do John é bloqueada

Mesma requisição – mas John enviou requisições suspeitas no passado

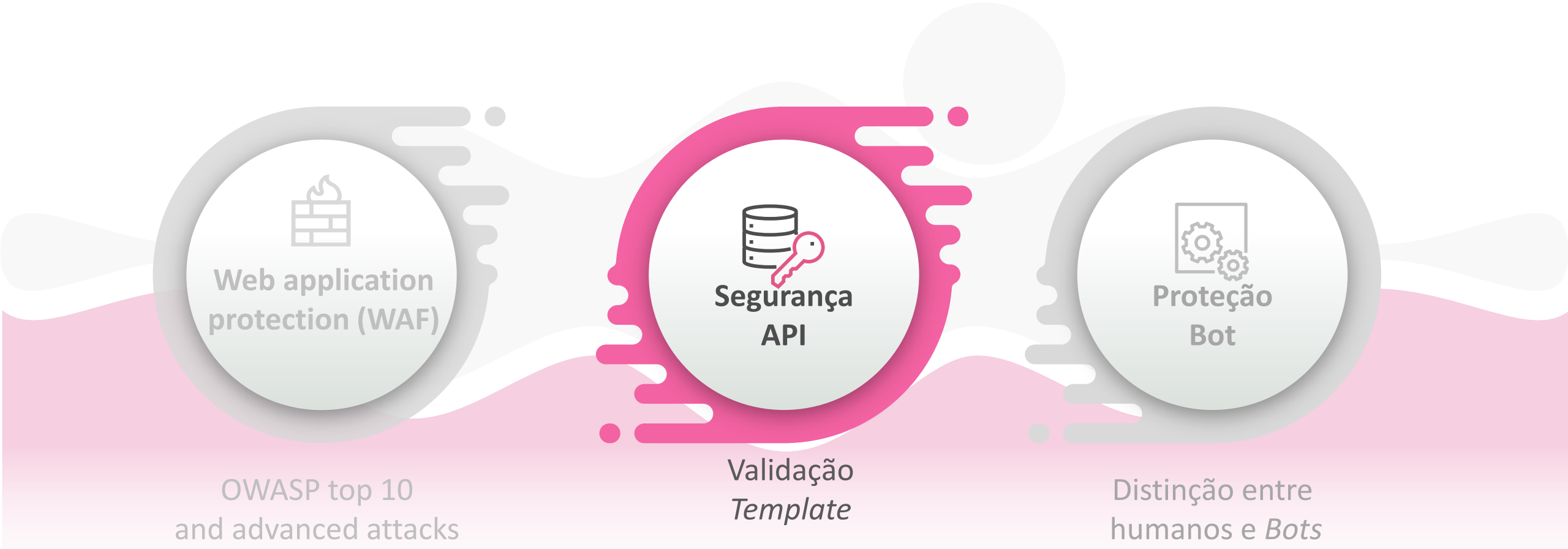
WAAP - Proteção contra os Vetores de Ataque

OWASP top 10
e ataques avançados

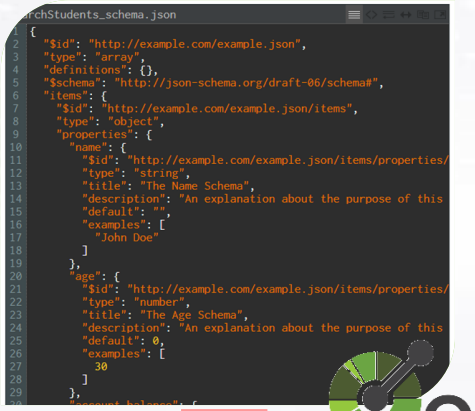
Validação
Template

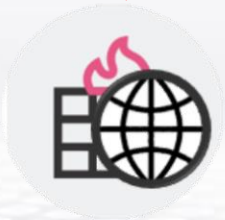
Distinção entre
humanos e *Bots*

WAAP - Proteção contra os Vetores de Ataque



Segurança para API: Validação

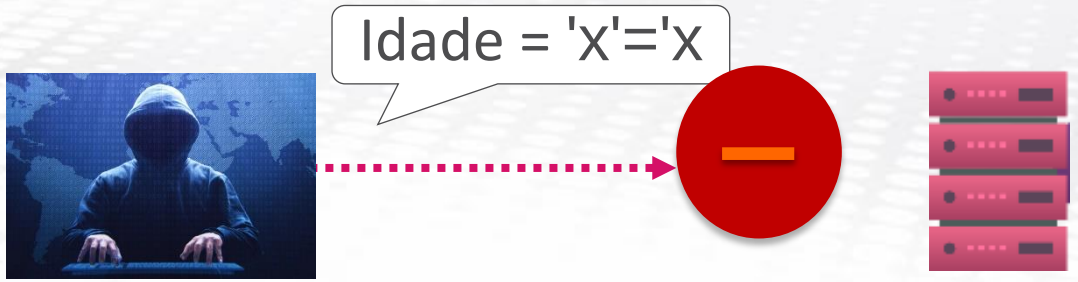




Criação de Whitelist para campos e valores

Exemplo – Valor do campo “Idade”

```
"age": {
  "$id": "http://example.com/example.json/items/properties/
  "type": "number",
```



WAAP - Proteção contra os Vetores de Ataque

OWASP top 10
e ataques avançados

Validação
Template

Distinção entre
humanos e *Bots*

WAAP - Proteção contra os Vetores de Ataque

OWASP top 10
and advanced attacks

Validação
Template

Distinção entre
humanos e *Bots*

https://owasp.org/www-community/attacks/Credential_stuffing

Proteção Contra Bots

Injeção de scripts em páginas web

Coleta dos dados enviados identificando padrões

Tomada de Decisão Bot ou não

Suporte a Diversos Tipos de Workloads / Benefícios

Web Server

Reverse Proxy

API Gateway

Linux VM

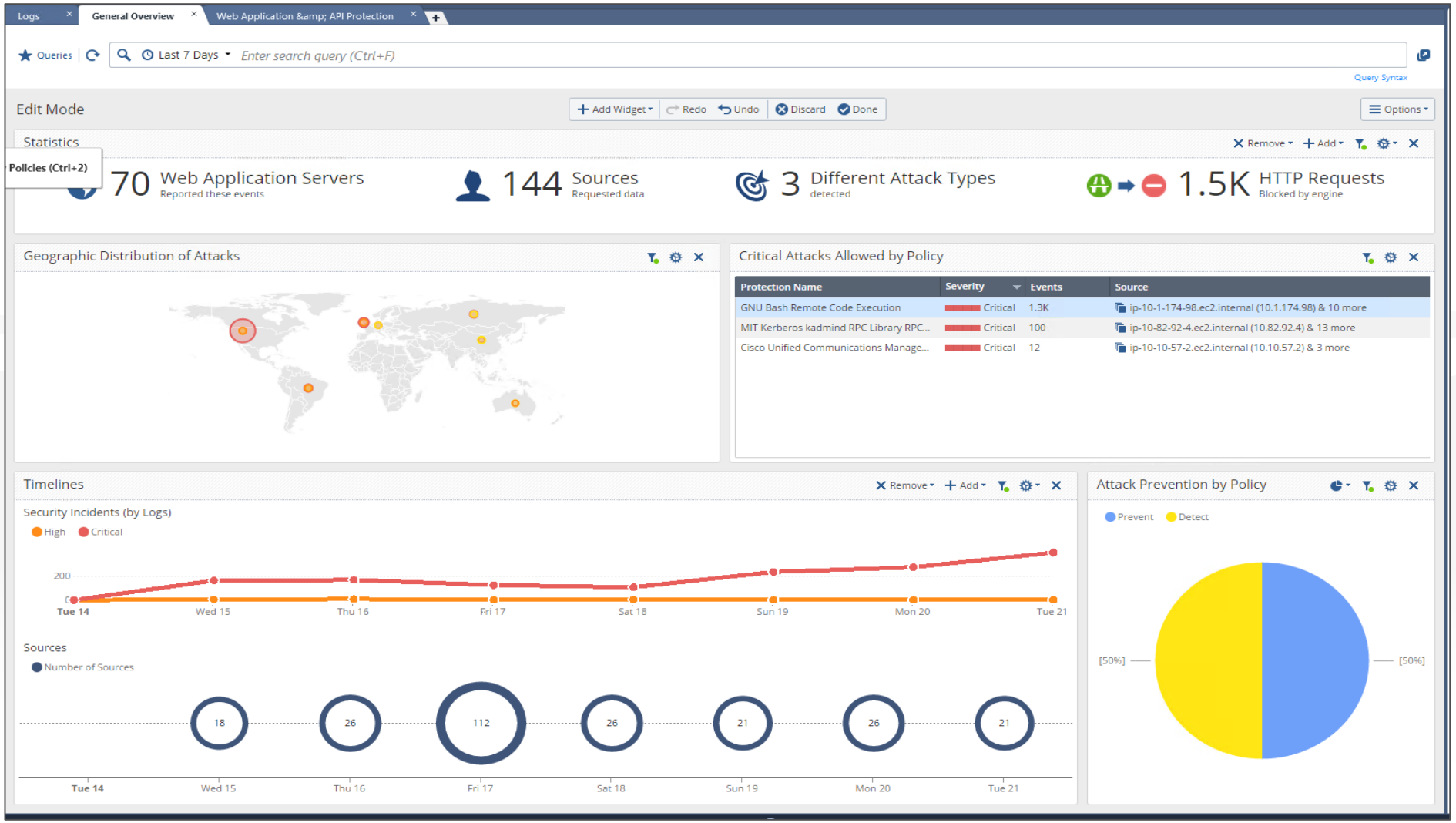
Kubernetes Ingress

POD

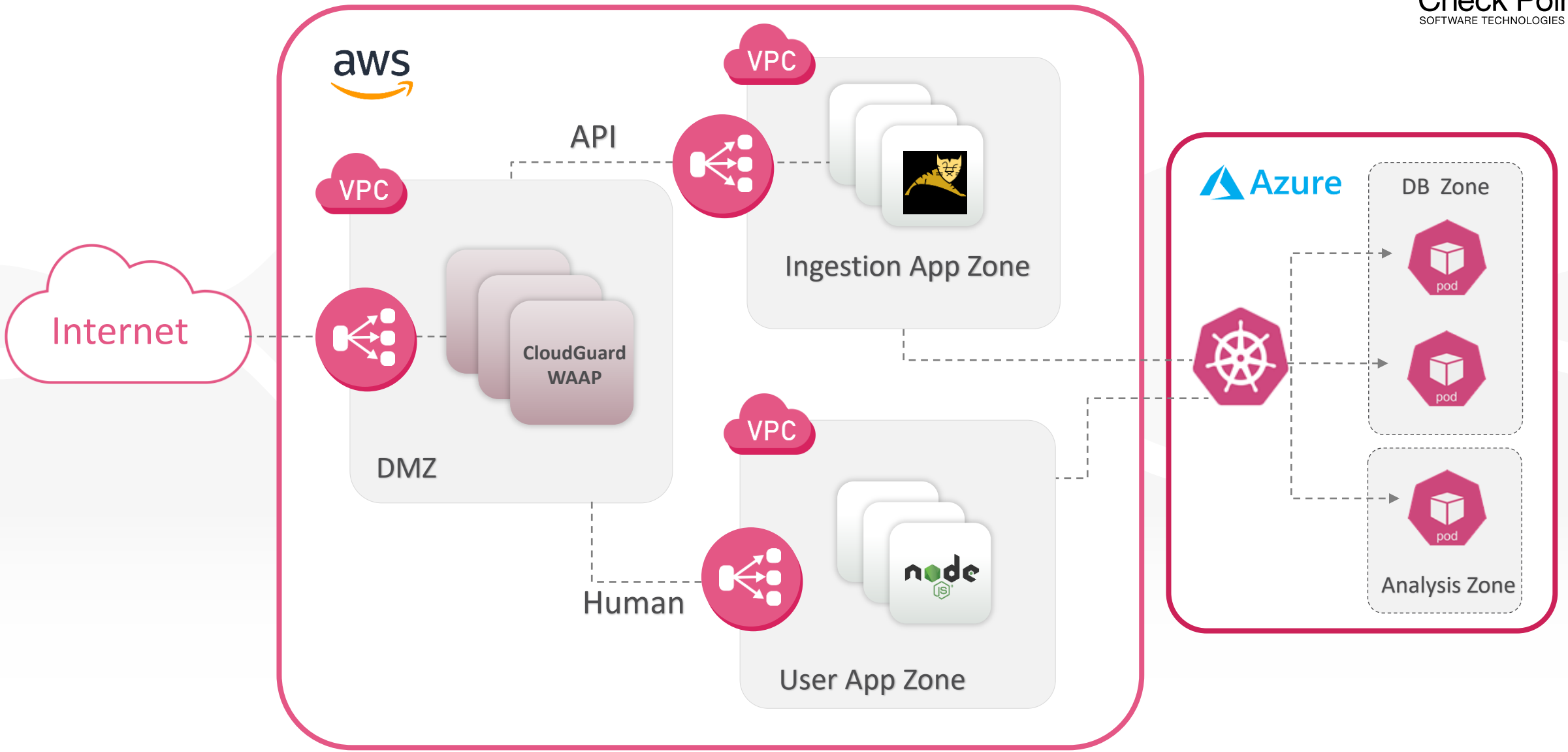
Service Mesh

Serverless

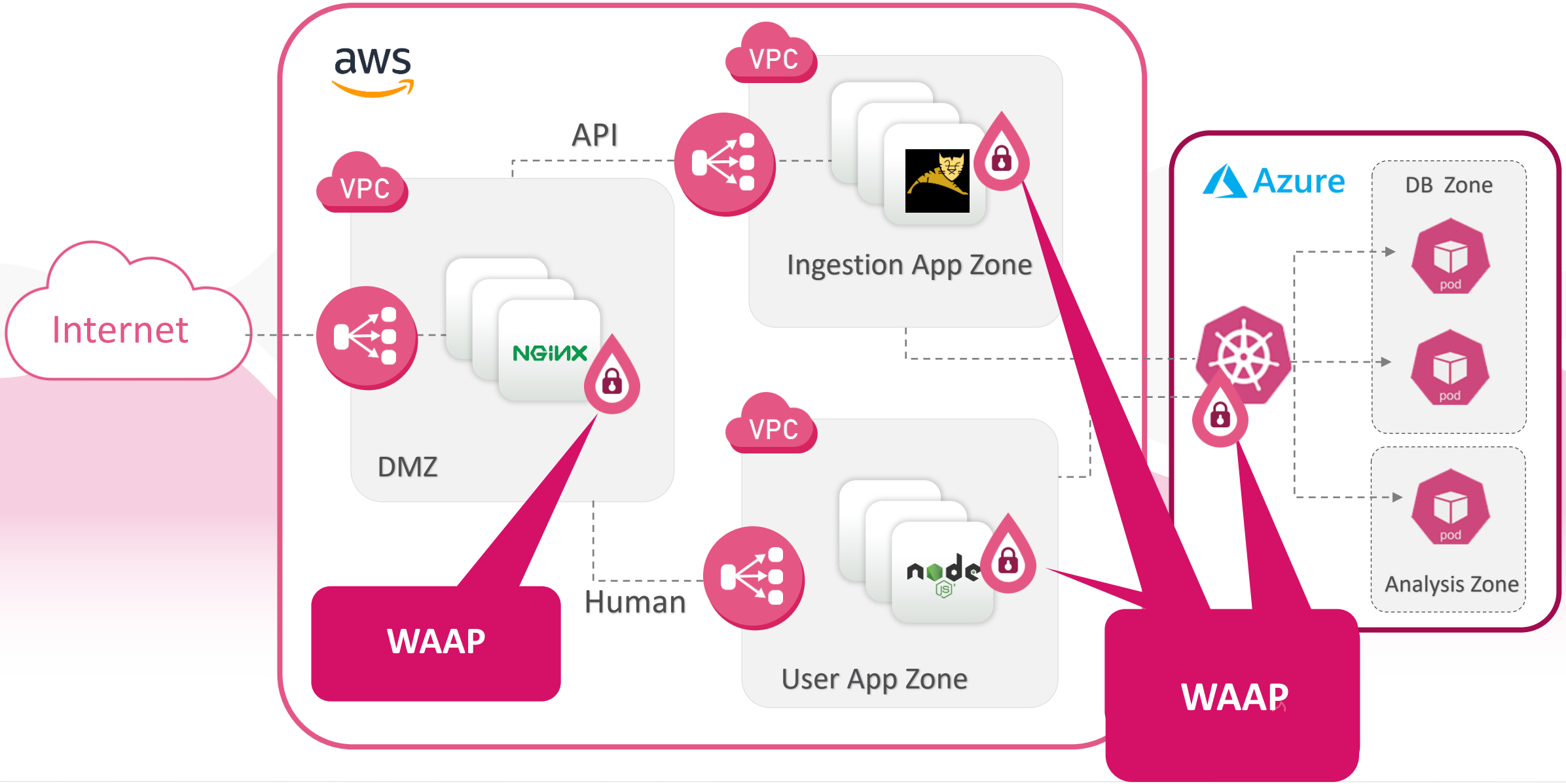
Visualização Integrada de Eventos WAAP



Casos de Uso - Design com Proxy Reverso



Casos de Uso - Design com Agentes Embarcados



CHECK POINT

CloudGuard

Segurança

Gerenciamento de postura de segurança e Proteção contra ameaças avançadas

Automático

De implantação à políticas de proteção geradas automaticamente durante CI / CD e prevenção em tempo de execução

Em Todo Lugar

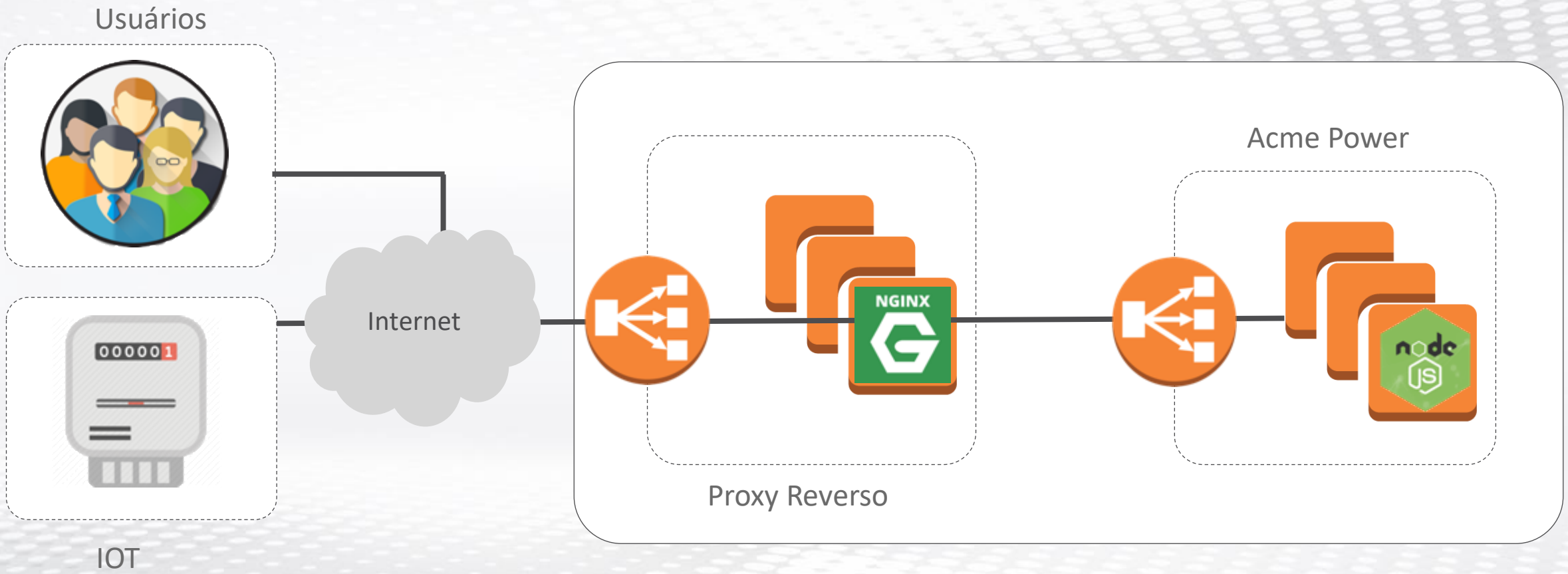
De CI / CD à produção, de nuvens privadas a públicas e em qualquer workload

UNIFIED CLOUD NATIVE SECURITY PLATFORM

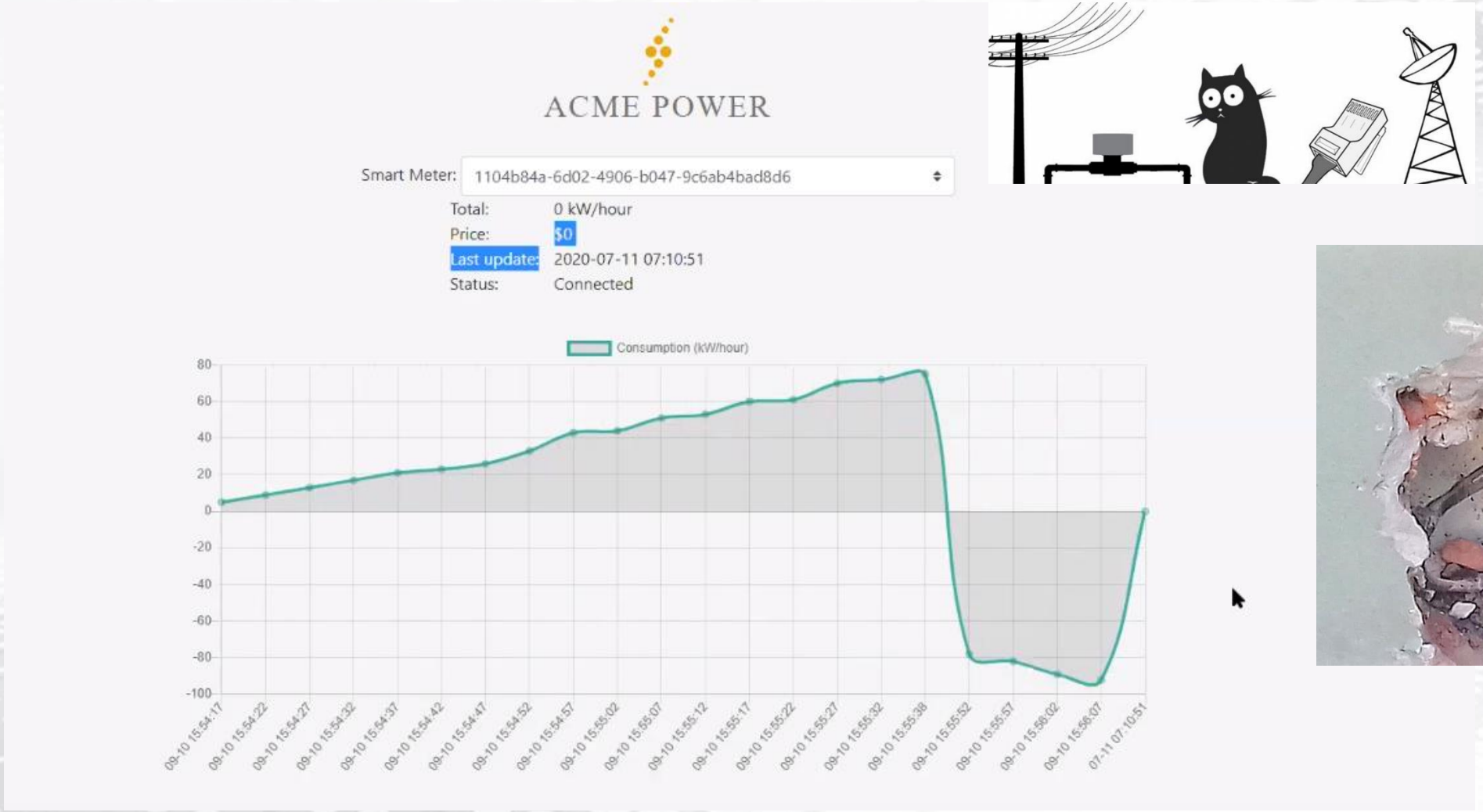
Check Point
SOFTWARE TECHNOLOGIES

DEMO

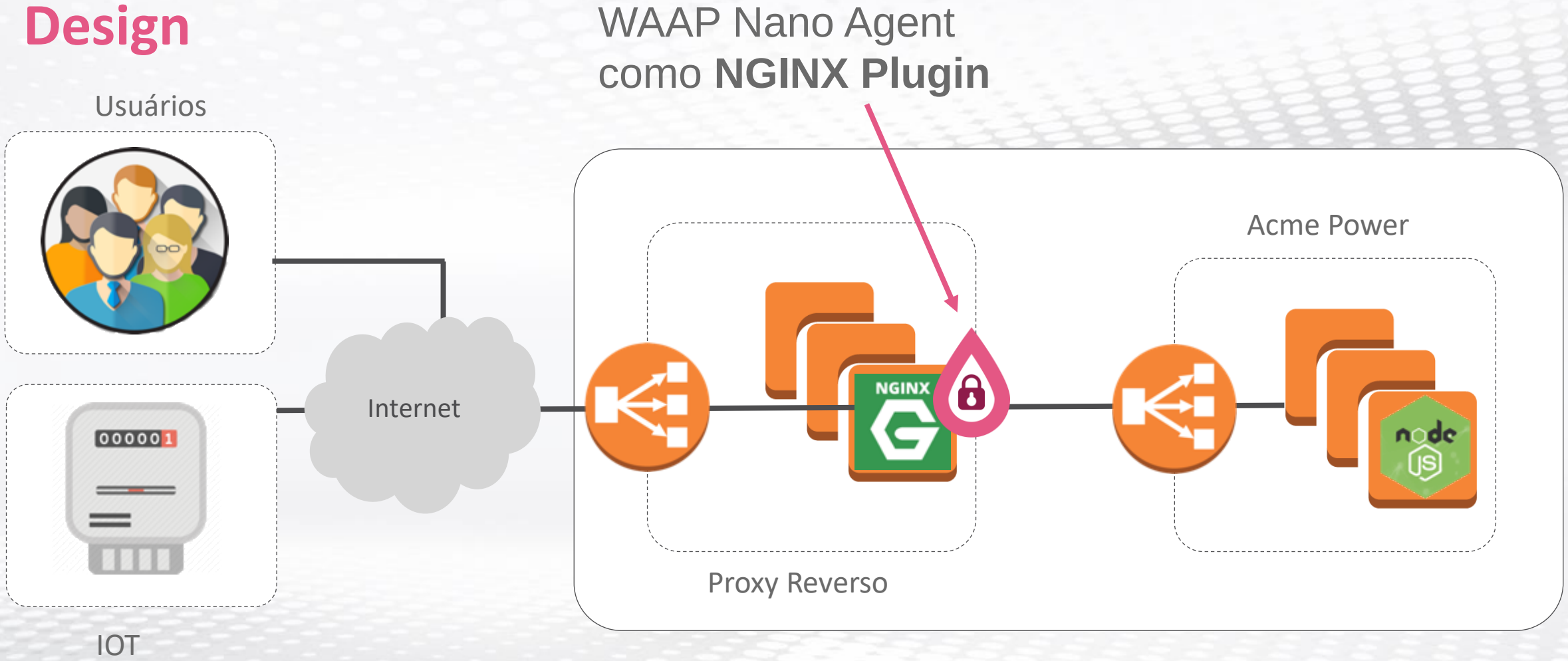
Design



Design


ACME POWER
Smart Meter: 1104b84a-6d02-4906-b047-9c6ab4bad8d6
Total: 0 kW/hour
Price: $0
Last update: 2020-07-11 07:10:51
Status: Connected
Consumption (kW/hour)
80
60
40
20
0
-20
-40
-60
-80
-100
09-10 15:54:17
09-10 15:54:22
09-10 15:54:27
09-10 15:54:32
09-10 15:54:37
09-10 15:54:42
09-10 15:54:47
09-10 15:54:52
09-10 15:54:57
09-10 15:55:02
09-10 15:55:07
09-10 15:55:12
09-10 15:55:17
09-10 15:55:22
09-10 15:55:27
09-10 15:55:32
09-10 15:55:38
09-10 15:55:52
09-10 15:55:57
09-10 15:56:02
09-10 15:56:07
07-11 07:10:51

Design


WAAP Nano Agent
como **NGINX Plugin**
Usuários
IOT
Internet
NGINX
Acme Power
Proxy Reverso

Perguntas?

Check Point®
SOFTWARE TECHNOLOGIES LTD

OBRIGADO!

Henrique Moisés – Security Engineer

José Irapuan – Security Engineer