



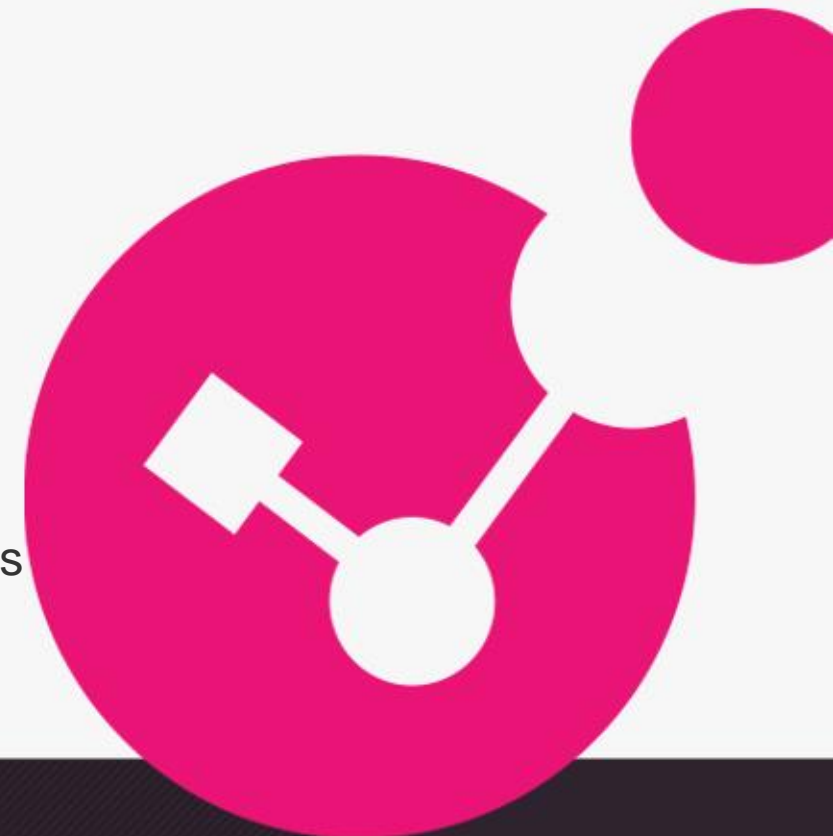
# ATAQUES AVANÇADOS DE DNS E PHISHING

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

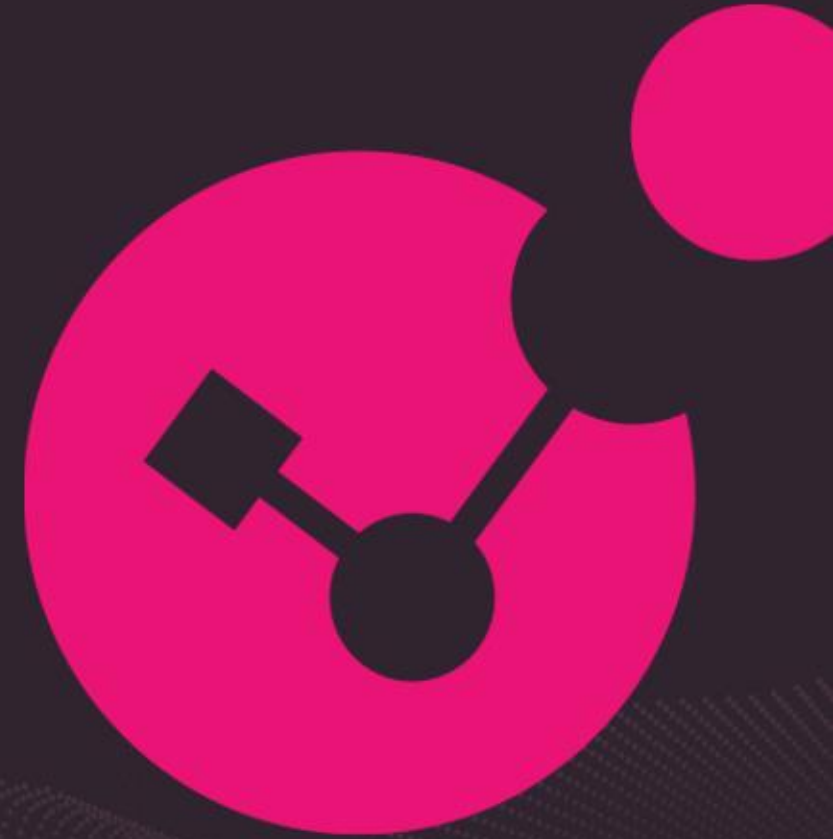
Setembro, 2023



YOU DESERVE THE BEST SECURITY

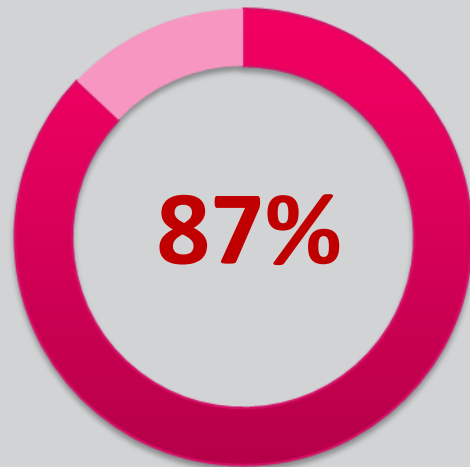
# Agenda

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



# **CARACTERÍSTICAS DE UM ATAQUE USANDO DNS**





**87%**  
das organizações  
sofreram ataques  
de DNS em 2020



**\$950K**  
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

## 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

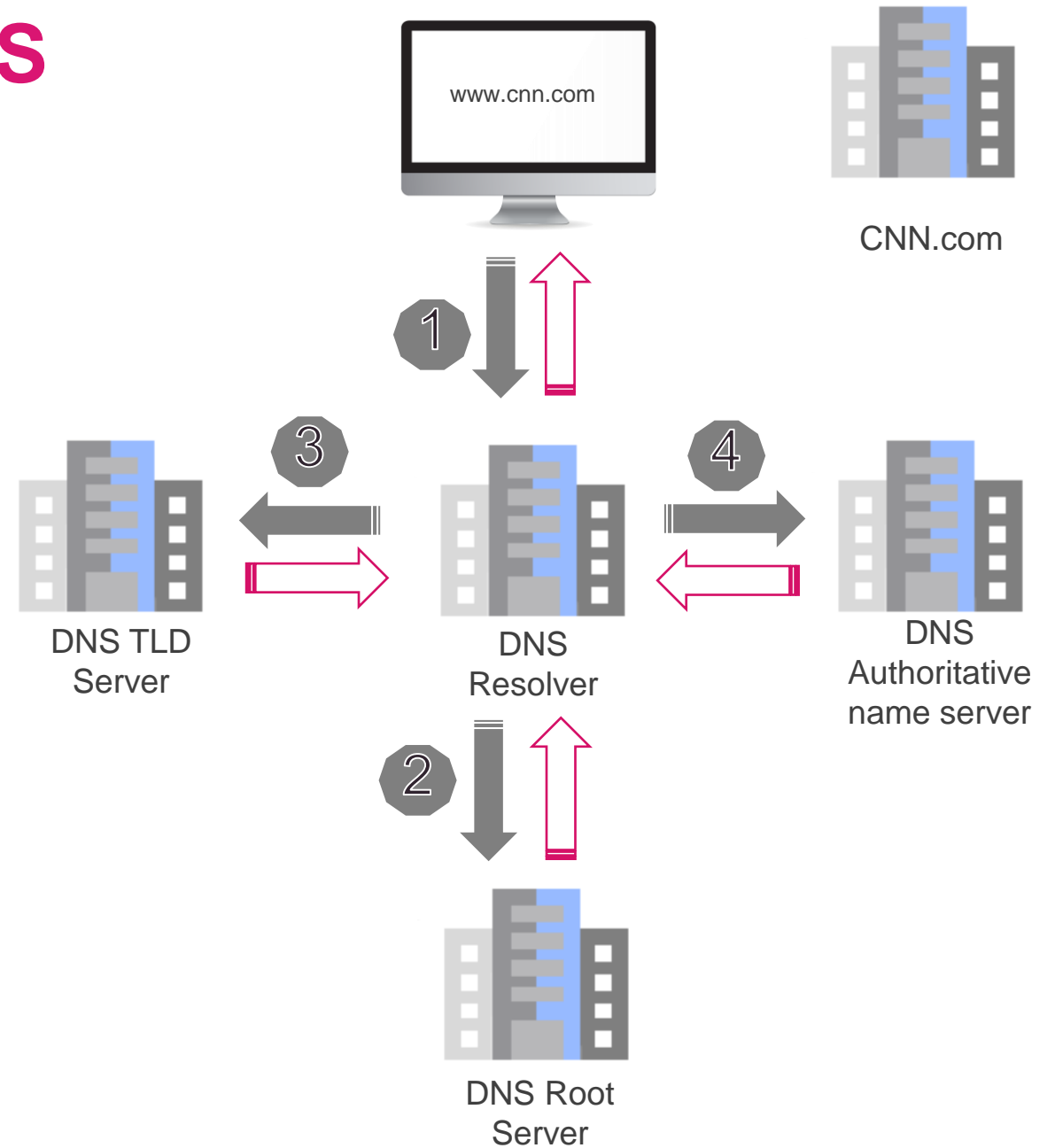
World Intellectual Property Organization,  
September 2022

# 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.

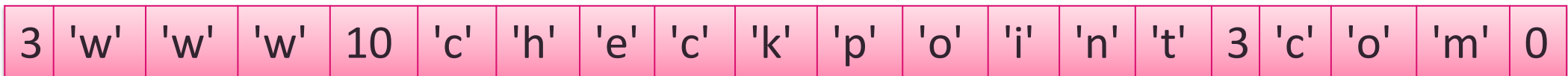


# DNS EM POUCAS PALAVRAS - LIMITAÇÕES

- 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

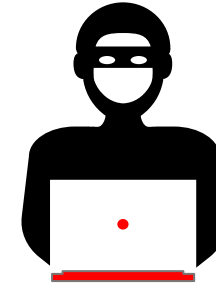
```
dns.qry.name == "www.checkpoint.com"
No.    Time           Source            Destination       Protocol Length  Info
-----
7 8.616627      192.168.10.200    192.168.170.11   DNS        101     Standard query 0xf51e A www.checkpoint.com OPT
8 8.632951      192.168.170.11   192.168.10.200   DNS        195     Standard query response 0xf51e A www.checkpoint.com CNAME d4epvaz4tpdrm.cloudfront.net A 13.24

> Frame 7: 101 bytes on wire (808 bits), 101 bytes captured (808 bits) on interface \Device\NPF...
> Ethernet II, Src: LCFCHeFe_69:4f:ea (84:a9:38:69:4f:ea), Dst: CheckPoi_ci:05:05 (00:11:32:05:05:05)
> Internet Protocol Version 4, Src: 192.168.10.200, Dst: 192.168.170.11
> User Datagram Protocol, Src Port: 63259, Dst Port: 53
> Domain Name System (query)
  Transaction ID: 0xf51e
  Flags: 0x0120 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 1
  Queries
    www.checkpoint.com: type A, class IN
      Name: www.checkpoint.com
      [Name Length: 18]
      [Label Count: 3]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
  Additional records
    [Response In: 8]
```

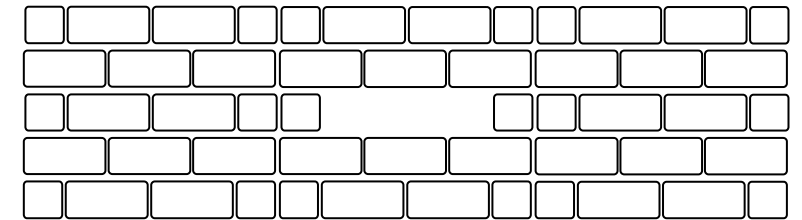


# POR QUE O DNS É UM PONTO DE INTERESSE PARA HACKERS?

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



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



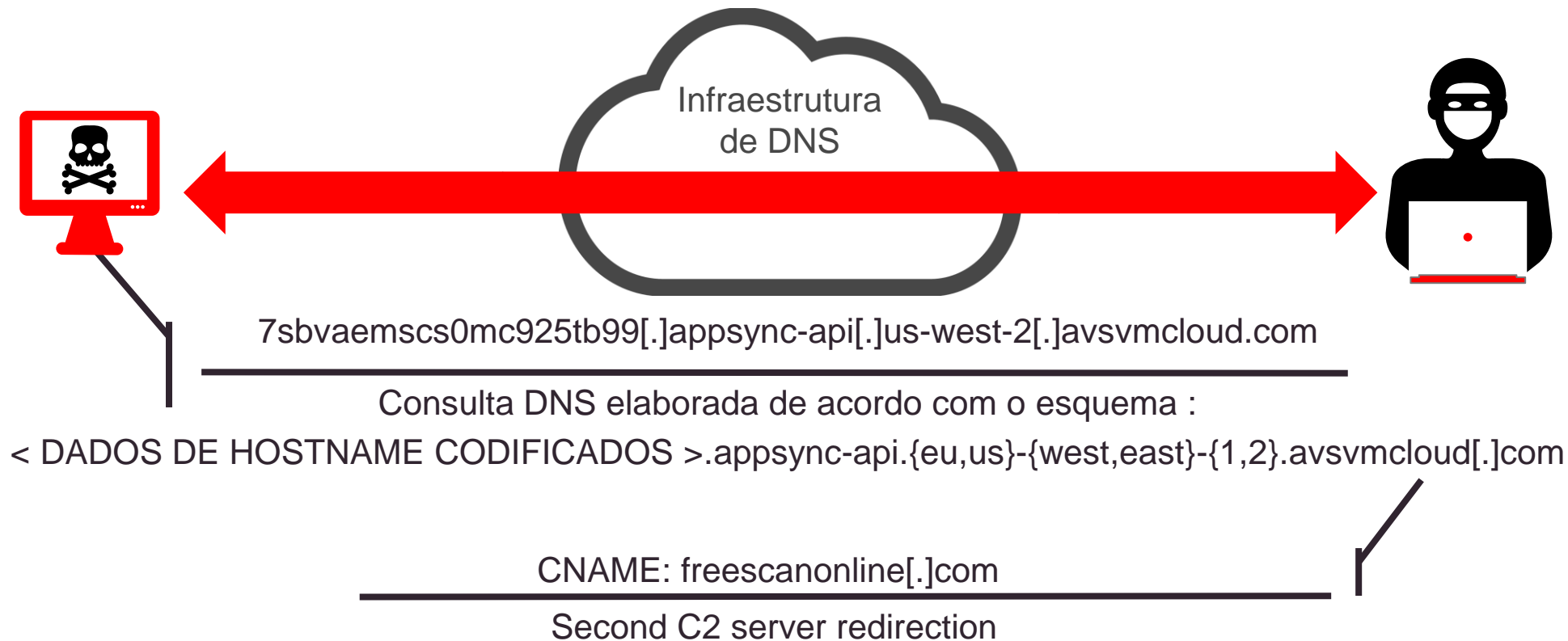
Por estas razões, o DNS é um excelente canal para comunicação C2





# EXEMPLO DE MALWARE AVANÇADO

SunBurst usou tunelamento DNS para canal C2



The background features a light gray network diagram on the right side, consisting of several circular nodes connected by lines. The rest of the background is filled with a pattern of small, light gray dots arranged in concentric, overlapping circles that create a sense of depth and movement.

# **APROVEITANDO O DEEP LEARNING PARA PROTEGER CONTRA EXPLORAÇÕES DE DNS**

# DEEP LEARNING – THE BASICS

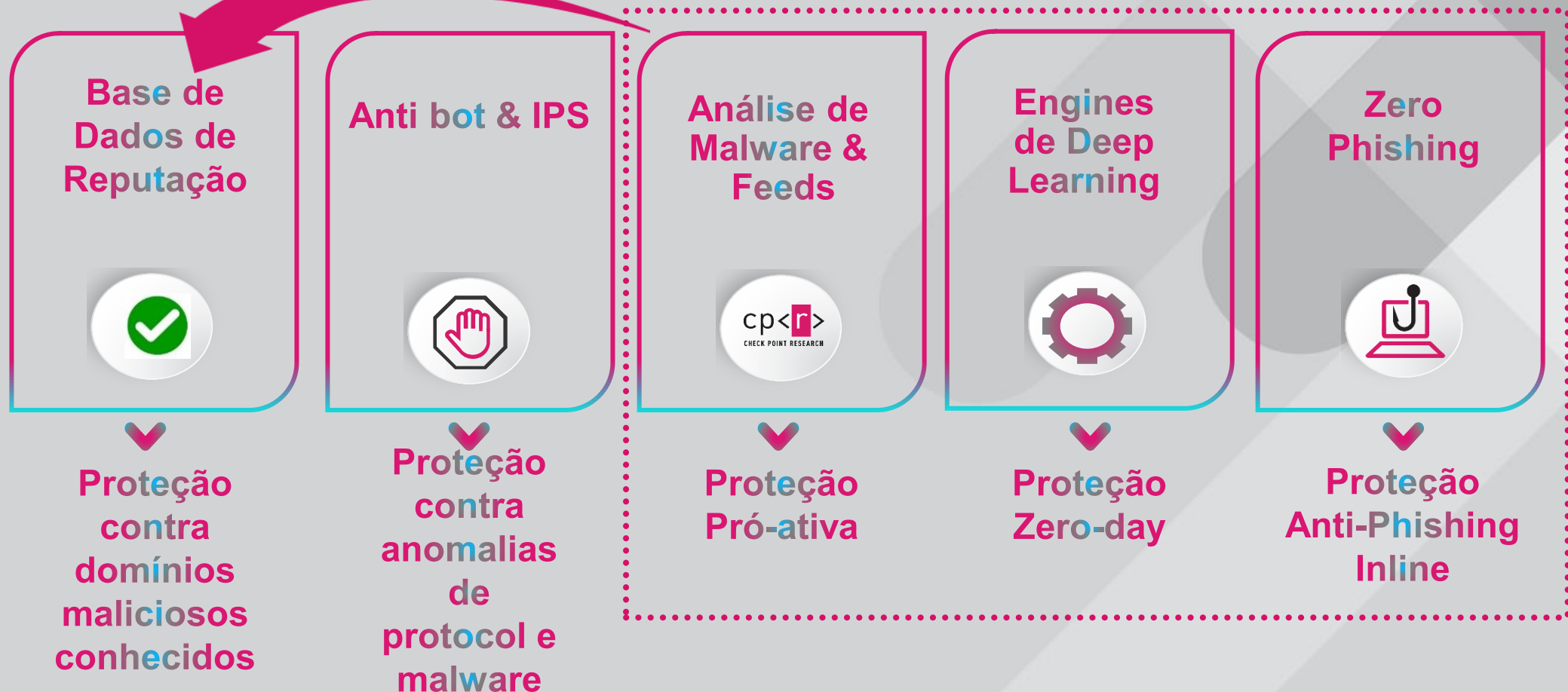
- Comece com MUITOS dados
  - Treine os dados em uma grande quantidade de GPUs
  - Deixe a máquina aprender sem escolher recursos e poucos classificadores

	<b>Machine Learning</b>	<b>Deep Learning</b>
Training dataset	Small	Large
Choose your own features	<b>Yes</b>	<b>No</b>
# of classifiers available	Many	Few
Training time	Short	Long



SEGURANÇA AVANÇADA DE DNS  
Powered by ThreatCloud

THREATCLOUD

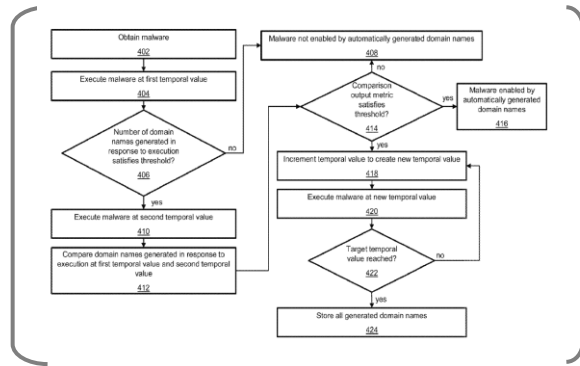


# PROTEÇÃO PROATIVA CONTRA DOMÍNIOS MALICIOSOS

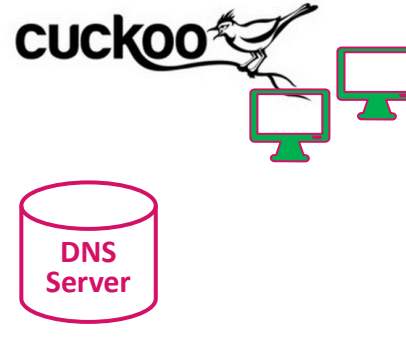
Extraia DGA de malware com sistema protegido patenteado



## Extração de Algoritmo



## Ambiente de emulação



## Aggregação e Enriquecimento



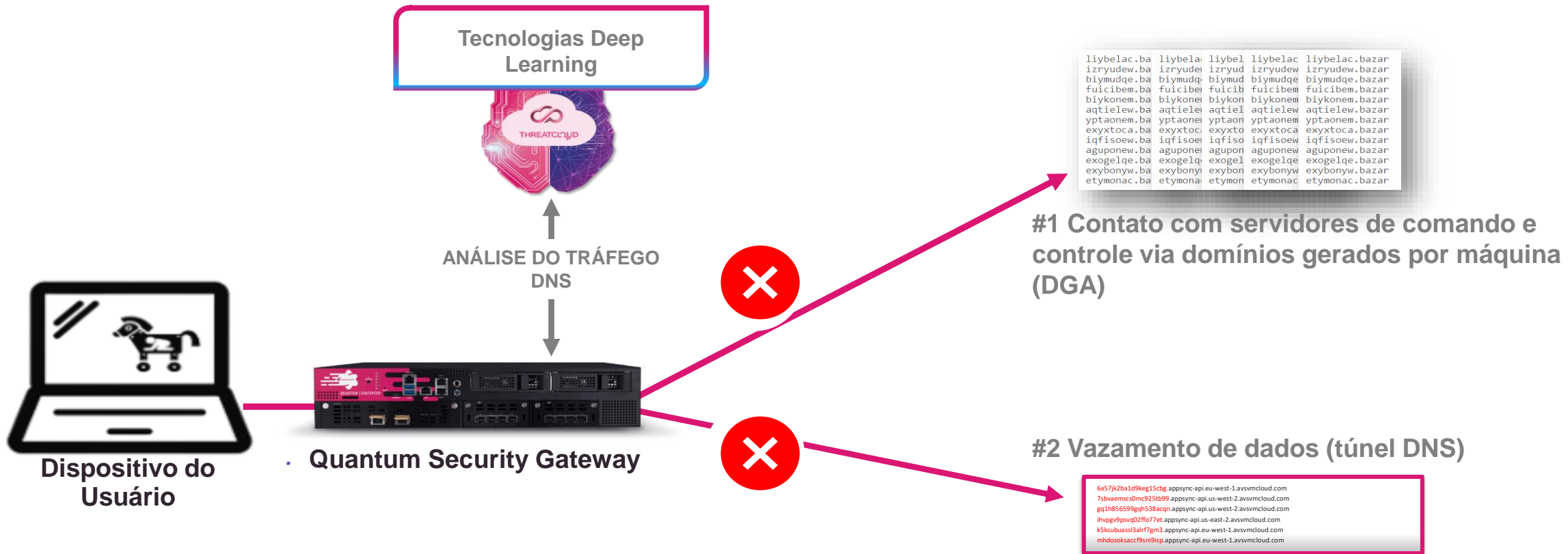
Mais de **650K** novos domínios por dia!

ash.cou**p**bat.com  
adz.cou**p**final.com  
ars.cou**p**hole.com  
aim.cou**p**homegame.com  
ask.cou**p**lose.com  
aff.cou**p**loss.com  
aal.cou**p**match.com  
aft.cou**p**playoff.com  
ami.cou**p**playoffgame.com  
jsn.don**e**core.net  
jso.don**e**div.net  
dfo.don**e**mace.net  
j**s**m.don**e**map.net

- Static DGA
- Date-Based DGA
- Feed Providers DGA
- Seed-Based DGA

# BLADE DE SEGURANÇA AVANÇADA PARA DNS

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

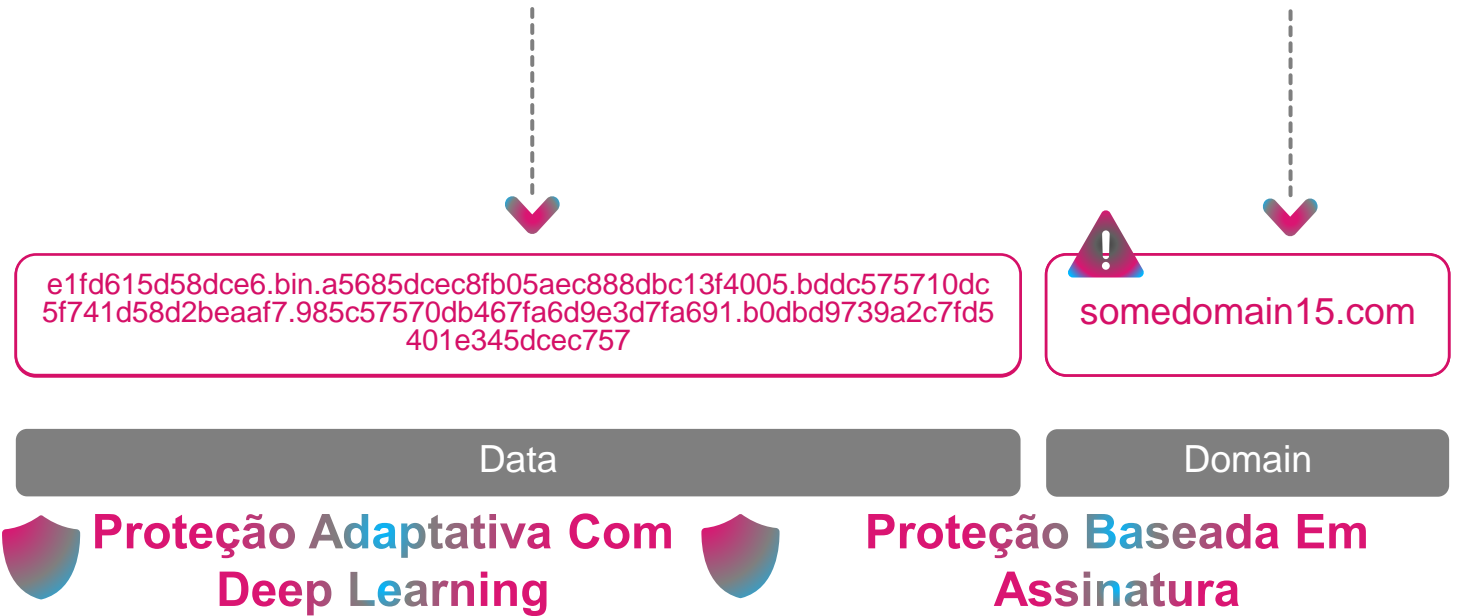


# CASO DE USO #1: UDPOs TUNELAMENTO DE DNS

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

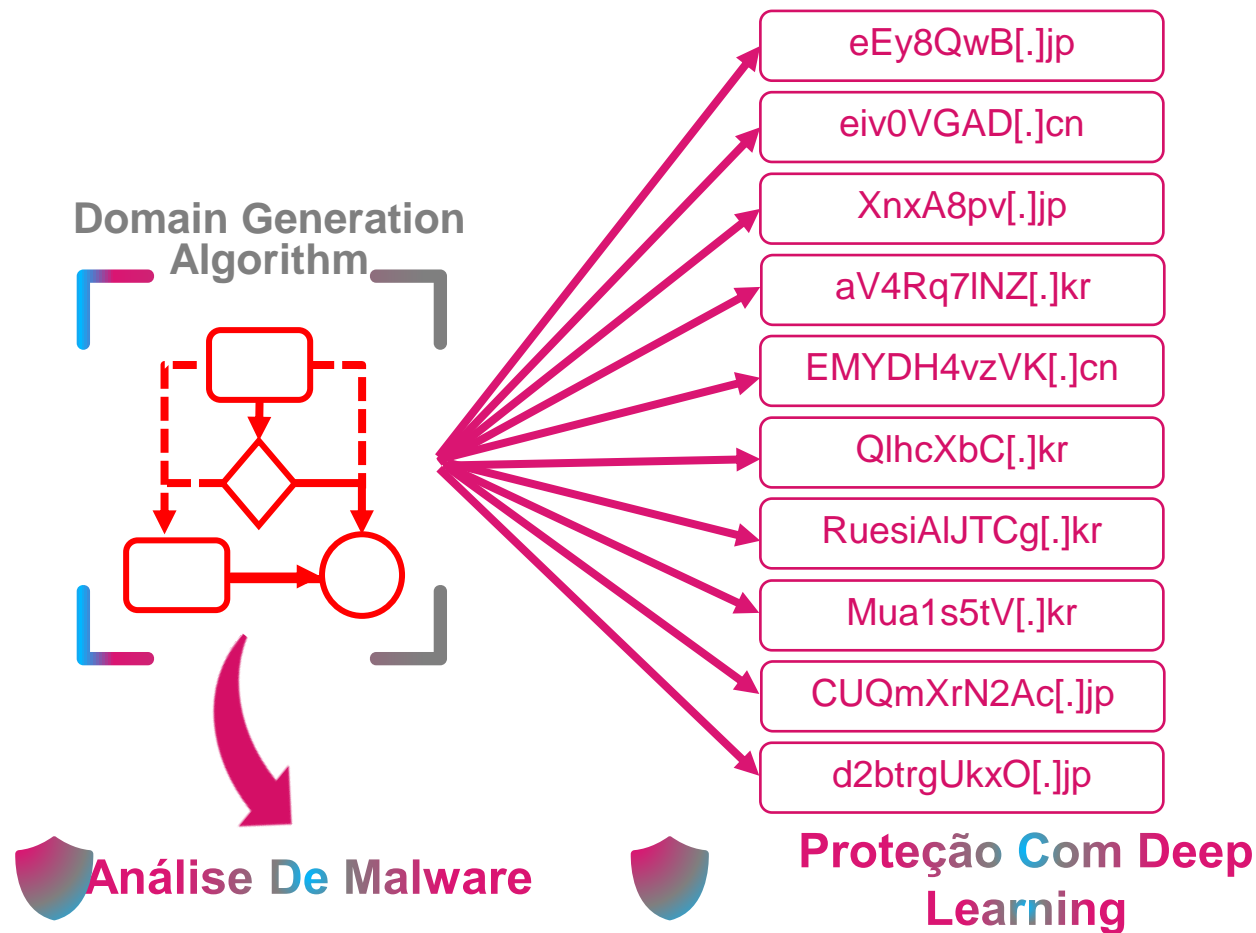
```
Domain Name System (query)
Transaction ID: 0x27bd
Flags: 0x0100 Standard query
0... .. = Response: Message is a query
.000 0... .. = Opcode: Standard query (0)
... ..0. .... = Truncated: Message is not truncated
... ..1 .... = Recursion desired: Do query recursively
... ..0.. .... = Z: reserved (0)
... ..0 .... = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
> 0b41615cff56ce6.bin.a568264a8fb05a6b72ddbcb13f4005.bdd9e1fdf110dc5f741d58d2beaaf7.985c5757a7288467fa6d9e3deeb991.b0dbd9739a2c7fd5401e345dcec884.service-logme1n.network
```



# 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



Tecnologia AI



Threat intelligence



Em menos de **1 mês**

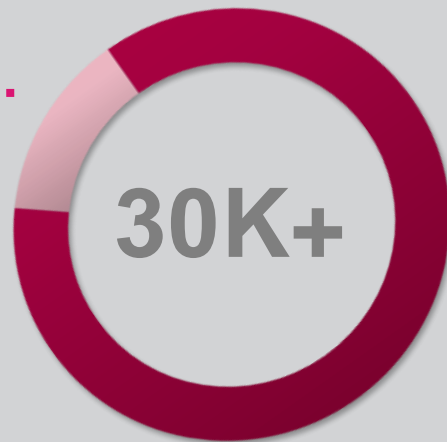
**650K+**

Novos domínios por dia

**Dezenas**

de famílias de malware cobertas

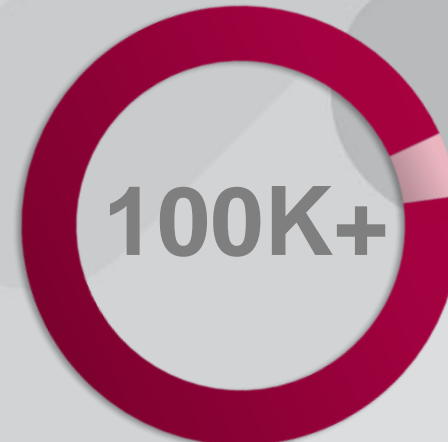
Milhares deles são novos



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

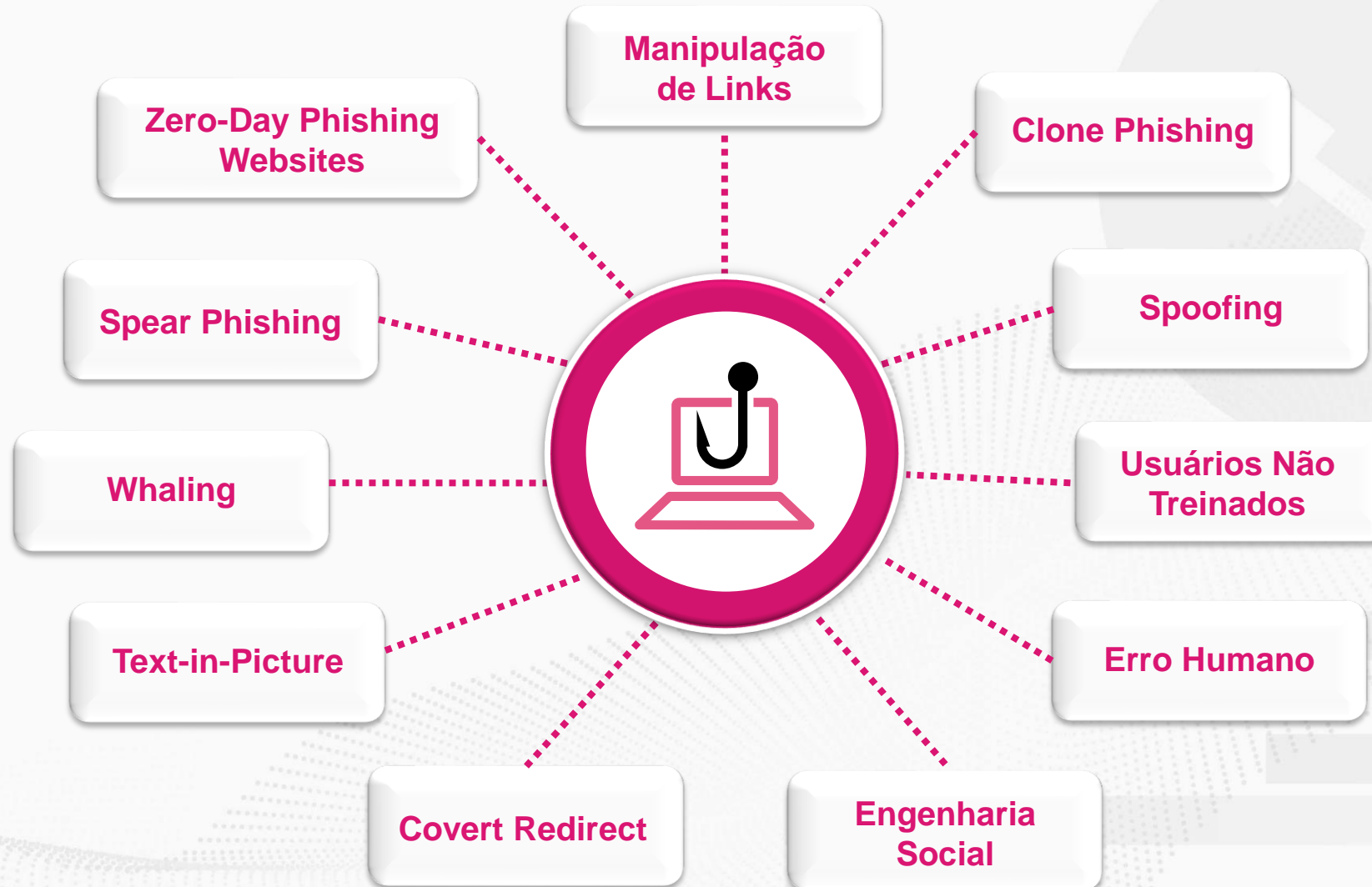


# O QUE É ZERO PHISHING?

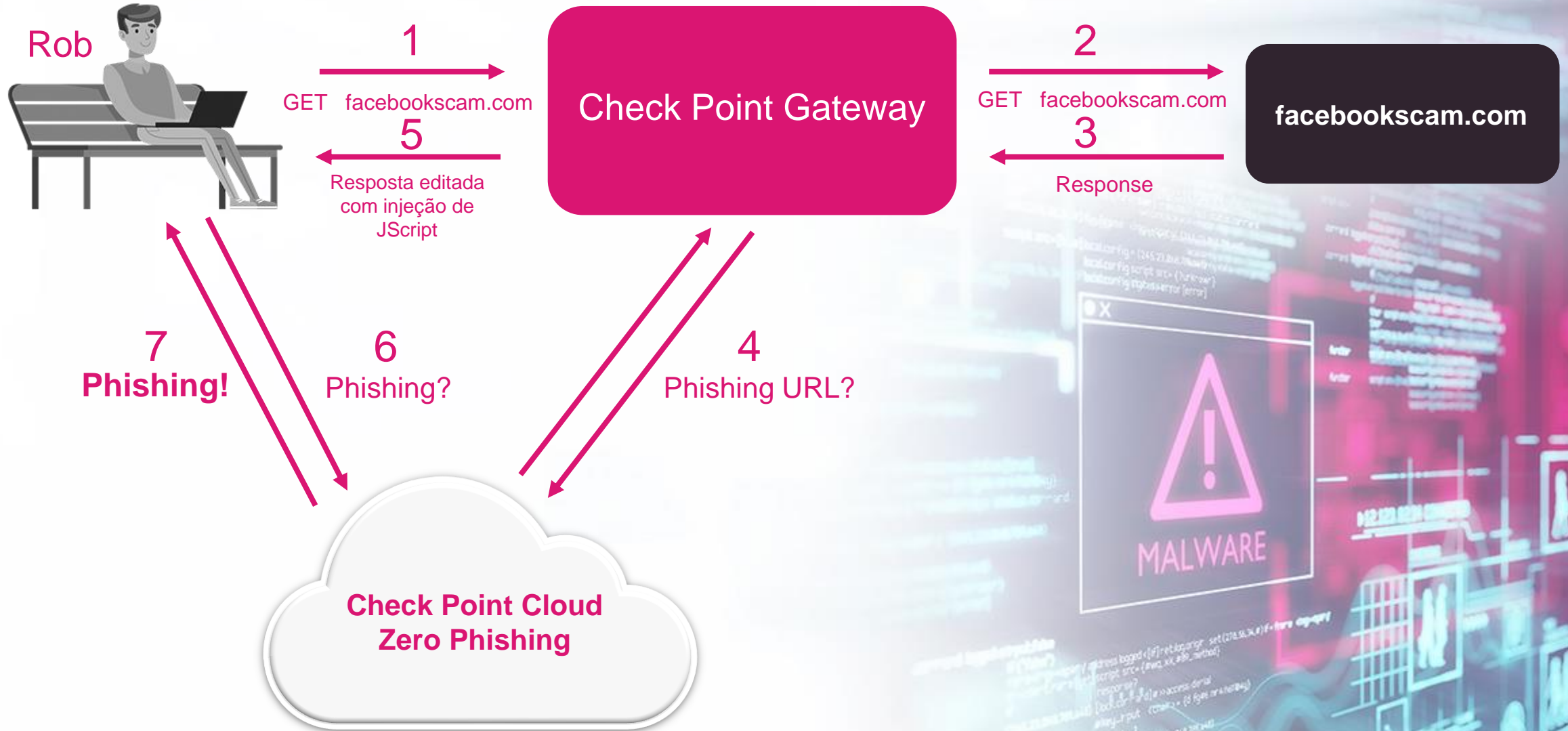
- A proteção Zero Phishing é alimentada por tecnologias patenteadas para evitar ataques de phishing de dia zero em sites.
- A proteção é realizada no Security Gateway, o que o torna independente de navegador e plataforma e não depende de uma solução de segurança de e-mail\*
- Esta proteção está incluída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



# PORQUE PHISHING NECESSITA DE PREVENÇÃO

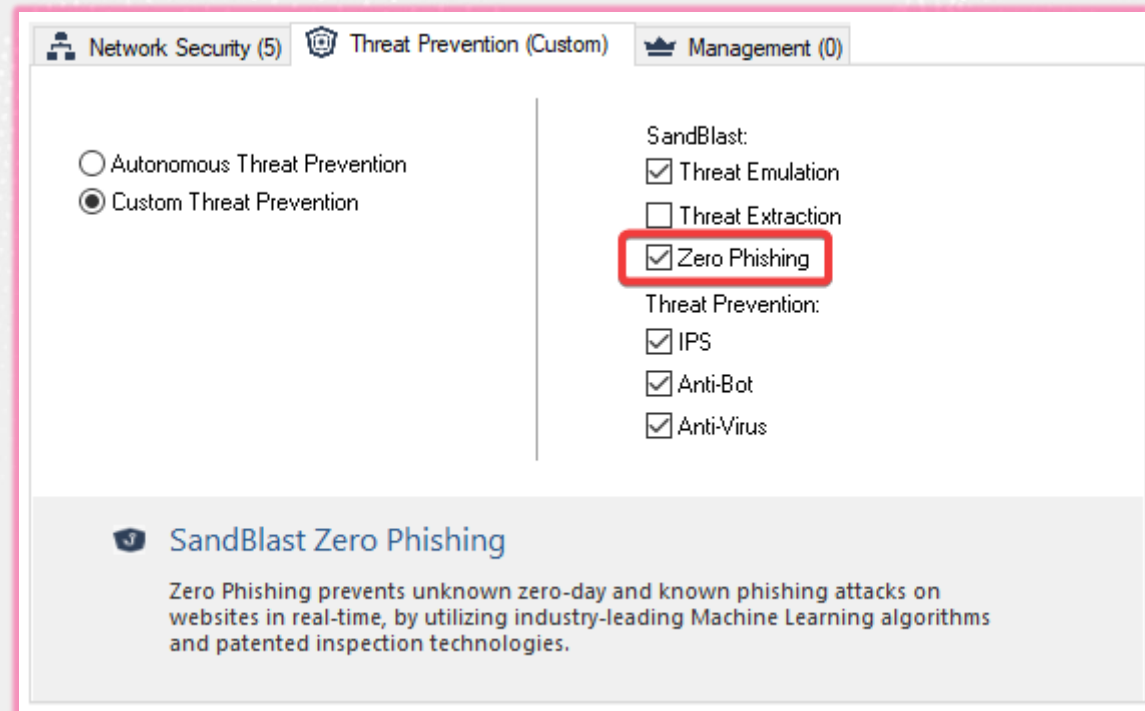


# ZERO-PHISHING – FLUXO DETALHADO



# ZERO-PHISHING – ATIVAÇÃO DA BLADE

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

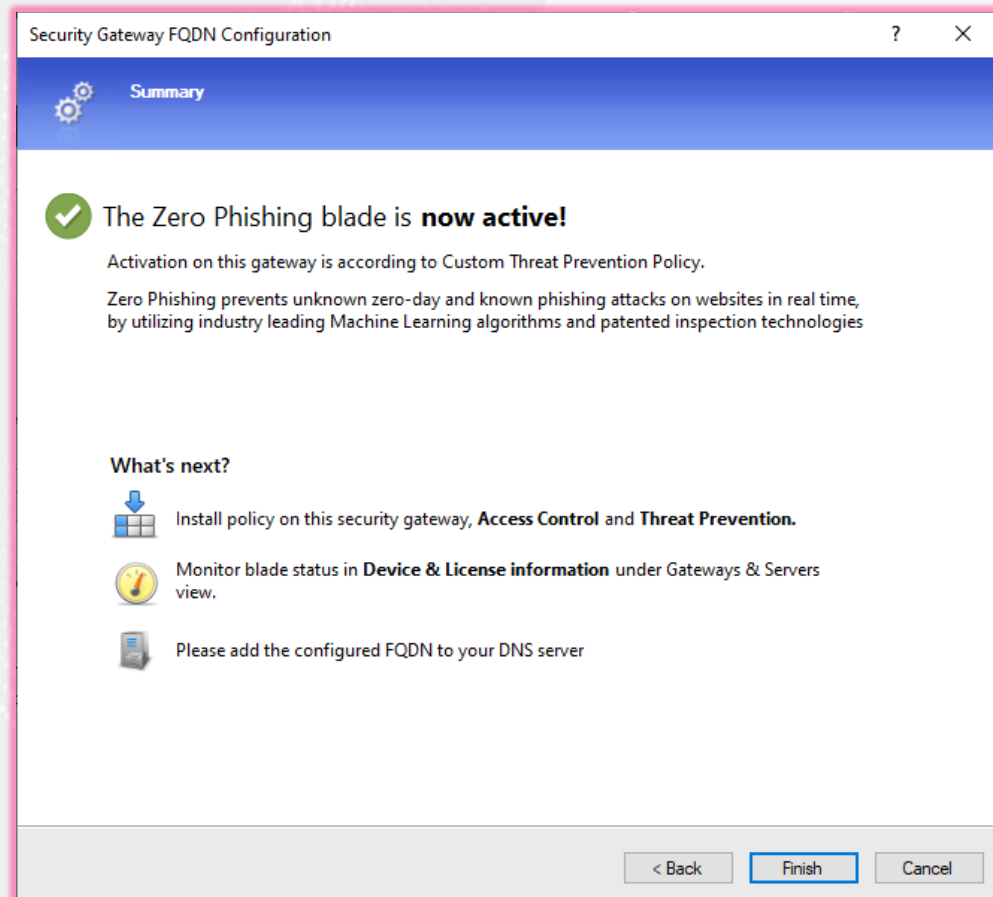
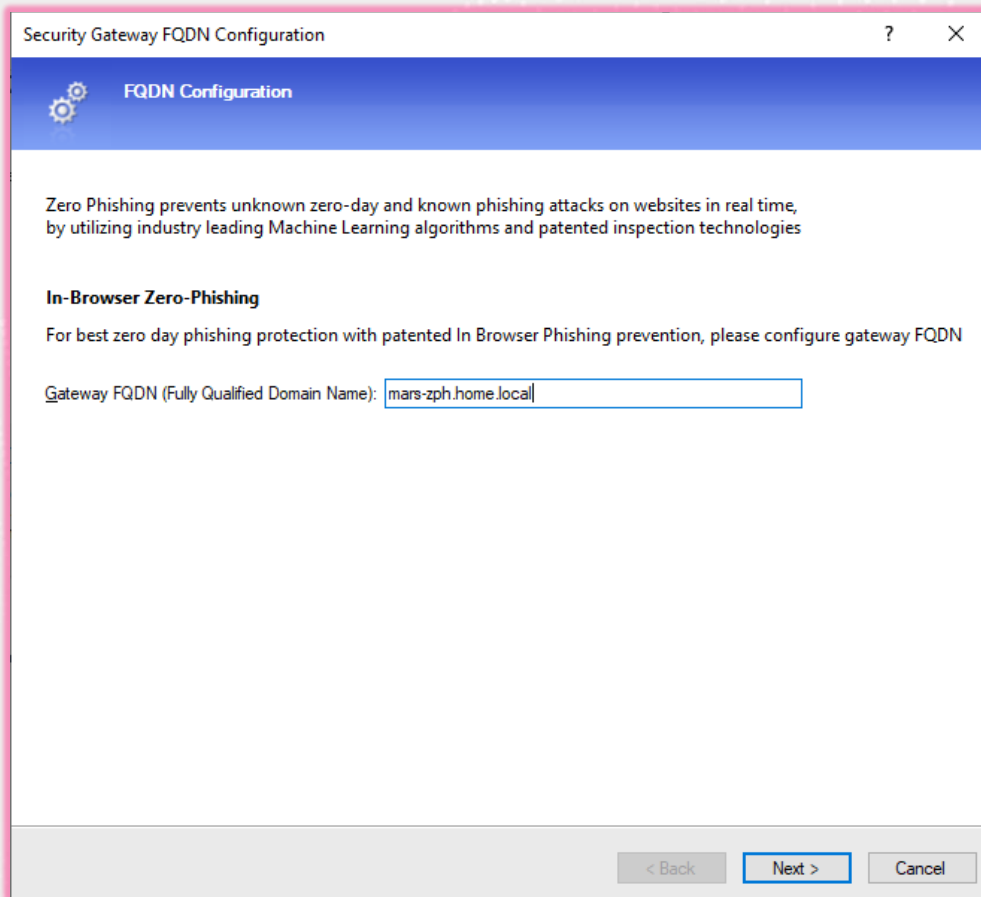


The screenshot shows the configuration page for Threat Prevention (Custom) in the Check Point management console. The page is divided into two main sections. On the left, there are two radio buttons: 'Autonomous Threat Prevention' (unselected) and 'Custom Threat Prevention' (selected). On the right, under the 'SandBlast:' section, there are three checkboxes: 'Threat Emulation' (checked), 'Threat Extraction' (unchecked), and 'Zero Phishing' (checked and highlighted with a red box). Below this, under the 'Threat Prevention:' section, there are three checkboxes: 'IPS' (checked), 'Anti-Bot' (checked), and 'Anti-Virus' (checked). At the bottom of the page, there is a section titled 'SandBlast Zero Phishing' with a brief description: 'Zero Phishing prevents unknown zero-day and known phishing attacks on websites in real-time, by utilizing industry-leading Machine Learning algorithms and patented inspection technologies.'



# 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.



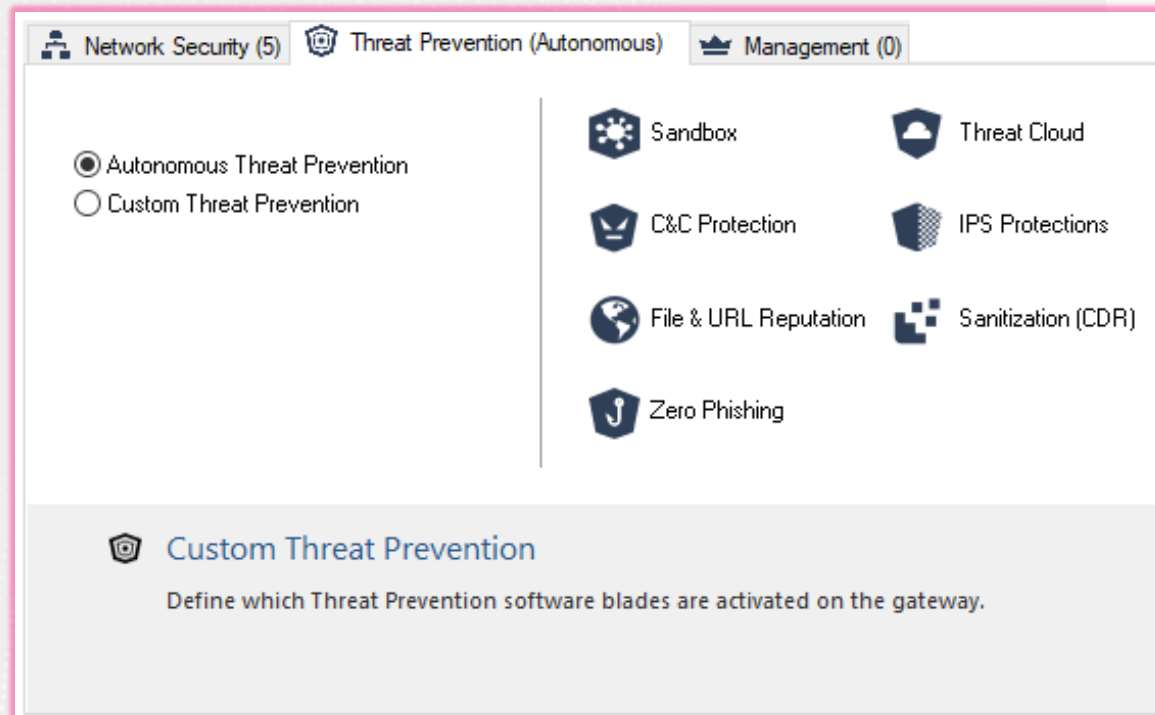
# ZERO-PHISHING - ATP

- 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](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

Threat Prevention

- Custom Policy
- Autonomous Policy
  - Policy
  - File Protections
  - Settings**
  - Exceptions
- HTTPS Inspection
  - Policy

Advanced Settings

Property Name	Value
Archives deep scan (impacts performance)	Off
<b>In-Browser Zero Phishing</b>	<b>On</b>
Policy Optimized for	Rapid delivery

## Custom Threat Prevention

Profiles

**Optimized**  
Provides excellent protection for all common network prod...

- General Policy
  - In-Browser Zero Phishing
- Mail
- IPS
  - Anti-Bot
  - Anti-Virus
- Threat Emulation
- Threat Extraction
- Zero Phishing**
- Indicators
- Malware DNS Trap

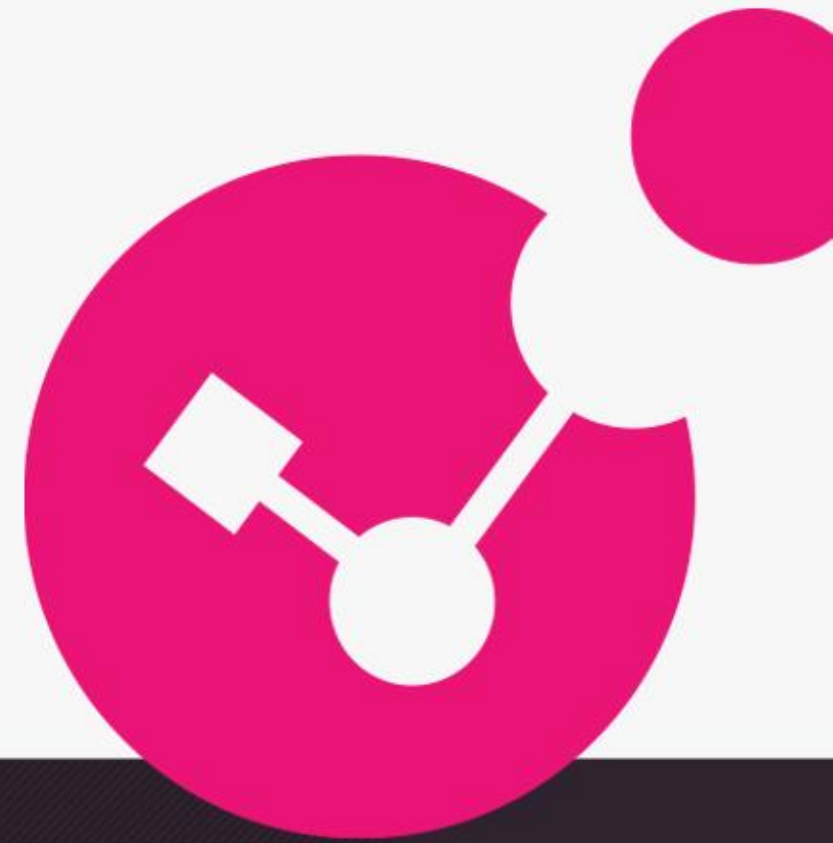
OK Cancel

DEMO





**Obrigado!**



YOU DESERVE THE BEST SECURITY