CHECK POINT™

# ATAQUES AVANÇADOS DE DNS E PHISHING

Como o AI e Deep Learning são utilizados para proteção contra ataques avançados de DNS e Phishing

José Irapuan – Security Engineer

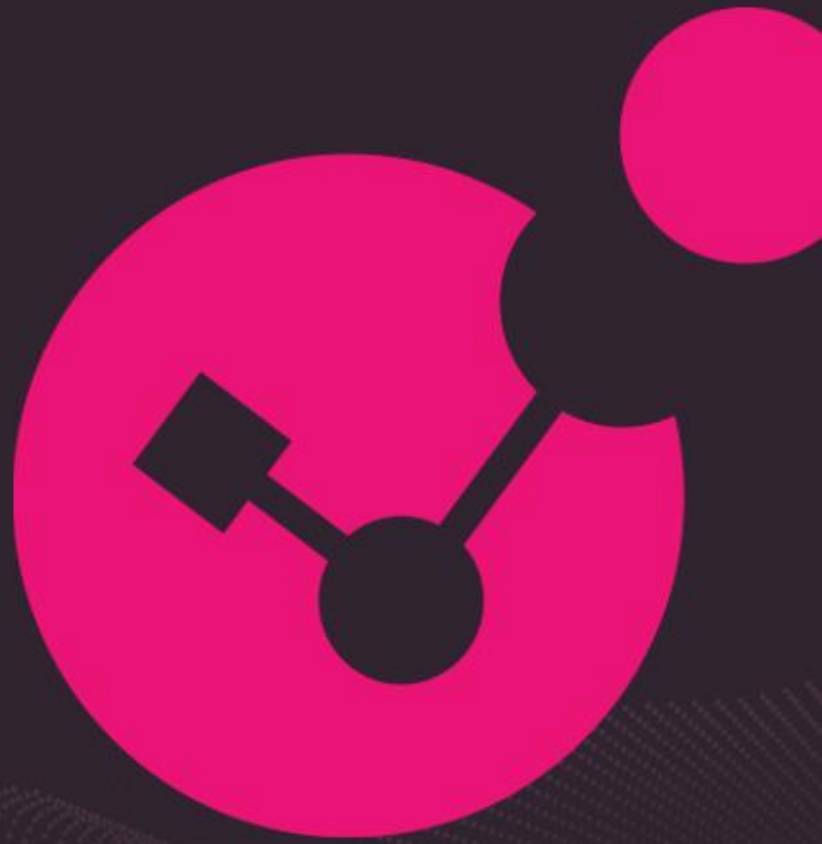
Lisandro Silva – Security Engineer

Setembro, 2023

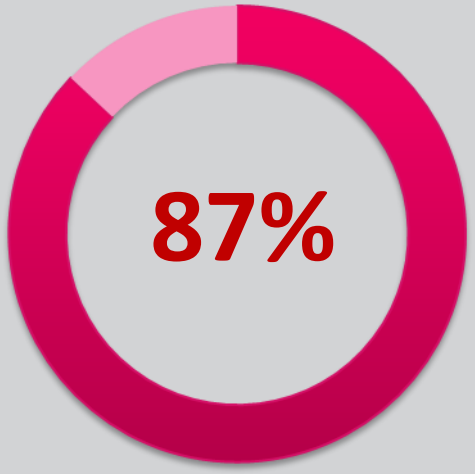
YOU DESERVE THE BEST SECURITY

# Agenda

- Características de um ataque usando DNS
- Segurança avançada para DNS
- Zero Phishing, prevenção avançada
- Demo



# CARACTERÍSTICAS DE UM ATAQUE USANDO DNS




**das organizações sofreram ataques de DNS em 2020**


**é o custo médio de um ataque de DNS**

**26% das organizações atacadas sofre roubo de dados**

**38% sofreram ataques baseados em malware**

**49% sofreram tentativas de phishing**

Fonte: Businesswire, de acordo com EfficientIP e IDC Report (Junho 2021)

# Qual é o problema com o DNS?

**Comunicação cliente-servidor não autenticada**

**A carga útil do DNS pode transportar qualquer dado**

**O tráfego DNS é permitido**

163 bilhões de solicitações + respostas de DNS

Akamai Traffic Map, 13-Sept-2022

Mais de 107 mil domínios registrados

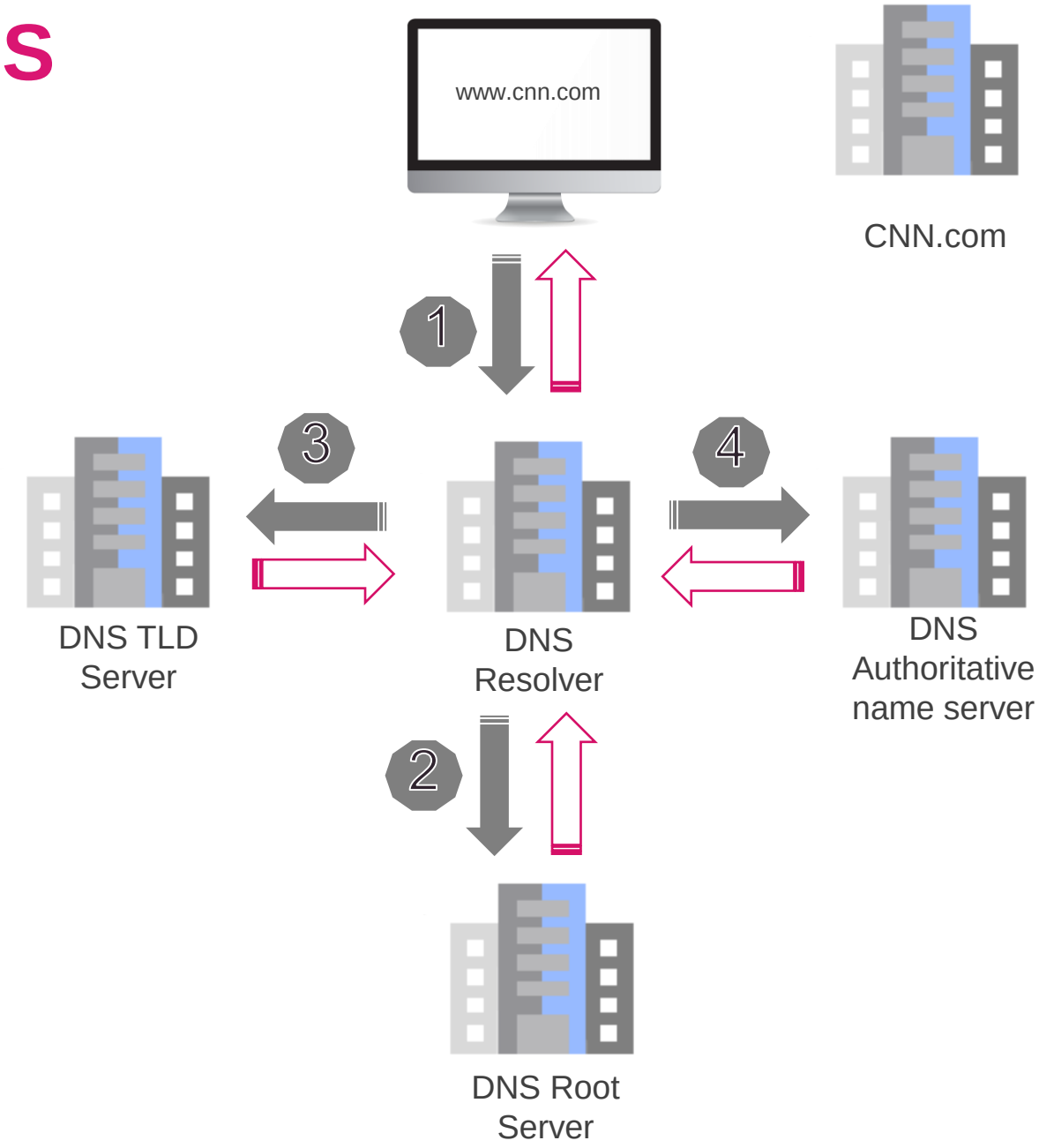
World Intellectual Property Organization, September 2022

# DNS EM POUCAS PALAVRAS

**O DNS é um protocolo da década de 1980 e é um dos blocos de construção da Internet.**

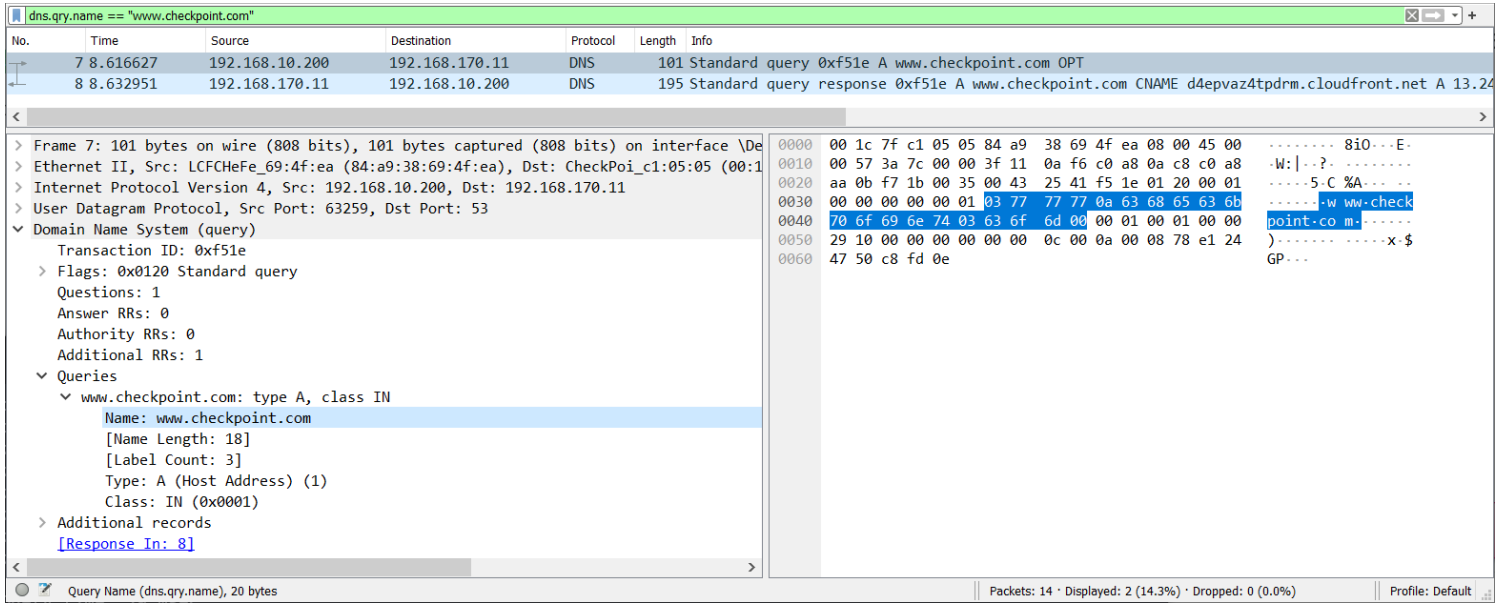
**DNS é um sistema hierárquico e descentralizado de "lista telefônica" que traduz URLs em IPs.**

**O protocolo consiste em consultas e respostas.**



# DNS EM POUCAS PALAVRAS - LIMITAÇÕES

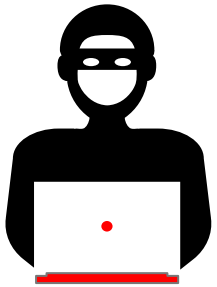
- 63 bytes de comprimento por subdomínio (rótulos)
  - Um rótulo consiste em um octeto de comprimento seguido por aquele número de octetos que representam o próprio nome
- O comprimento máximo legível de um nome DNS ASCII é de 253 caracteres
- Letras maiúsculas e minúsculas são permitidas, mas no caso do mesmo nome, são tratadas como iguais



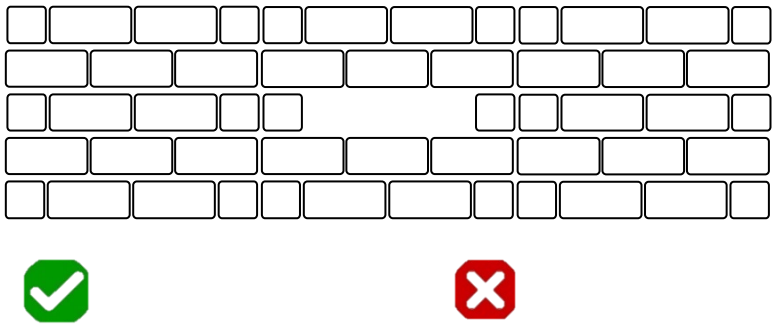

| 3 | 'w' | 'w' | 'w' | 10 | 'c' | 'h' | 'e' | 'c' | 'k' | 'p' | 'o' | 'i' | 'n' | 't' | 3 | 'c' | 'o' | 'm' | 0 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

# POR QUE O DNS É UM PONTO DE INTERESSE PARA HACKERS?

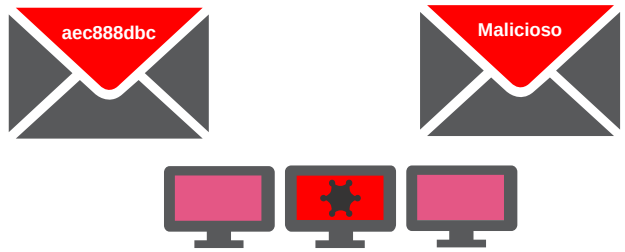
**DNS é uma forma aberta de entrar e sair da rede da organização**



**O protocolo DNS está desatualizado e precisa de medidas de segurança.**

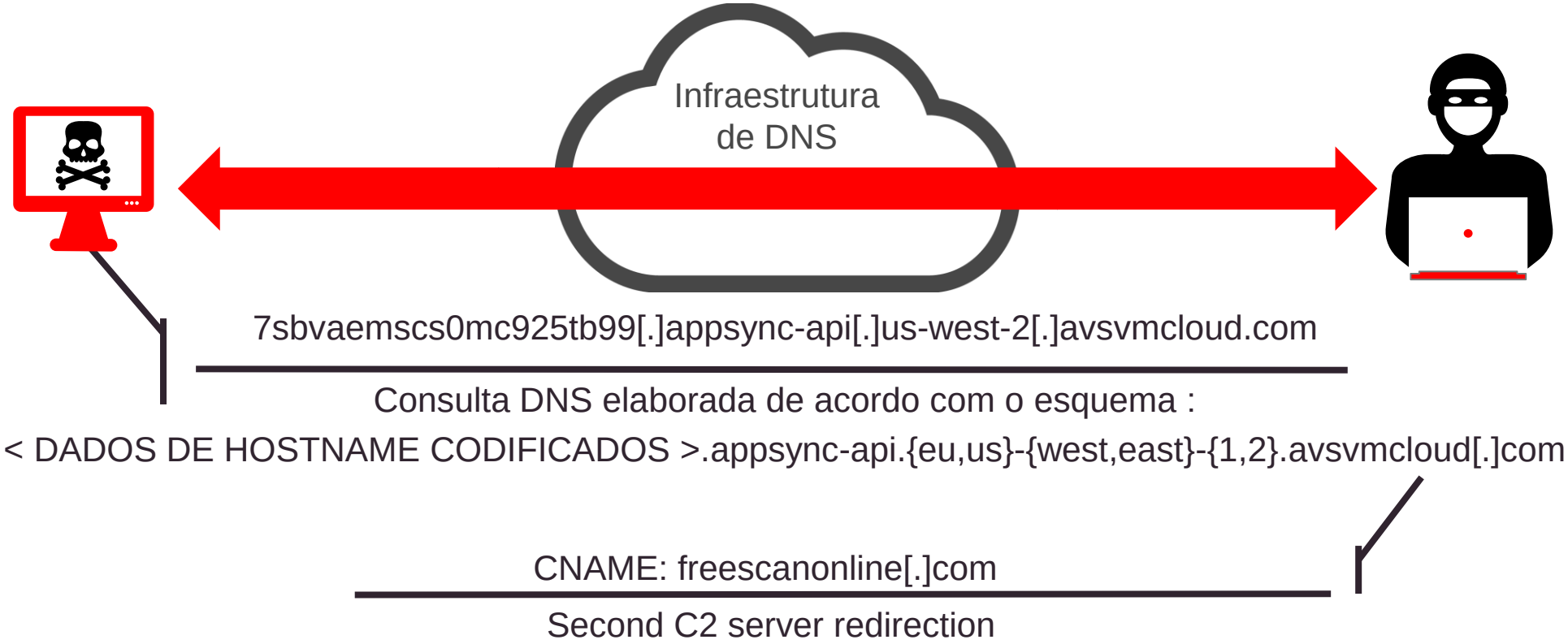


**Por estas razões, o DNS é um excelente canal para comunicação C2**



# EXEMPLO DE MALWARE AVANÇADO

## SunBurst usou tunelamento DNS para canal C2



# APROVEITANDO O DEEP LEARNING PARA PROTEGER CONTRA EXPLORAÇÕES DE DNS

# DEEP LEARNING – THE BASICS

- Comece com MUITOS dados
  - Treine os dados em uma grande quantidade de GPUs
  - Deixe a máquina aprender sem escolher recursos e poucos classificadores

| | Machine Learning | Deep Learning |
|---|---|---|
| Training dataset | Small | Large |
| Choose your own features | **Yes** | **No** |
| # of classifiers available | Many | Few |
| Training time | Short | Long |

# SEGURANÇA AVANÇADA DE DNS
## Powered by ThreatCloud

THREATCLOUD

**Base de Dados de Reputação**

Proteção contra domínios maliciosos conhecidos

**Anti bot & IPS**

Proteção contra anomalias de protocol e malware

**Análise de Malware & Feeds**

Proteção Pró-ativa

**Engines de Deep Learning**

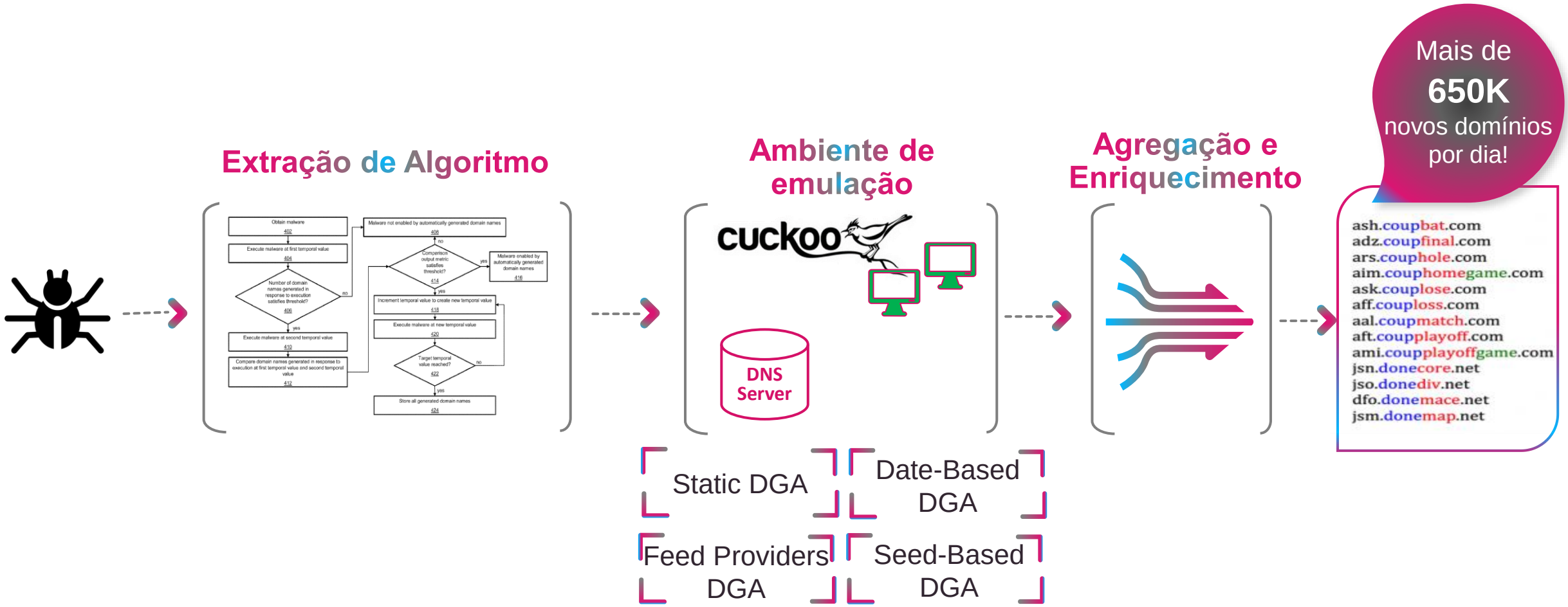
Proteção Zero-day

**Zero Phishing**

Proteção Anti-Phishing Inline

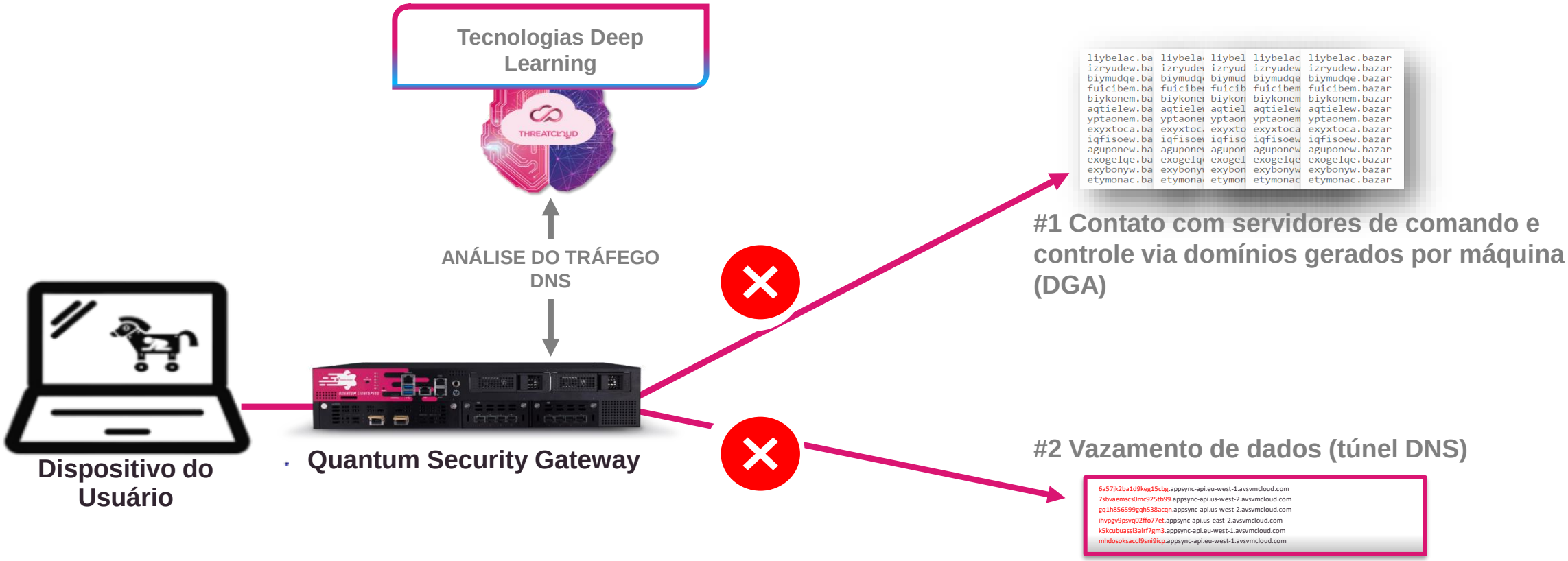
# PROTEÇÃO PROATIVA CONTRA DOMÍNIOS MALICIOSOS

Extraia DGA de malware com sistema protegido patenteado



# BLADE DE SEGURANÇA AVANÇADA PARA DNS

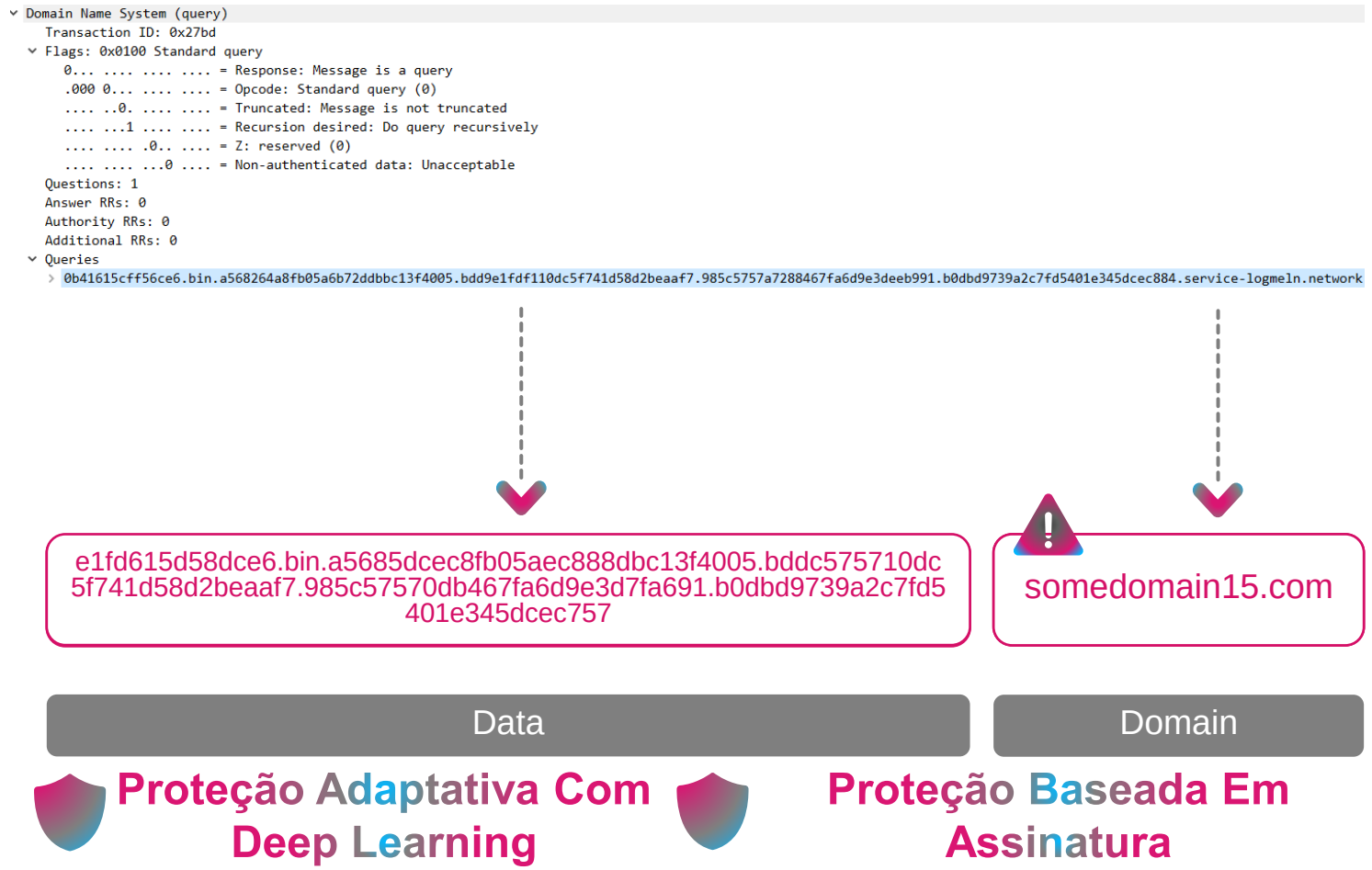
Bloqueia cinco vezes mais ataques baseados em DNS do que tecnologias baseadas em assinaturas



# CASO DE USO #1: UDPoS TUNELAMENTO DE DNS

**UDPoS é um malware PoS que se concentra no roubo de dados, principalmente informações de cartões de crédito**

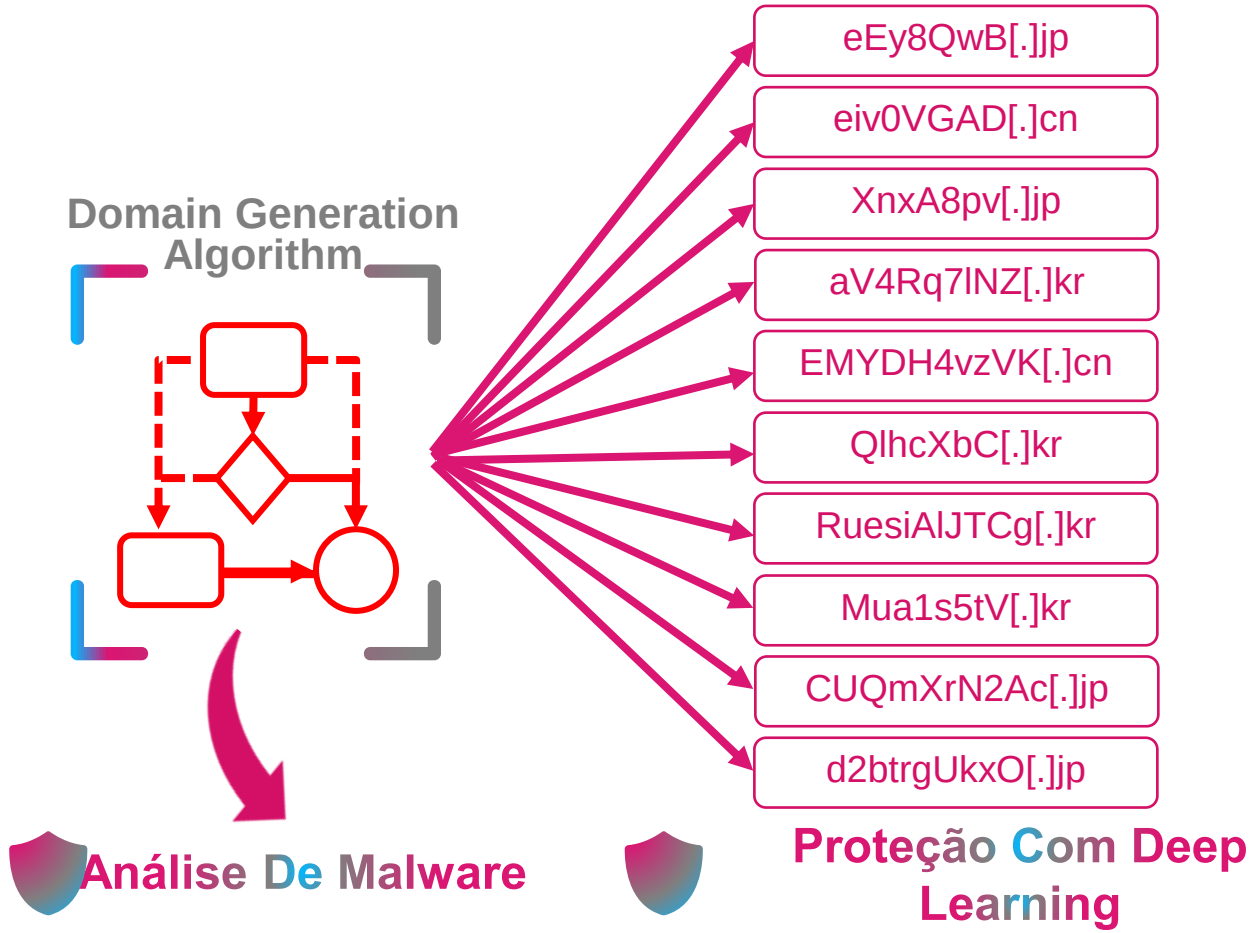
**Ele está usando servidor C2 predefinido e tunelamento DNS para exfiltrar os dados roubados e obter comandos**



# CASO DE USO #2: LEMONDUCK DGA TRAFFIC DETECTION

**LemonDuck é um malware que começou como Cryptominer e evoluiu nos últimos anos.**

**Agora é um malware multiplataforma com recursos avançados, incluindo a estrutura Cobalt Strike**



# SEGURANÇA DE DNS EM NÚMEROS

ZERO DAY PROTECTION

Tecnologia AI


Threat intelligence

PROACTIVE

cp<r>

**650K+**

Novos domínios por dia

Em menos de **1 mês**

**Dezenas**

de famílias de malware cobertas

Milhares deles são novos

**30K+**

Consultas DNS maliciosas estão sendo bloqueadas todos os dias por mecanismos de ML

**100K+**

Milhares deles são novos

Consultas DNS maliciosas estão sendo bloqueadas todos os dias pela detecção proativa

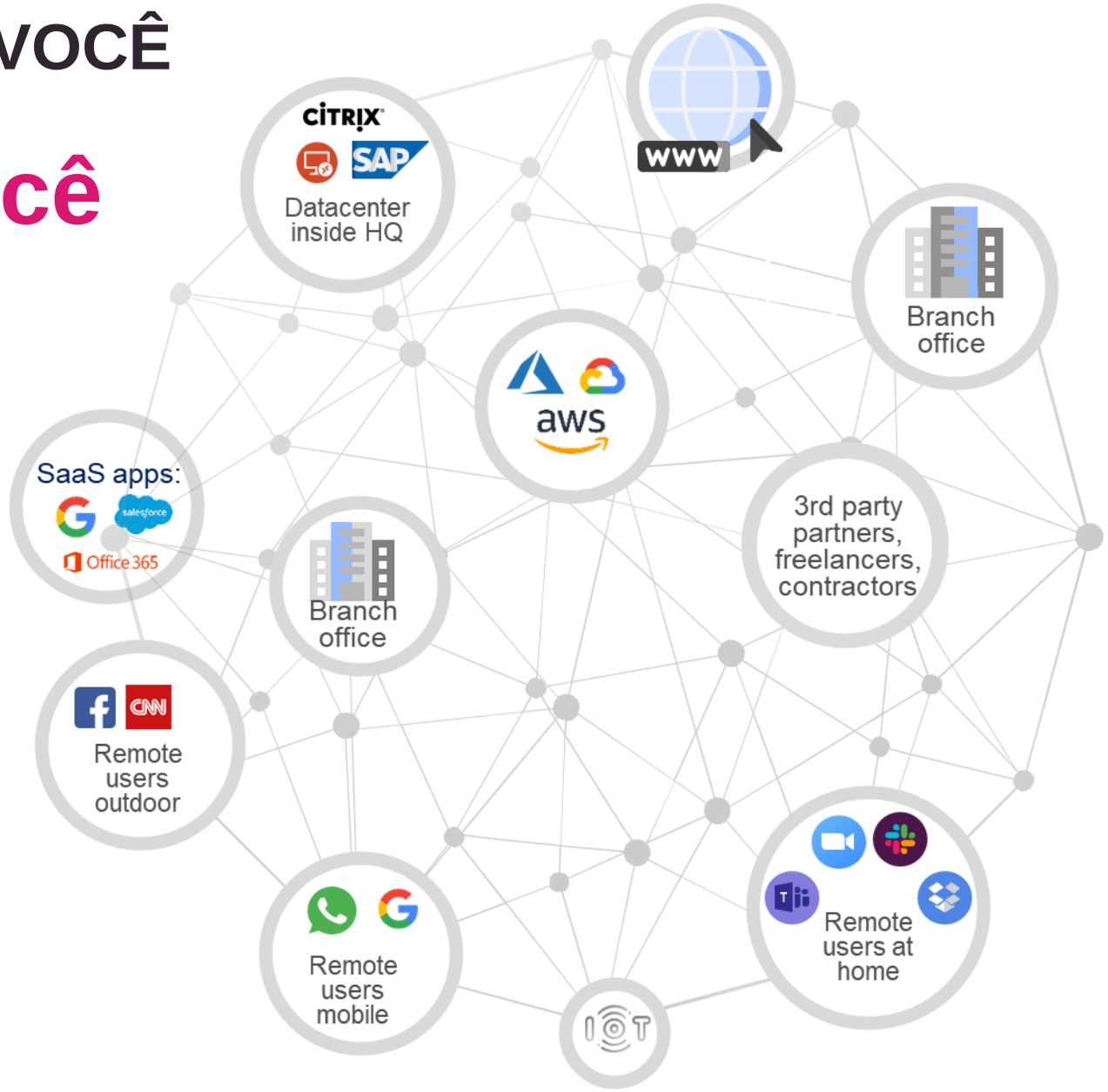
# NÃO IMPORTA QUAL PRODUTO VOCÊ ESTÁ USANDO

# Check Point protege você contra ataques DNS

**Proteção proativa**
Sistema avançado de análise de malware

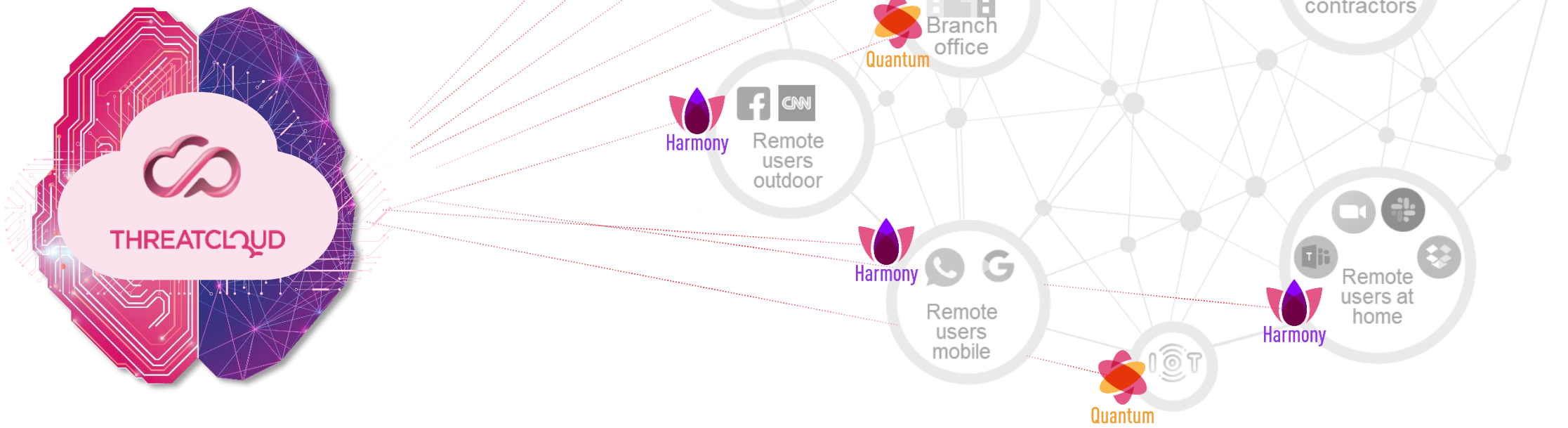
**Proteção Zero-day**
Mecanismos de aprendizado de máquina de última geração

**Proteção Anti-Phishing**
Zero Phishing com agente e sem agente em tempo real



# NÃO IMPORTA QUAL PRODUTO VOCÊ ESTÁ USANDO

# Check Point protege você contra ataques DNS

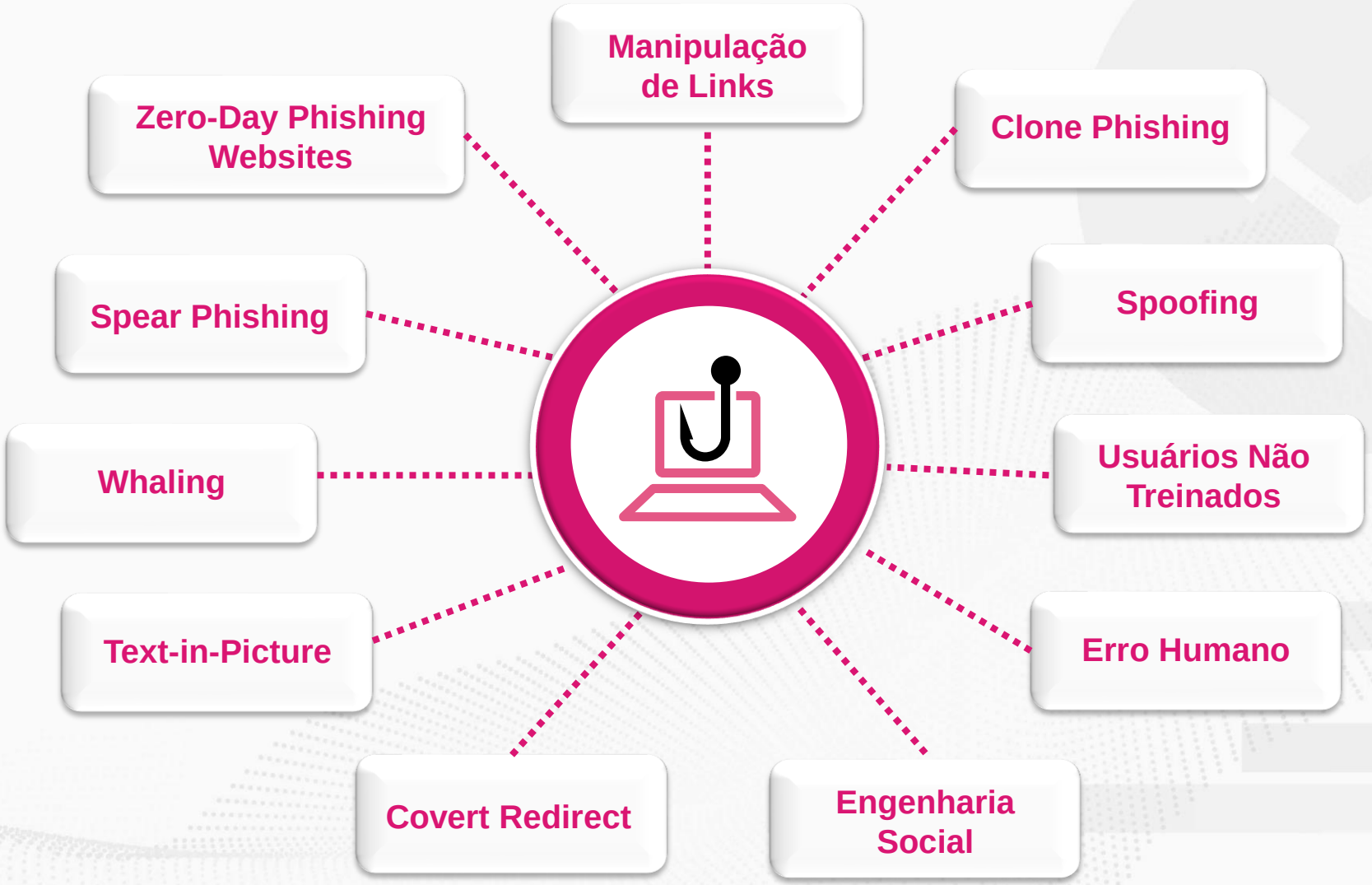


# ZERO PHISHING
# PREVENÇÃO AVANÇADA

# O QUE É ZERO PHISHING?

- A proteção Zero Phishing é alimentada por tecnologias patenteadas para evitar ataques de phishing de dia zero em sites.
- A proteção é realizada no Security Gateway, o que o torna independente de navegador e plataforma e não depende de uma solução de segurança de e-mail*
- Esta proteção está incluída no pacote de licença NGTX

# PORQUE PHISHING NECESSITA DE PREVENÇÃO



# ZERO-PHISHING – FLUXO DETALHADO

Rob

1

GET facebookscam.com

Check Point Gateway

2

GET facebookscam.com

**facebookscam.com**

3

Response

5

Resposta editada com injeção de JScript

4

Phishing URL?

6

Phishing?

7

**Phishing!**

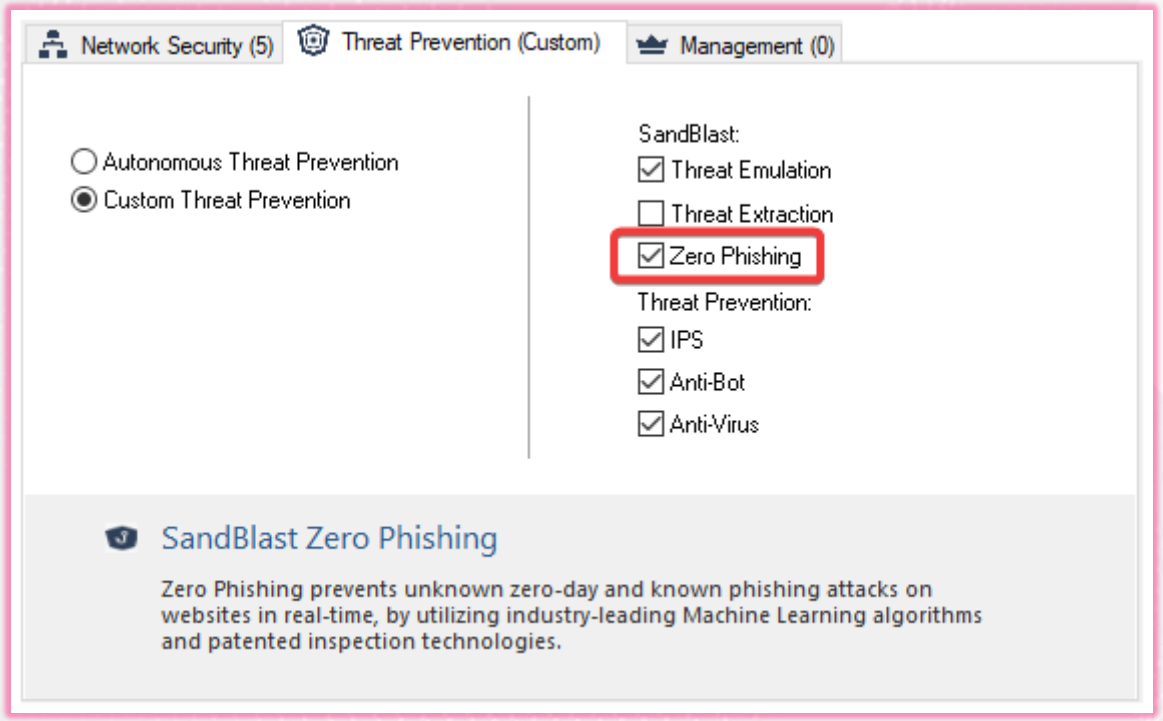
**Check Point Cloud Zero Phishing**



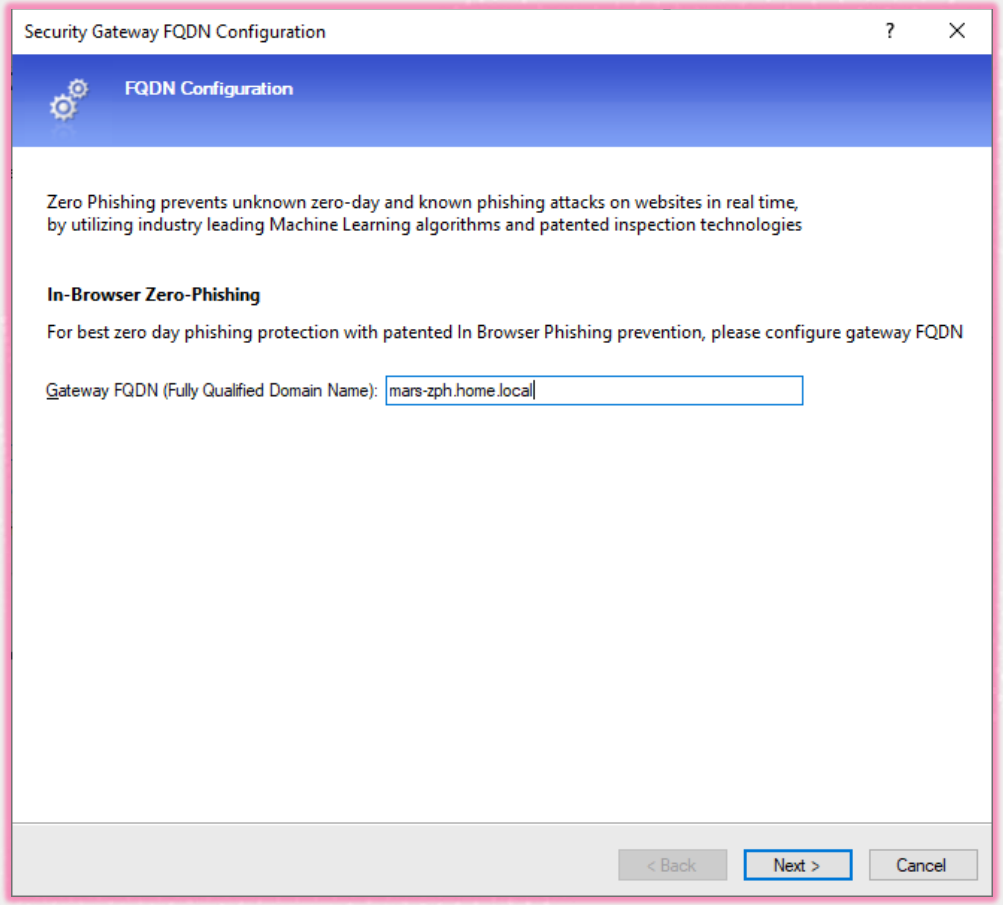
# ZERO-PHISHING – ATIVAÇÃO DA BLADE

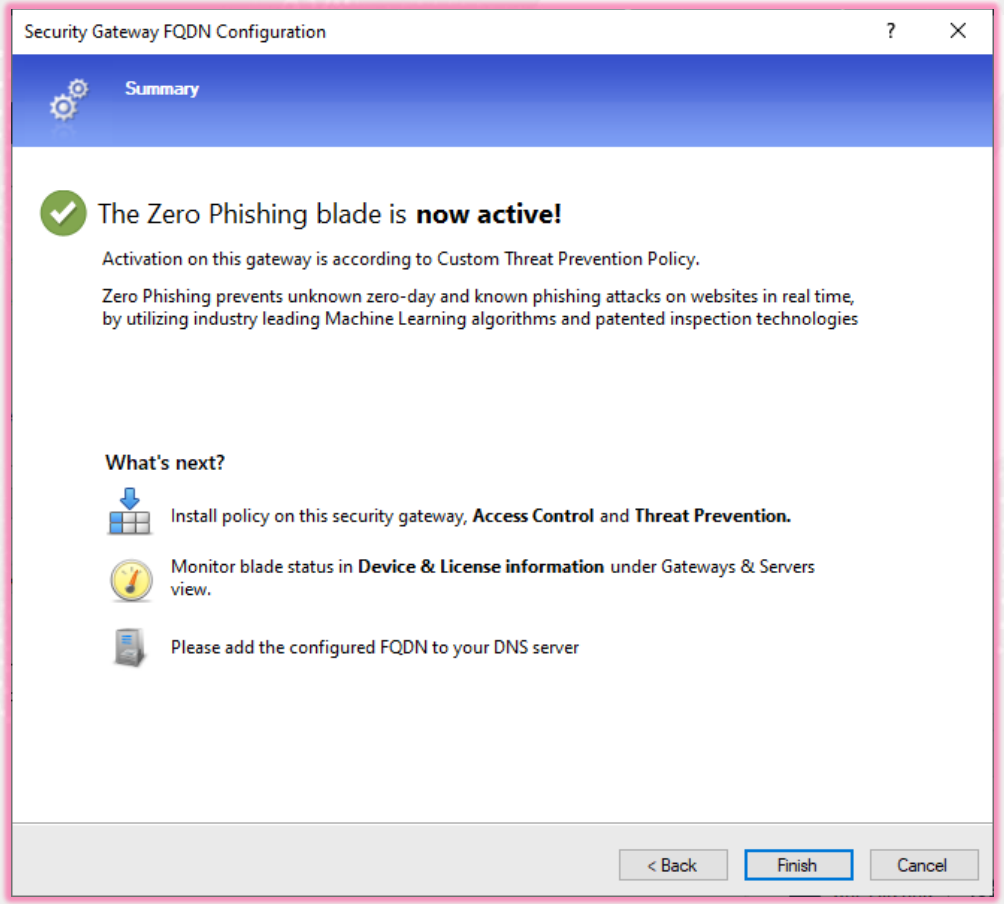
- Em *Custom Threat Prevention*, ativar *Zero Phishing*



# ZERO-PHISHING – ATIVAÇÃO DA BLADE

- Seguir os passos do wizard
  - Escolha o FQDN que não é usado no GW. O servidor DNS (usado pelo GW e clientes) precisa apontar para o IP correto do GW. Em seguida, instale políticas.



# ZERO-PHISHING - ATP

- Com o uso do ATP (Autonomous Threat Prevention), o recurso já fica ativo por padrão nos perfis Perimeter (recomendado) e Strict (URL em tempo real).

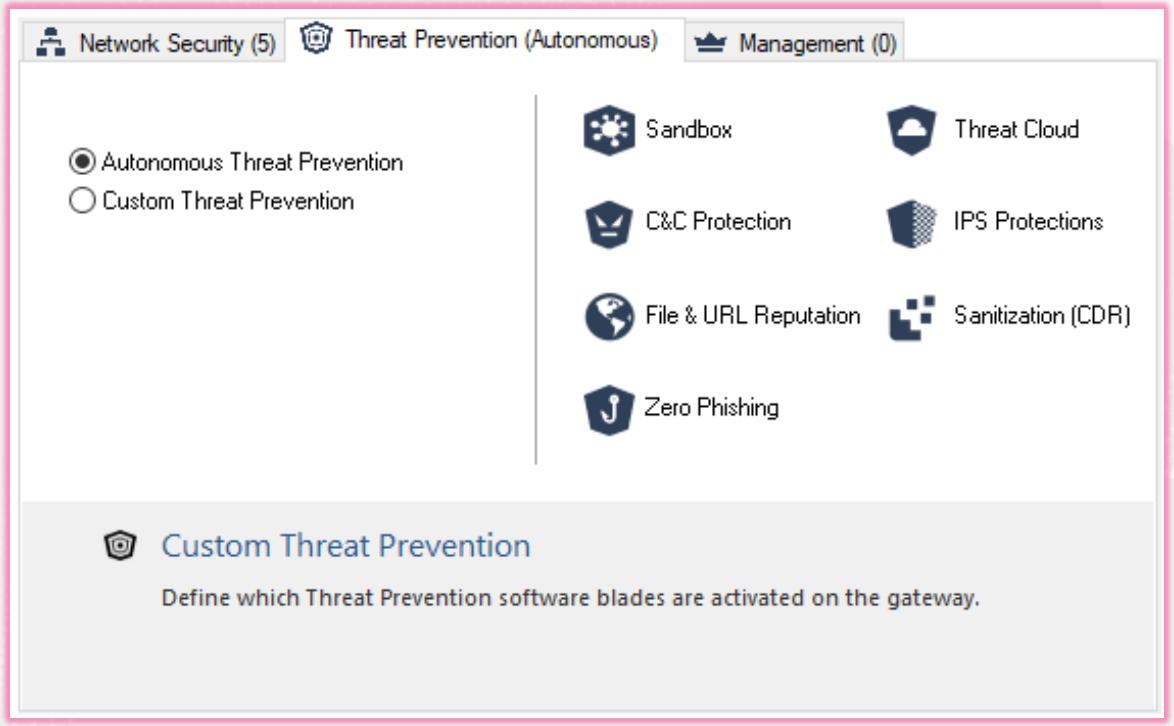
- Só é preciso configurar o FQDN no objeto Gateway na guia Zero-Phishing. Isso é necessário para que a proteção Zero Phishing no navegador funcione corretamente.

- O Zero Phishing no navegador está desativado por padrão em todos os perfis. Precisa de ativação!

**Notes:** https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_ThreatPrevention_AdminGuide/Content/Topics-TPG/Configuring_Zero_Phishing_Settings-Autonomous_Threat_Prevention.htm

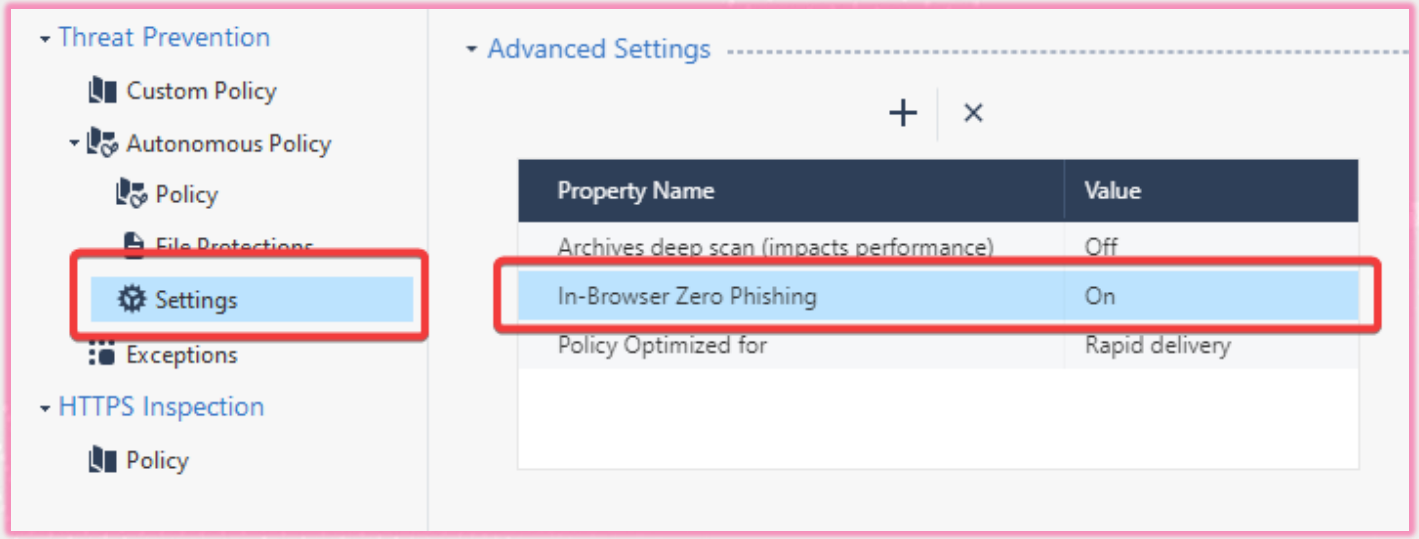
# ATIVANDO A PREVENÇÃO AUTÔNOMA DE AMEAÇAS ZERO-PHISHING

- Se a inspeção HTTPS estiver inativa, nenhuma ação adicional será necessária
- Se a Inspeção HTTPS estiver ativa, o novo portal requer um certificado, que será gerado automaticamente
- Vá para a guia Zero-Phishing no GW e configure o FQDN

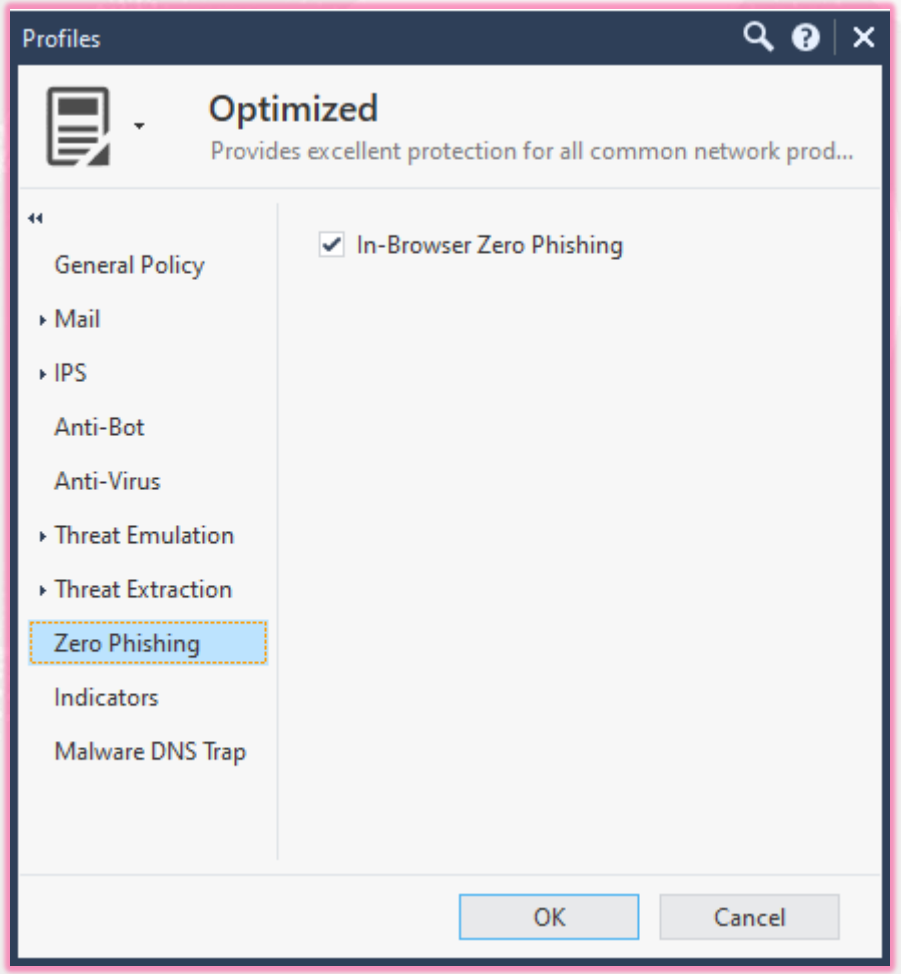


# COMO ATIVAR/DESATIVAR ZERO-PHISHING NO NAVEGADOR

## Autonomous Threat Prevention



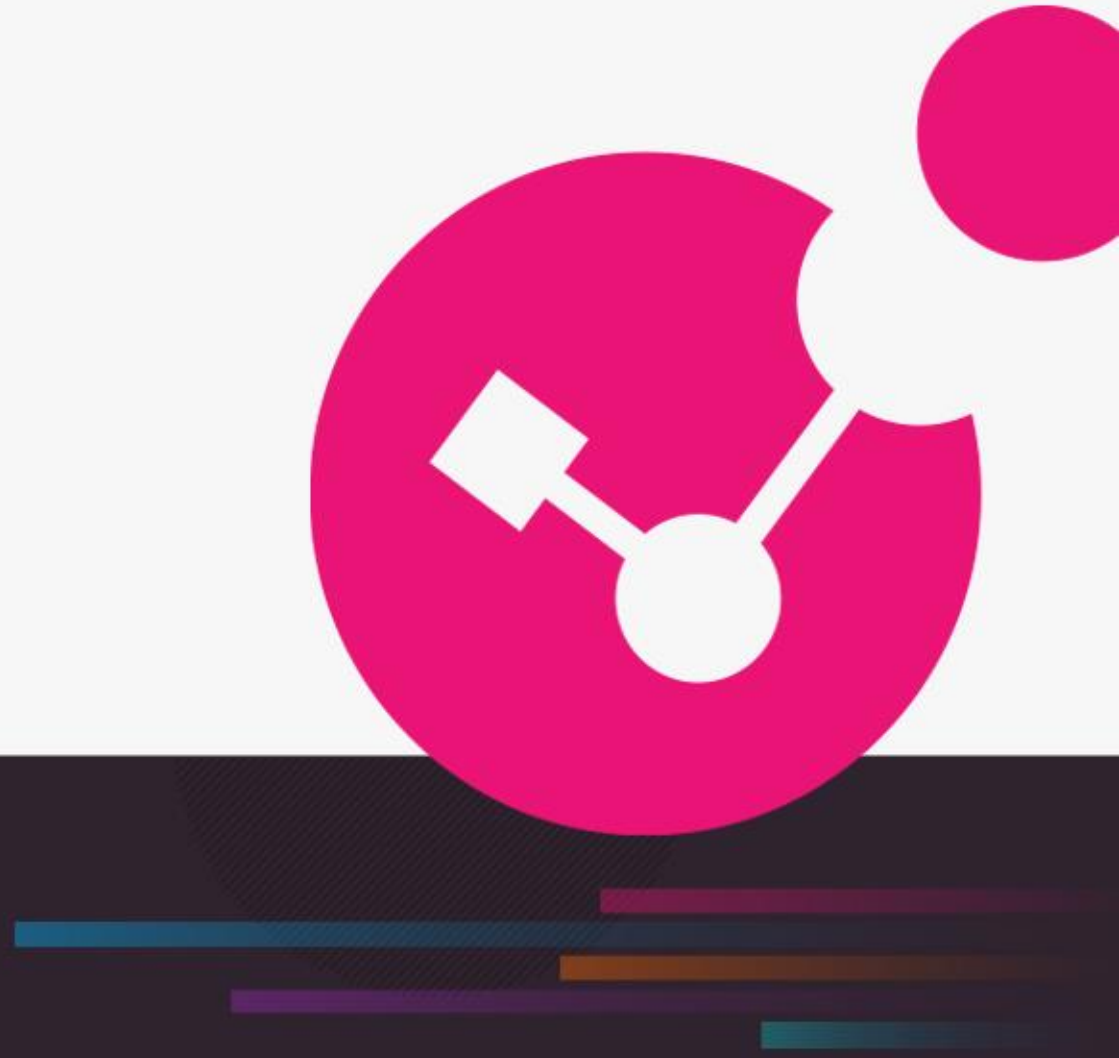

## Custom Threat Prevention



# DEMO

CHECK POINT™

# Obrigado!



YOU DESERVE THE BEST SECURITY