EL DNS Y FORMAS DE VULNERAR LA SEGURIDAD

UNIVERSIDAD VERACRUZ
CUDI
Septiembre 2023

Presentador

- Gerardo Mendoza

Infoblox Solutions Architect

infoblox

BUSINESS CHALLENGES

Multi-cloud

SaaS

IoT/OT

Source: “20/20 Visibility Clarifies Network Security”, A Forrester Consulting Paper Commissioned by Infoblox, July 2022

+30

Security tools

$4M

Average cost of a data breach

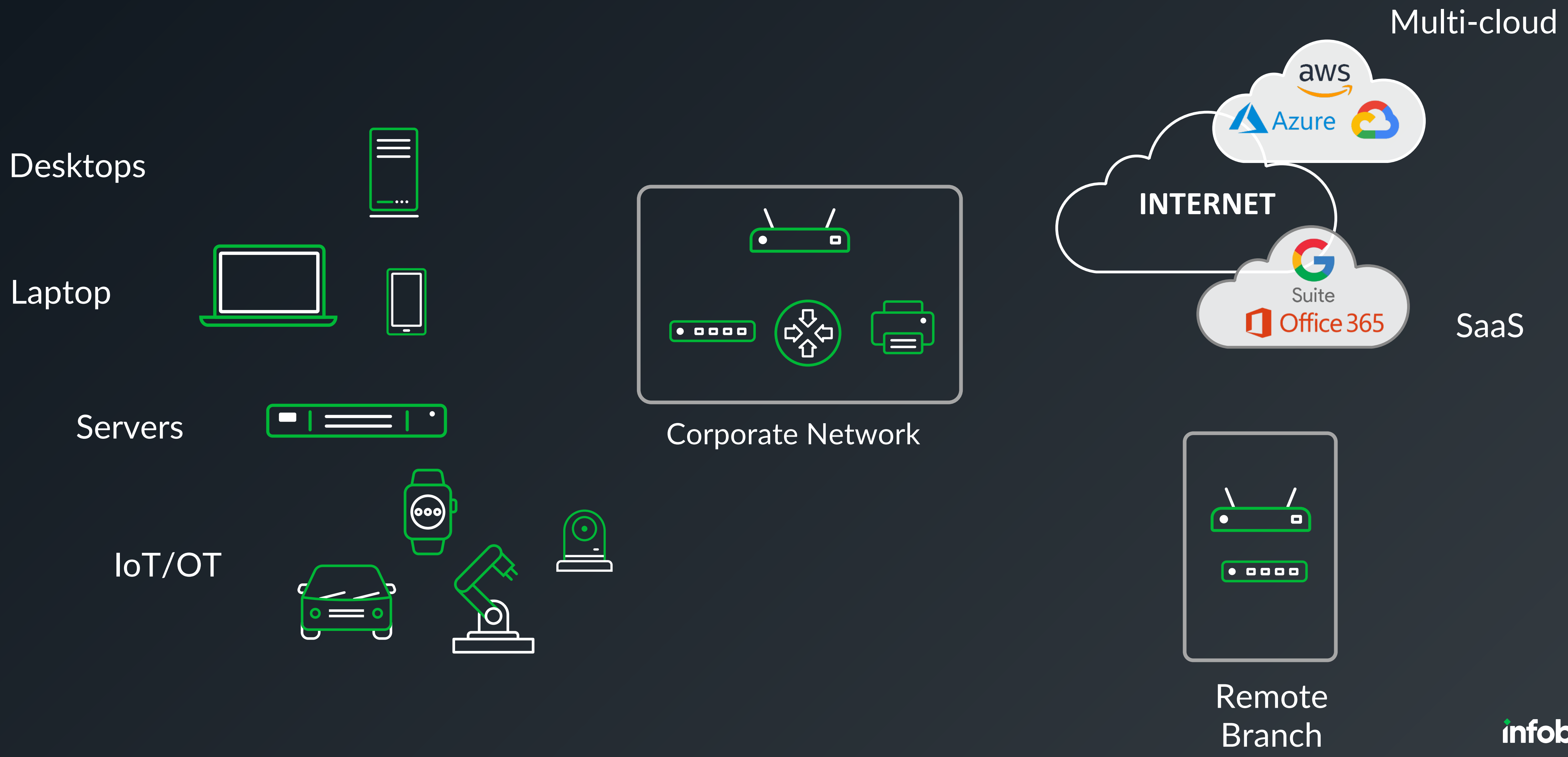
270

Average days to identify and contain

Source: 2022 IBM Data Breach Report

infoblox

PERIMETER HAS DISSAPPEARED



Desktops

Laptop

Servers

IoT/OT

Corporate Network

INTERNET

Multi-cloud

SaaS

Remote Branch

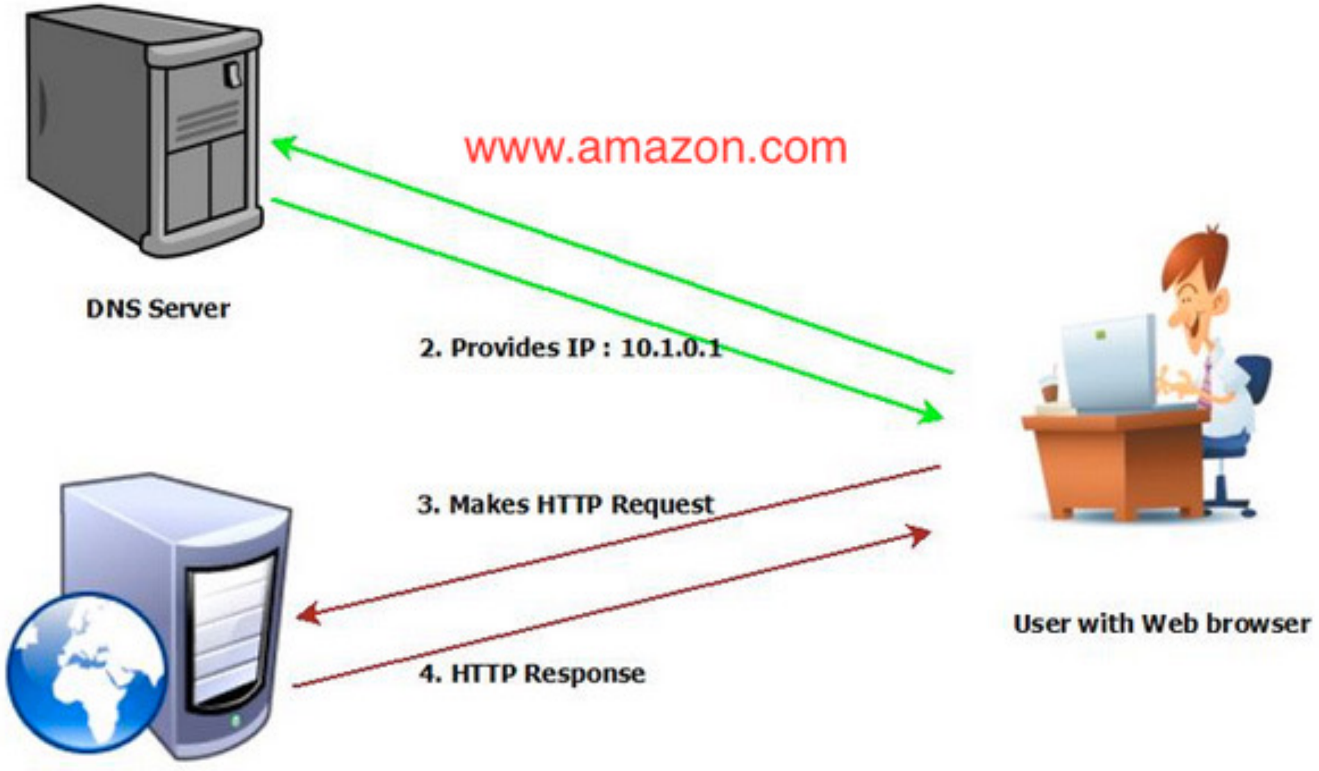
Question:

¿Qué protocolo de red ha sido usado en el 92%* de los Ciberataques recientes?

Domain Name System

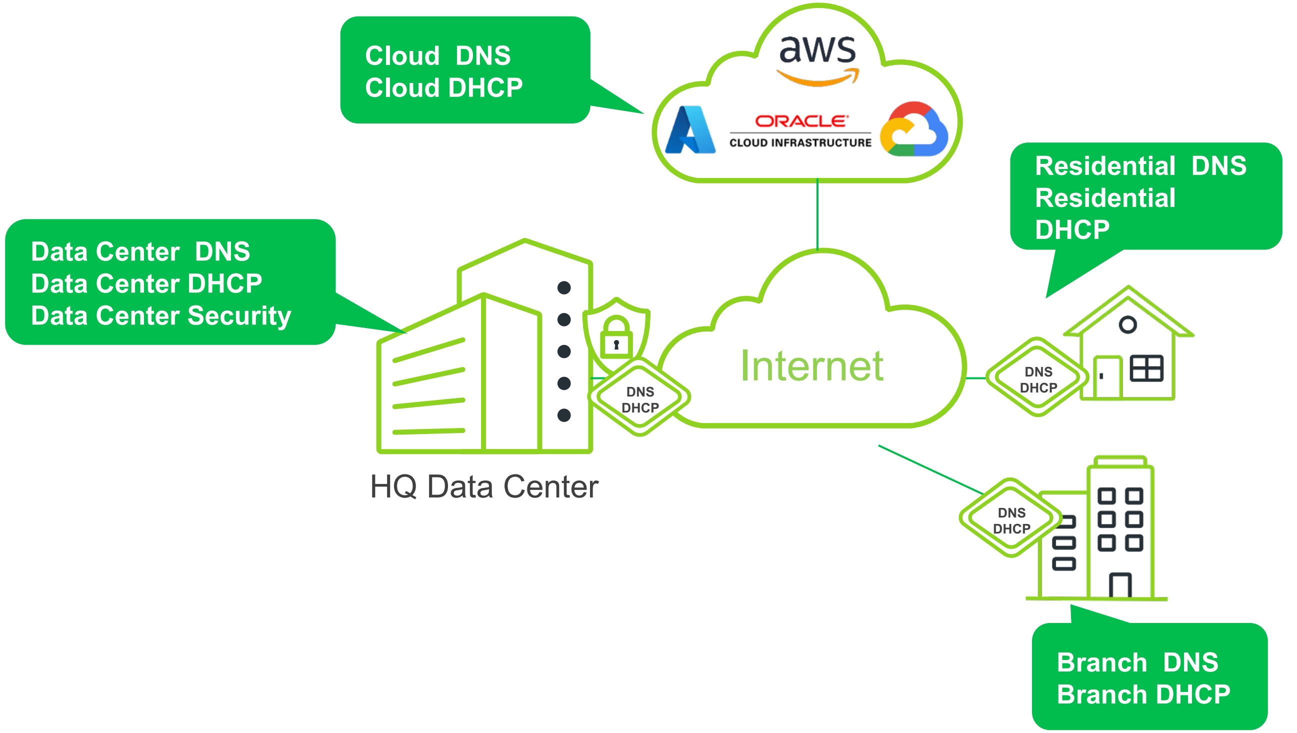
*NSA

TODOS los elementos de la red dependen del DNS



- Cada usuario, dispositivo y aplicación en la red de cómputo, necesita conocer la dirección (IP) de los sistemas y dispositivos a los que se va a conectar.
  Para ello, utilizan el servicio de DNS para la traducción.

DNS es LA BASE de las redes actuales



- Provides mission critical network connectivity needed to run a business
- If DNS is down, network is shut off from the Internet, critical IT applications become inaccessible

*NSA

DATOS ESCALOFRIANTES

- **91% del malware usa DNS** para:
  - Enviar tráfico a sitios maliciosos
  - Comunicarse con servidores C&C
  - Transporte (túnel/robo) de datos

- **68% de las empresas no monitorean su DNS**

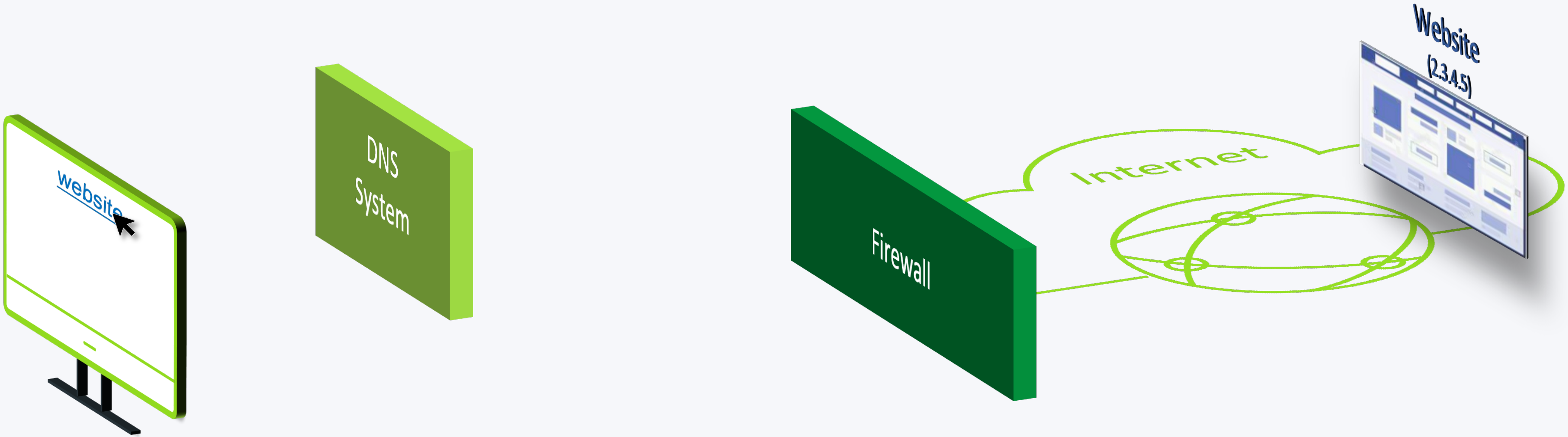
- **46% de los negocios han experimentado robo de información a través del DNS.**

- **Un ataque típico se mitiga en 5h, un ataque al DNS 6.5 horas**

¿Y CÓMO OPERA

EL MALWARE?

TYPICAL MALWARE/RANSOMWARE



website

DNS System

Firewall

Internet

Website (2.3.4.5)

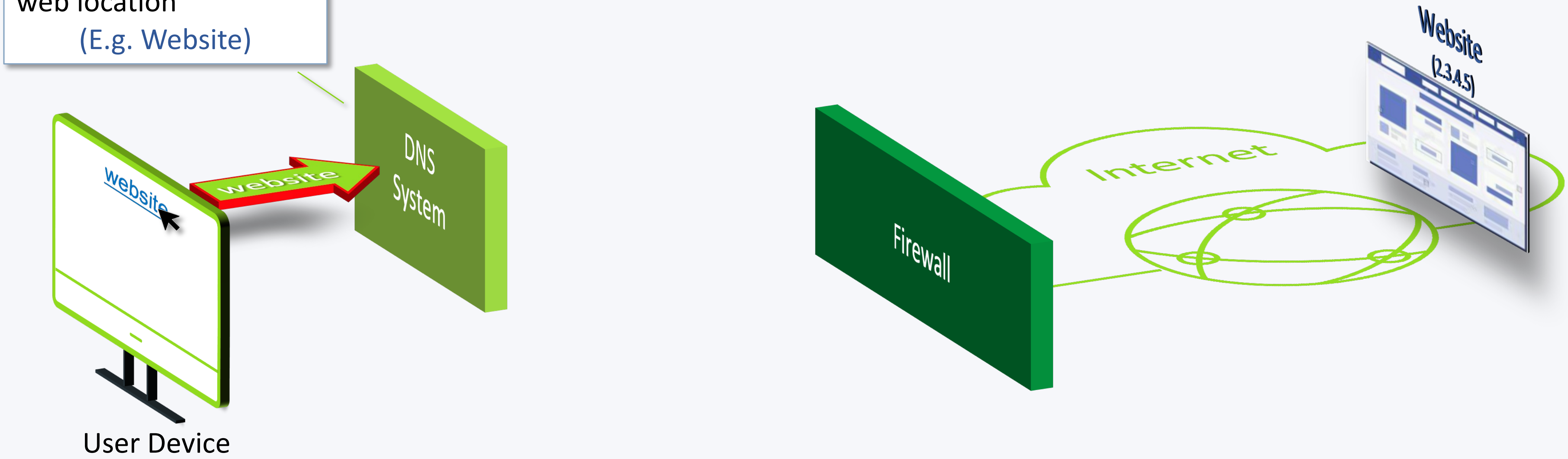
User Device

TYPICAL MALWARE/RANSOMWARE

1. DNS REQUEST

Request IP address for web location

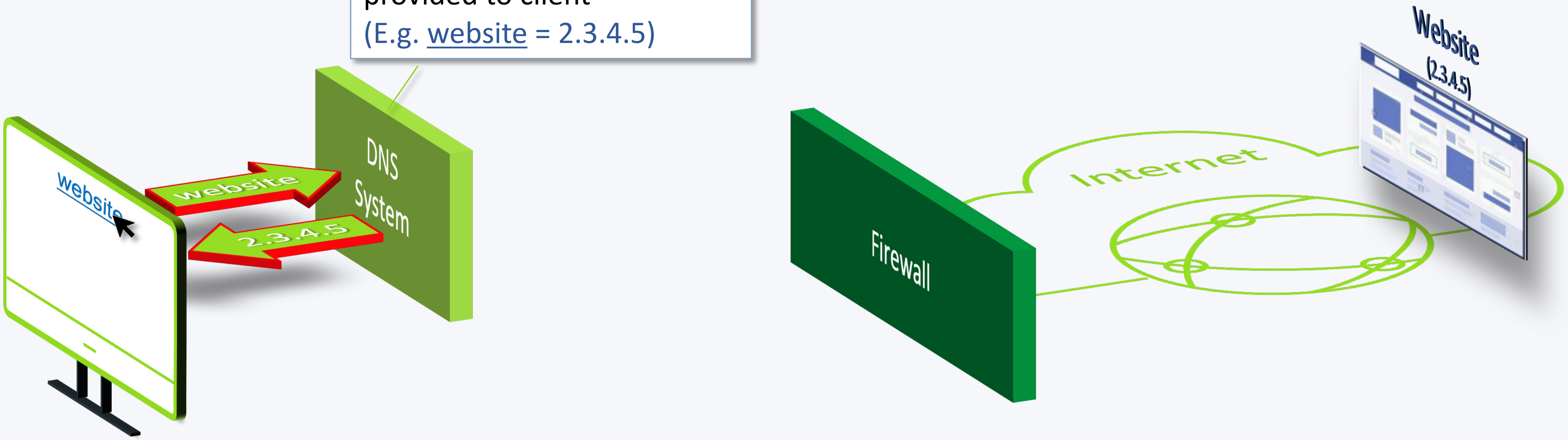
(E.g. Website)



TYPICAL MALWARE/RANSOMWARE

2. DNS RESPONSE

IP address for web location provided to client
(E.g. website = 2.3.4.5)

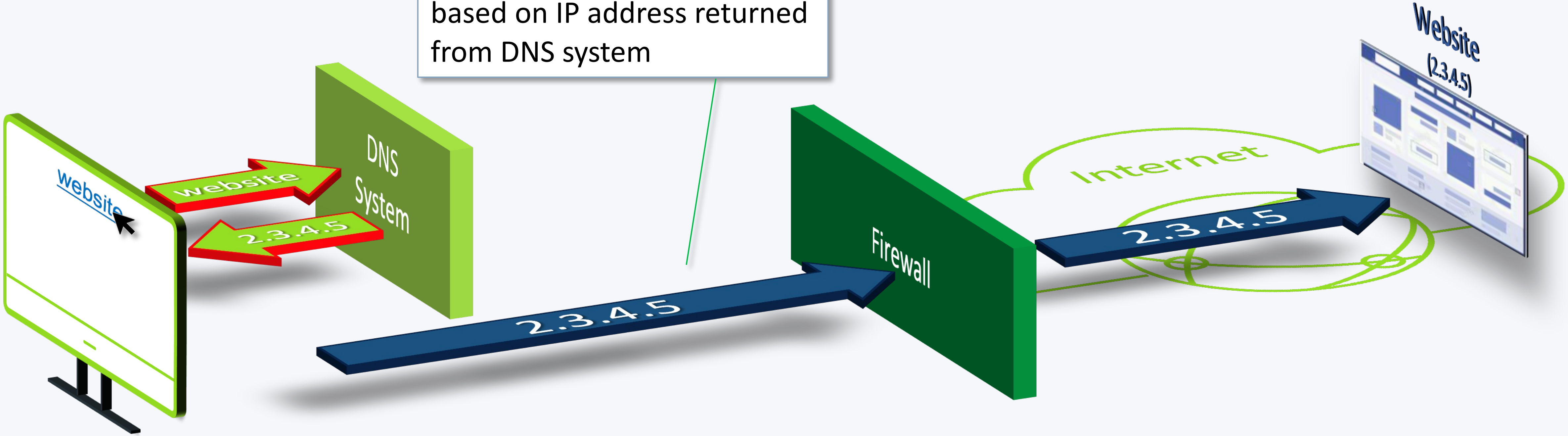


User Device

TYPICAL MALWARE/RANSOMWARE

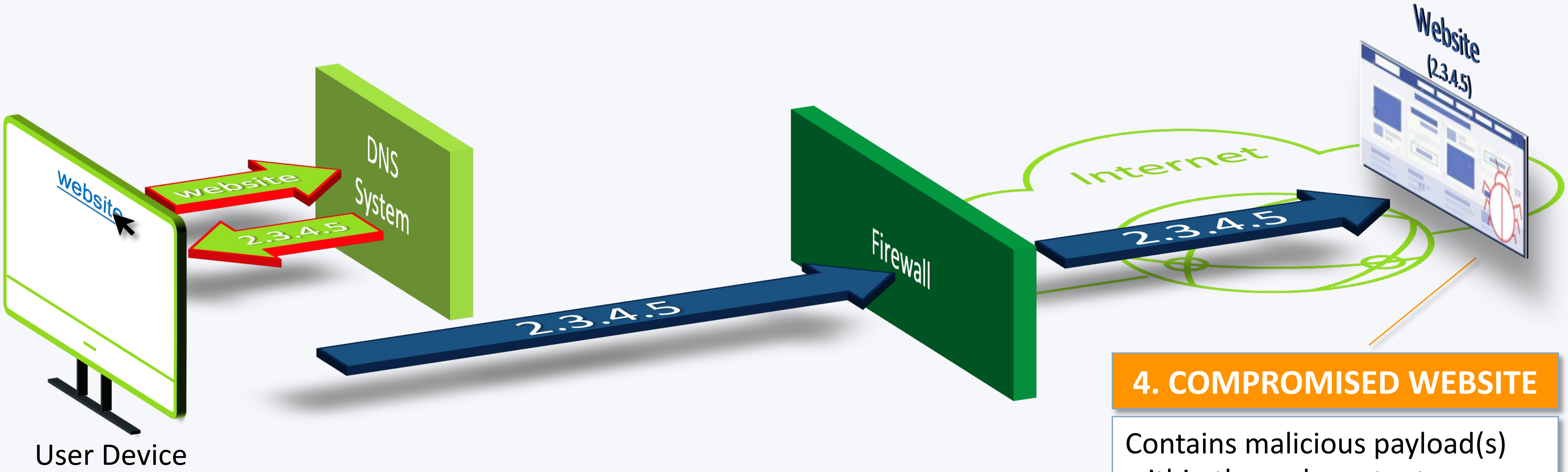
3. CONNECT TO WEBSITE

Client connects to “website” based on IP address returned from DNS system



User Device

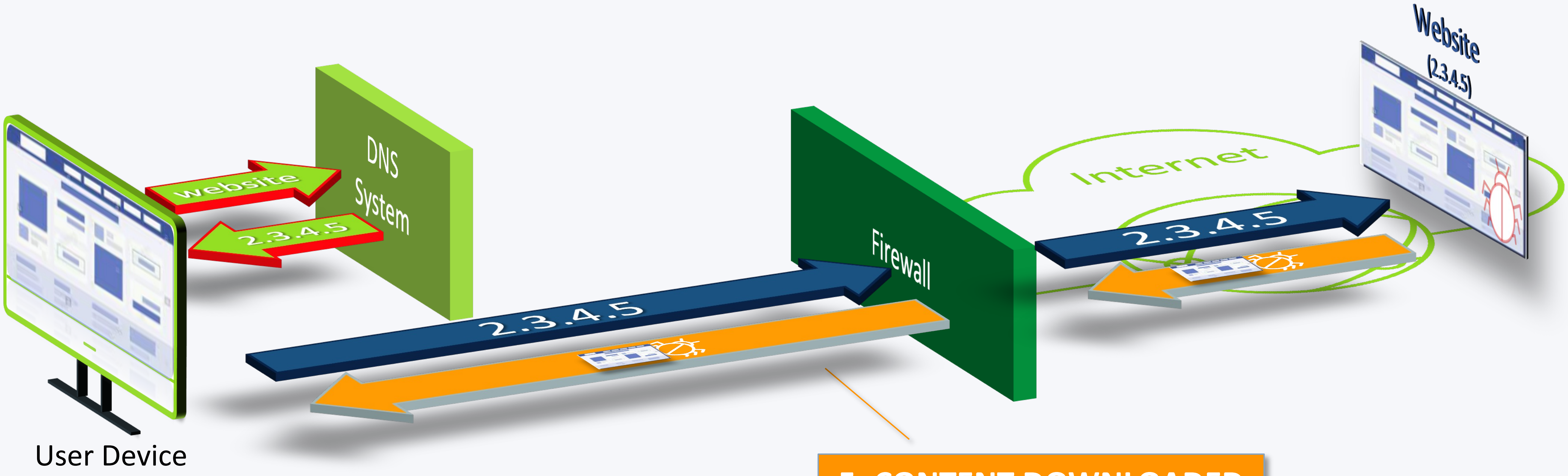
TYPICAL MALWARE/RANSOMWARE



4. COMPROMISED WEBSITE

Contains malicious payload(s) within the web content

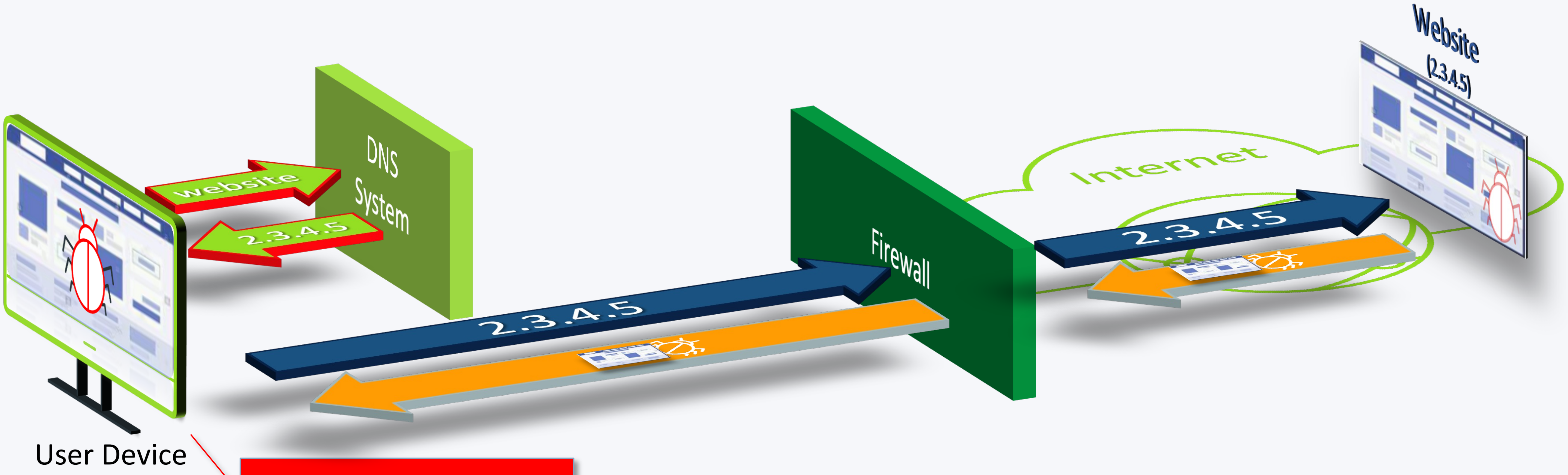
TYPICAL MALWARE/RANSOMWARE



5. CONTENT DOWNLOADED

Malicious payload(s) downloaded along with the web content

TYPICAL MALWARE/RANSOMWARE



6. INFECTION

Device infected with
malware/ransomware

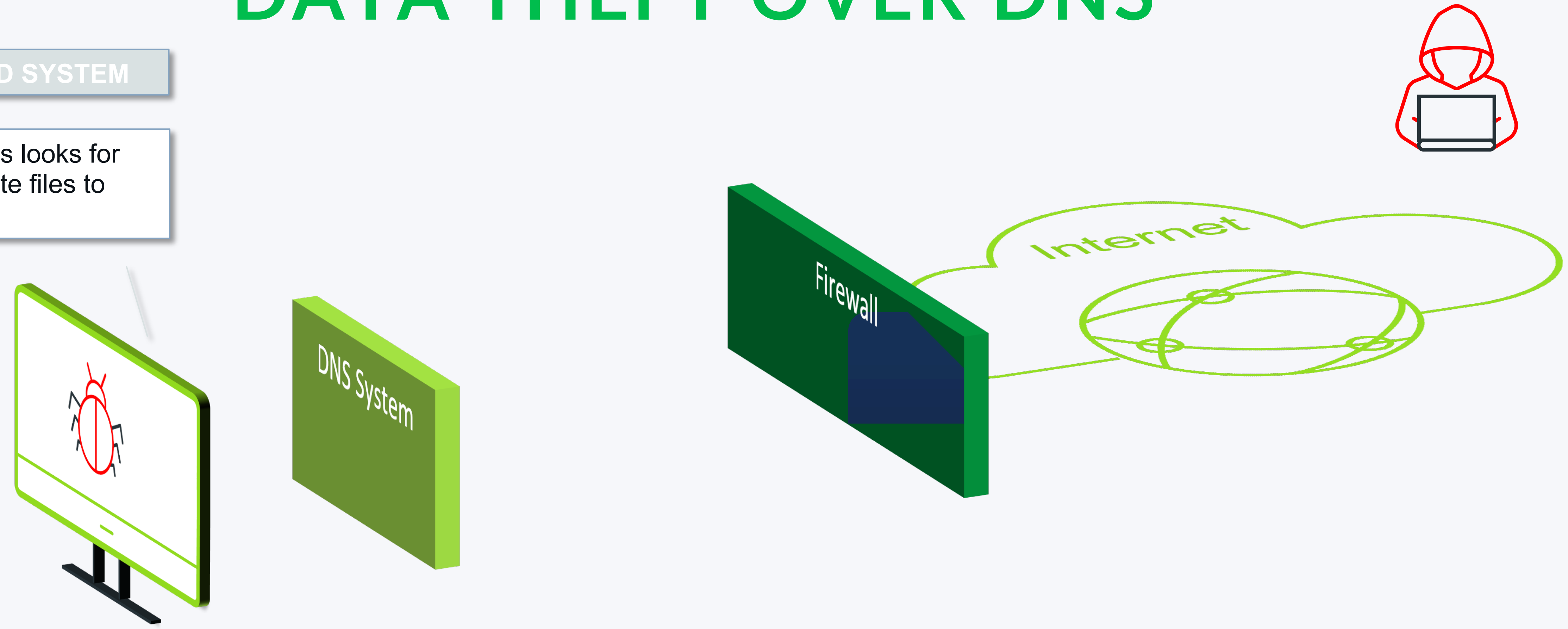
¿QUÉ ES ESO DE LA

EXFILTRACIÓN DE DATOS?

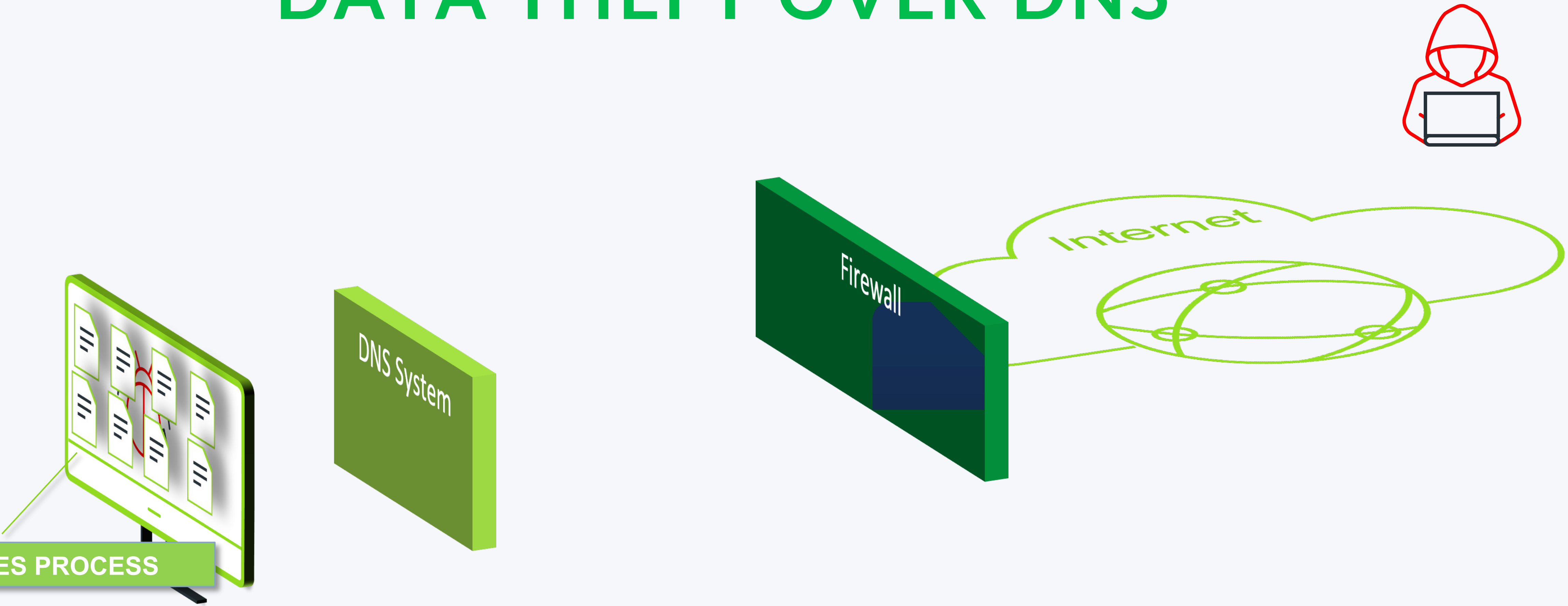
DATA THEFT OVER DNS

1. INFECTED SYSTEM

Malware breaks looks for local and remote files to exfiltrate



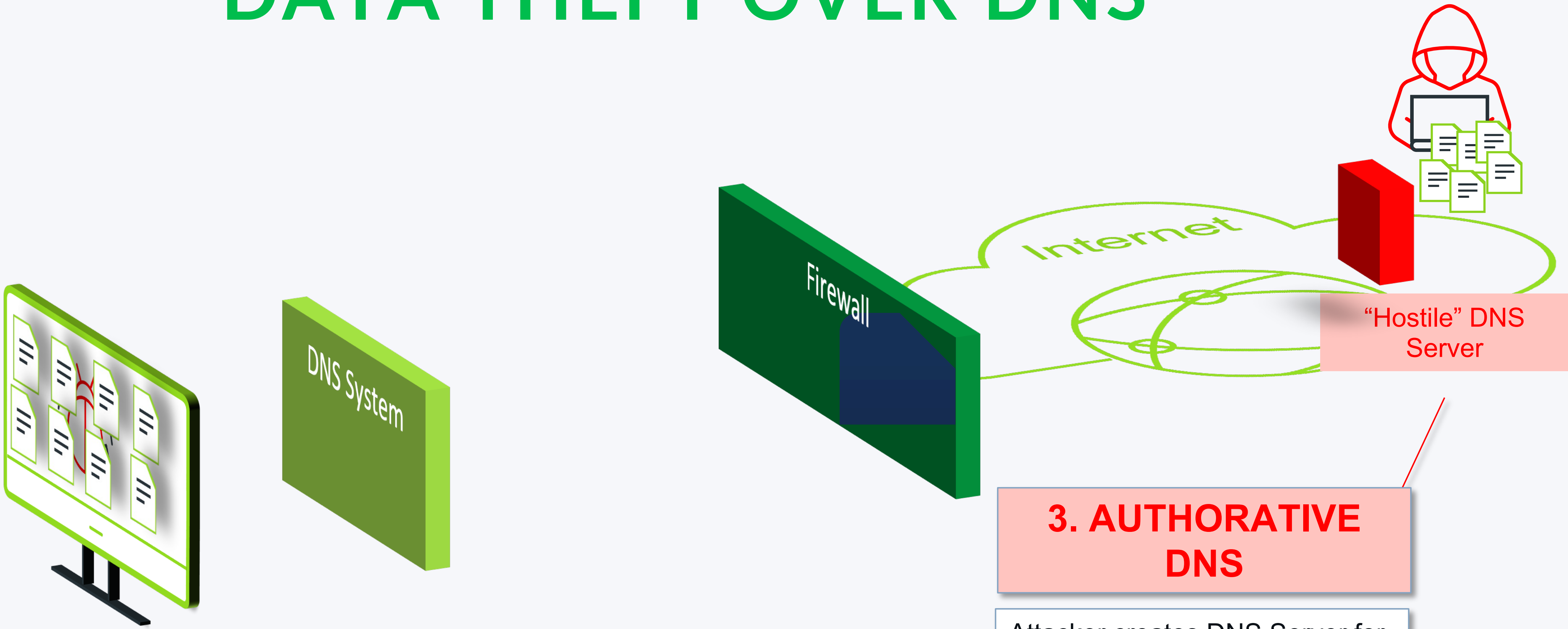
DATA THEFT OVER DNS



2. FILES PROCESS

Discoveres files are “broken” into multiple small fragments

DATA THEFT OVER DNS



“Hostile” DNS Server

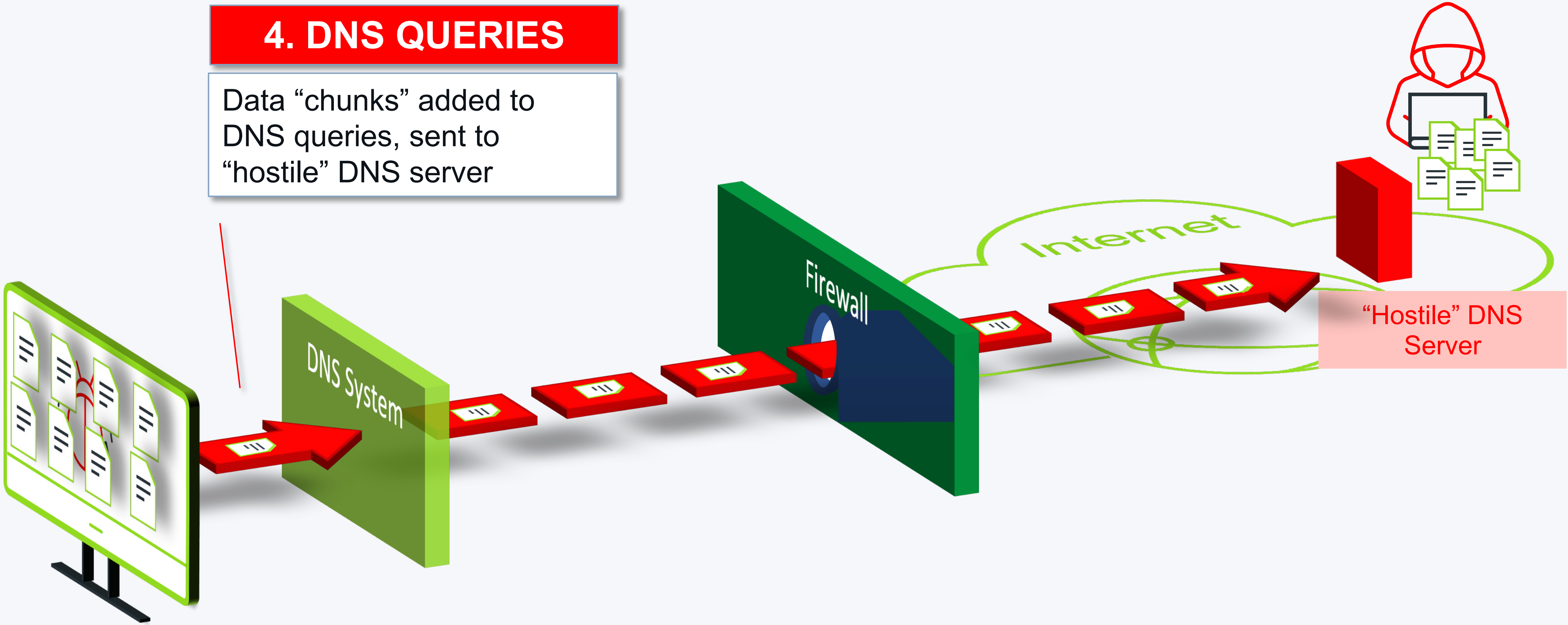
3. AUTHORATIVE DNS

Attacker creates DNS Server for their domains

DATA THEFT OVER DNS

4. DNS QUERIES

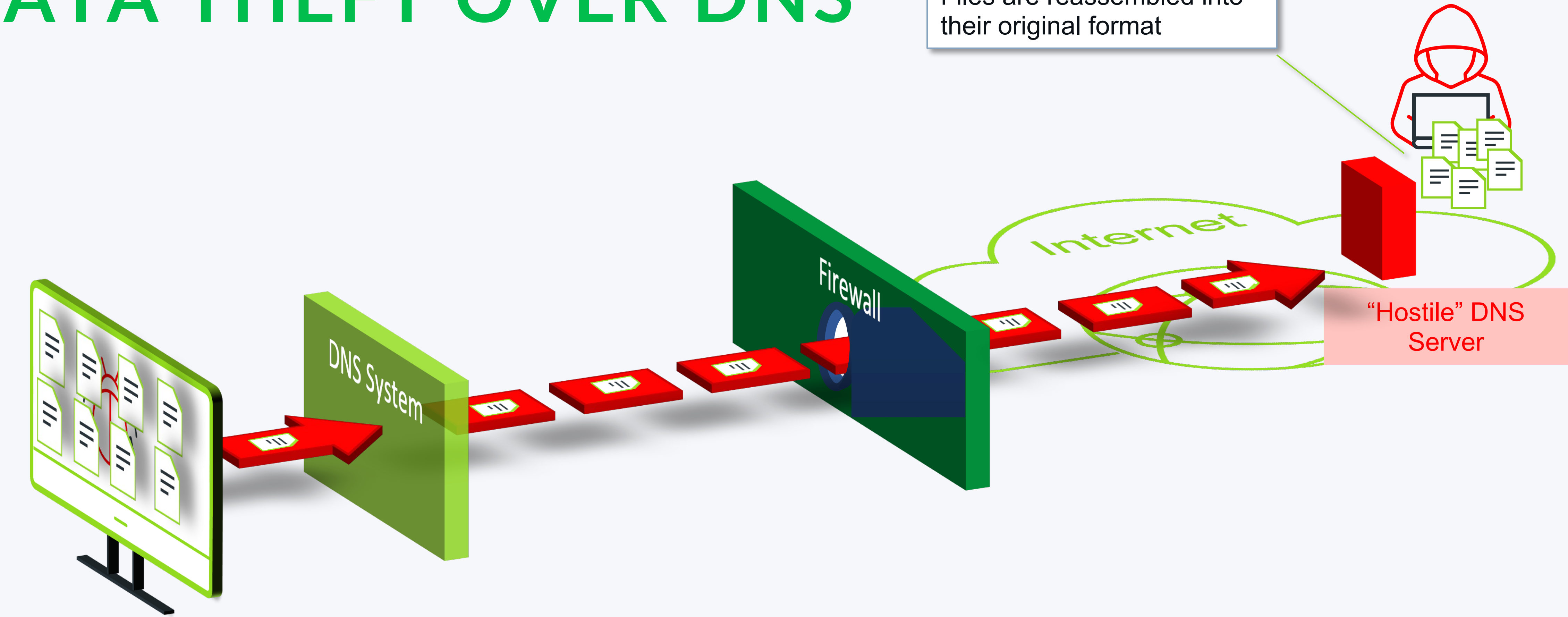
Data “chunks” added to DNS queries, sent to “hostile” DNS server



DATA THEFT OVER DNS

5. FILES EXFILTRATED

Files are reassembled into their original format



Y SEGURAMENTE

TE ESTÁ PASANDO A TÍ

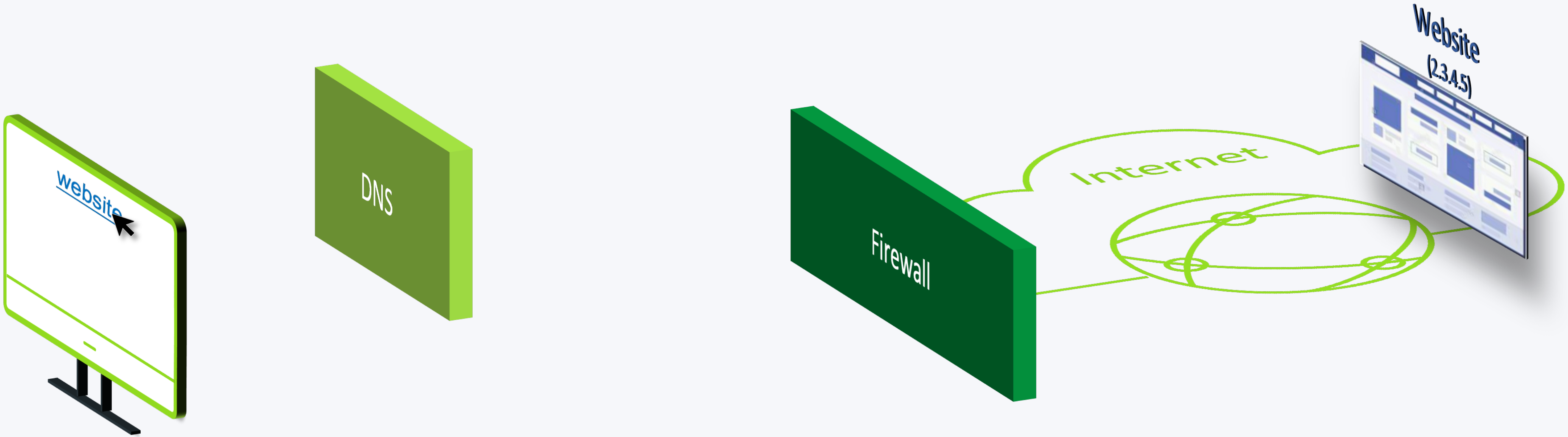
(solo que no lo sabes)

*NSA

¿CÓMO ME PROTEJO

DEL MALWARE?

B1TD MALWARE/RANSOMWARE PROTECTION

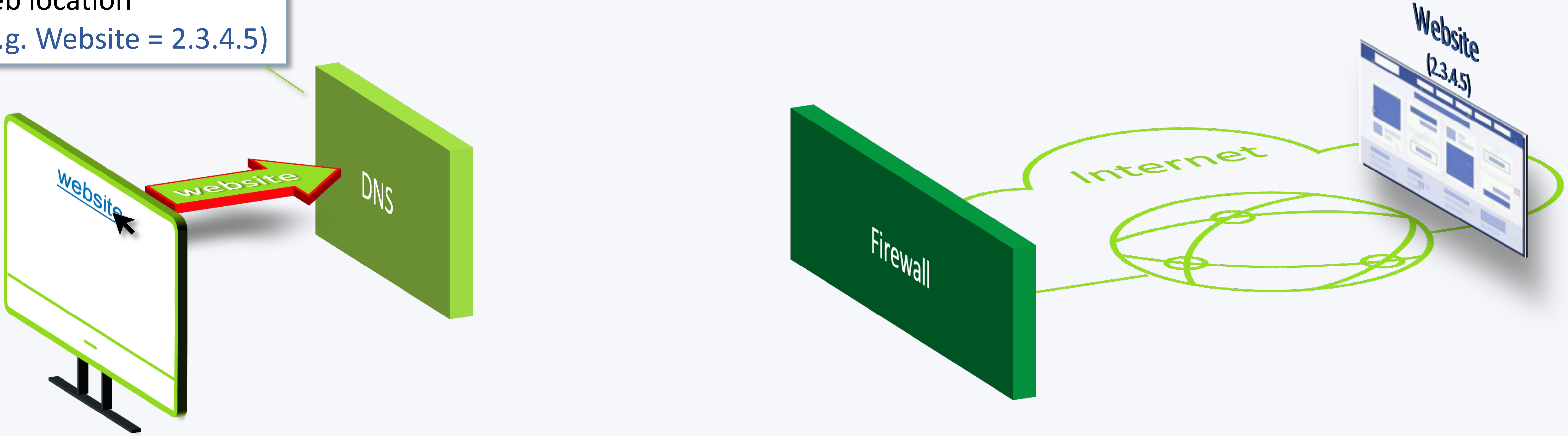


B1TD MALWARE/RANSOMWARE PROTECTION

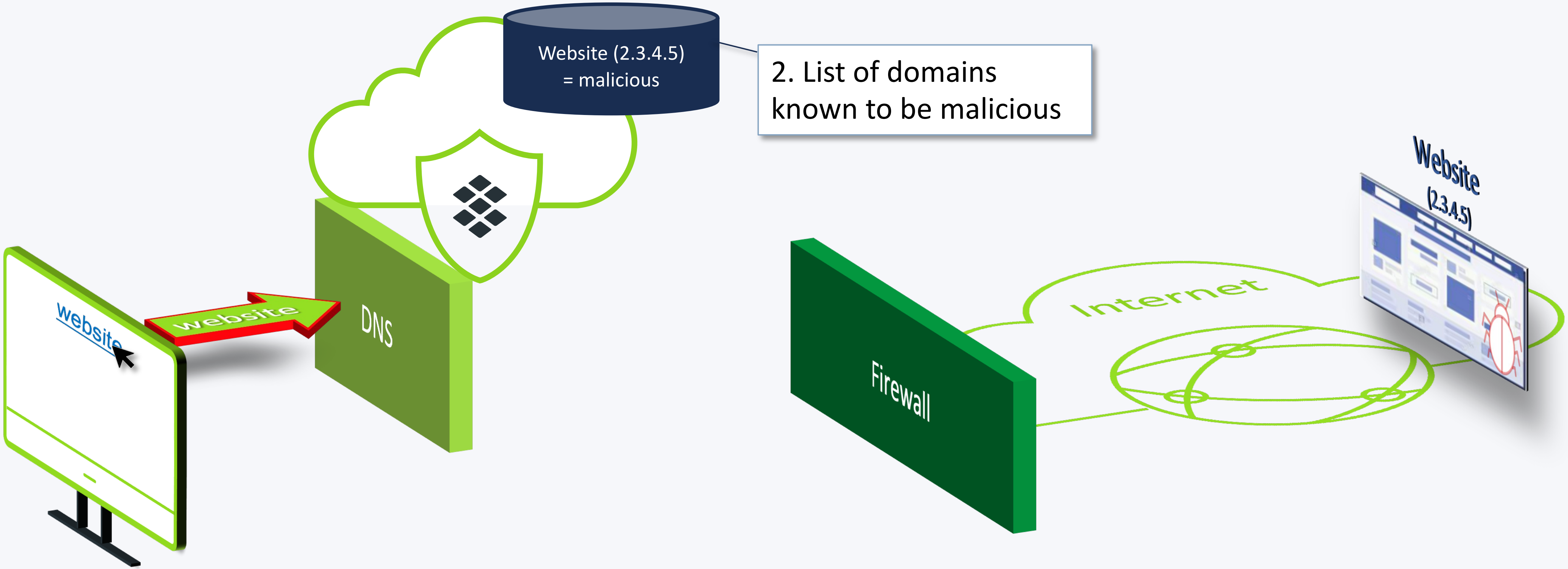
1. DNS REQUEST

Request IP address for web location

(E.g. Website = 2.3.4.5)

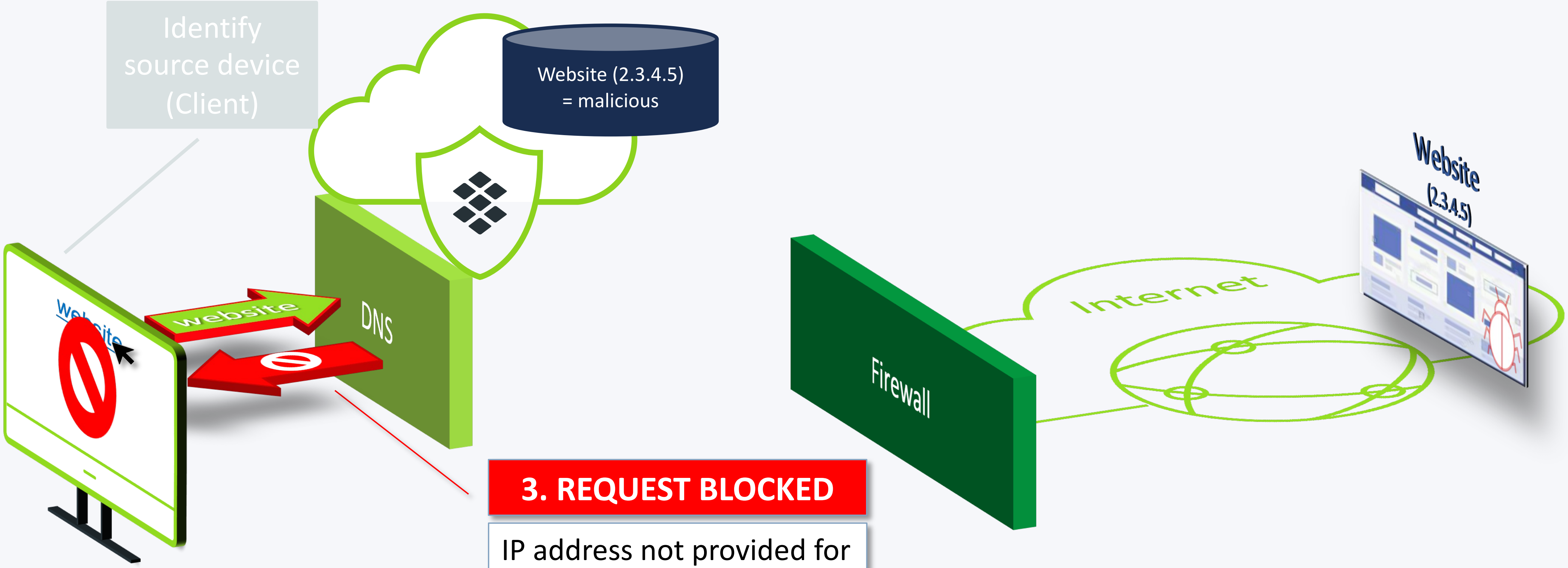


B1TD MALWARE/RANSOMWARE PROTECTION



2. List of domains known to be malicious

B1TD MALWARE/RANSOMWARE PROTECTION


Identify source device (Client)
Website (2.3.4.5) = malicious
website
website
DNS
Firewall
Internet
Website (2.3.4.5)

3. REQUEST BLOCKED

IP address not provided for website location

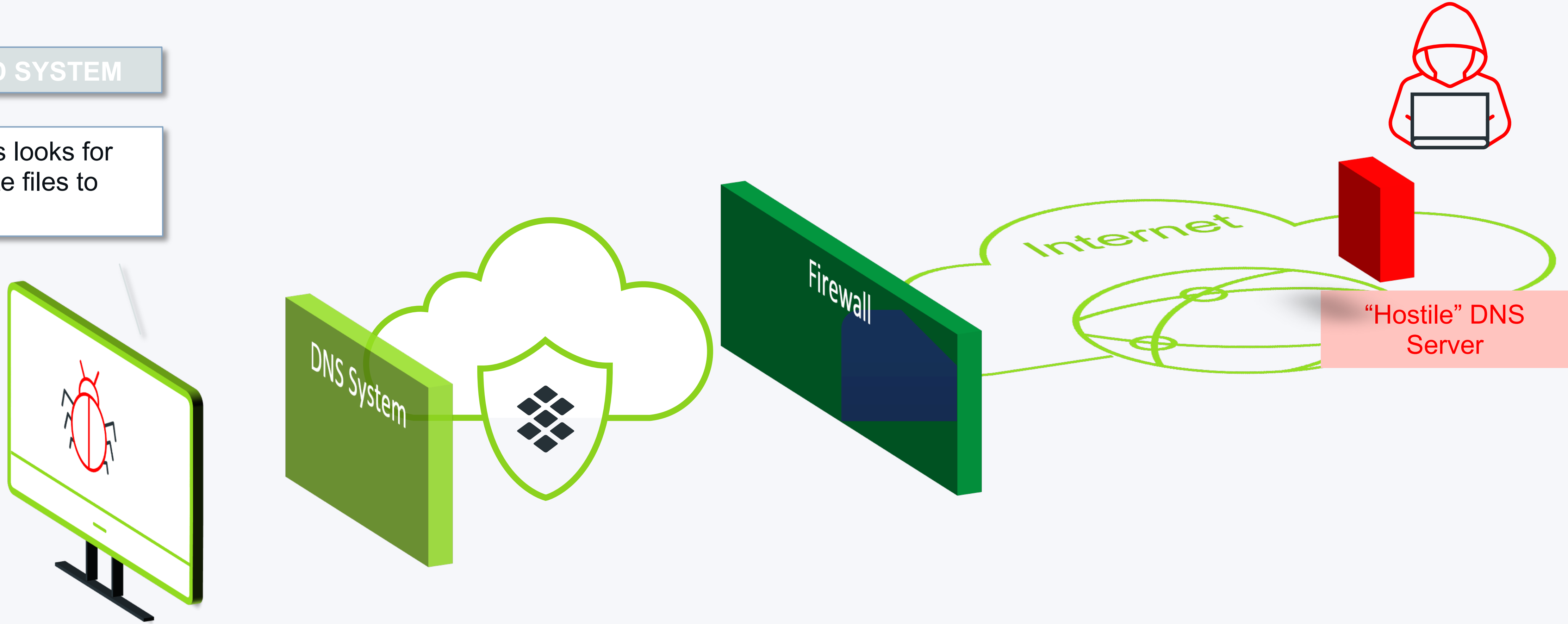
¿CÓMO ME PROTEJO CONTRA LA

EXFILTRACIÓN DE DATOS?

INFOBLOX PROTECTION FROM DATA THEFT

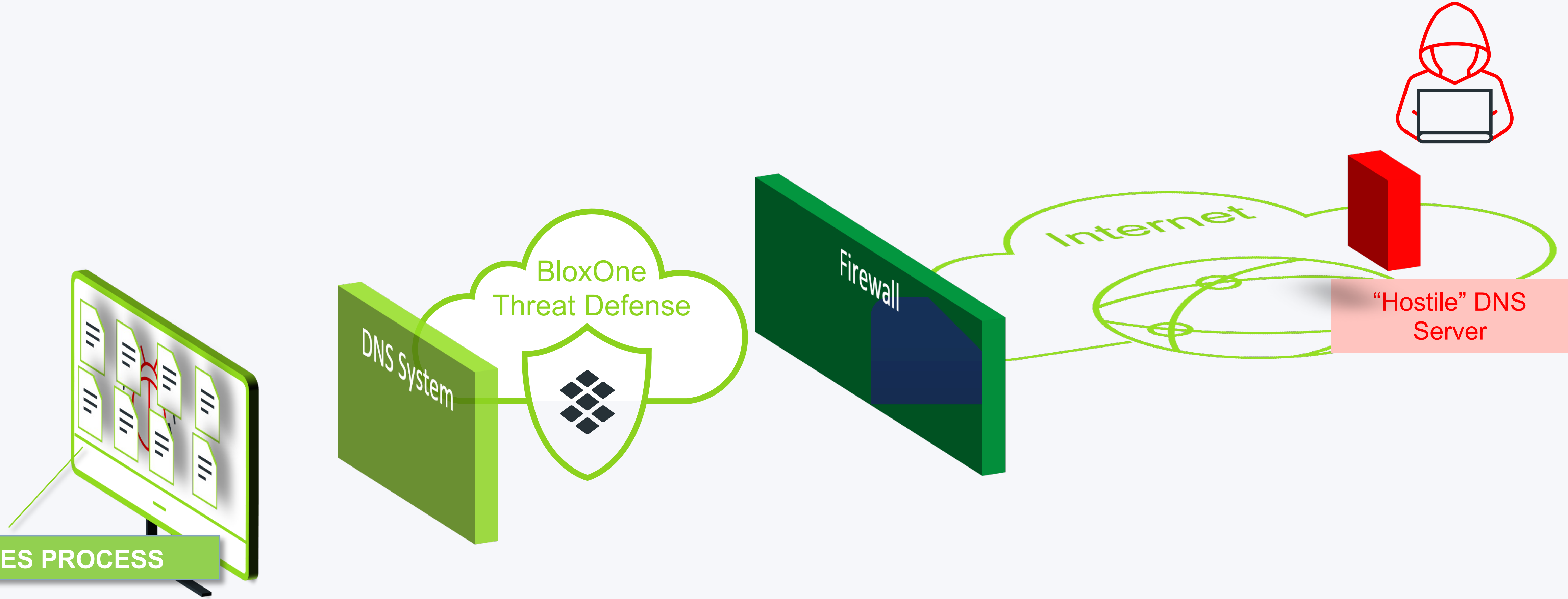
1. INFECTED SYSTEM

Malware breaks looks for local and remote files to exfiltrate



“Hostile” DNS Server

INFOBLOX PROTECTION FROM DATA THEFT



2. FILES PROCESS

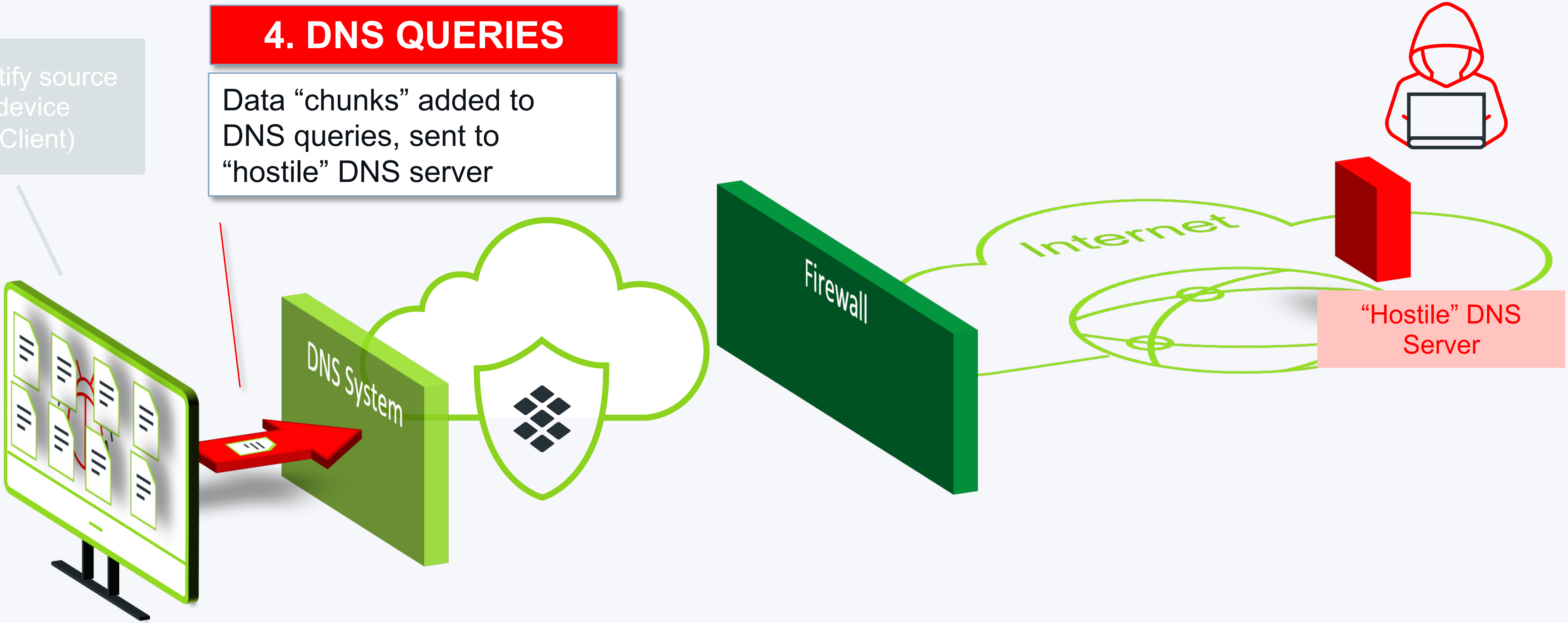
Discoveres files are "broken" into multiple small fragments

INFOBLOX PROTECTION FROM DATA THEFT

Identify source device (Client)

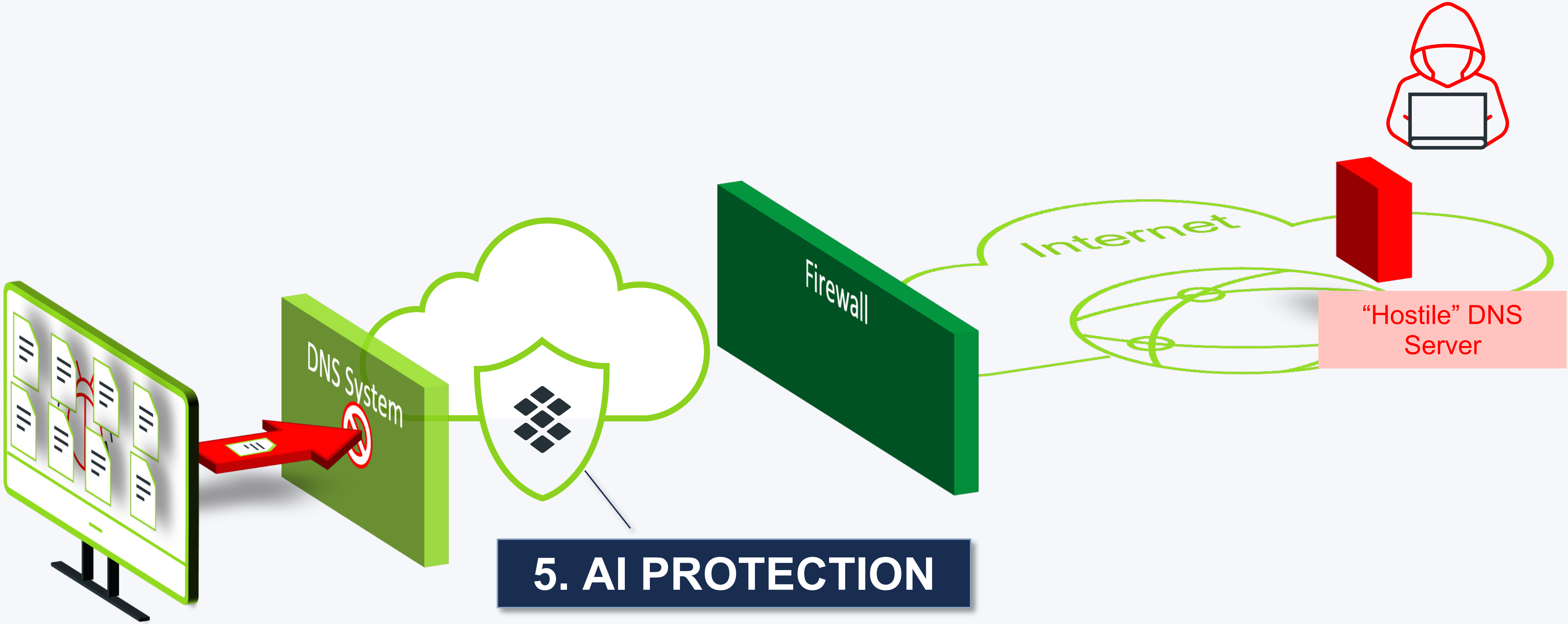
4. DNS QUERIES

Data “chunks” added to DNS queries, sent to “hostile” DNS server



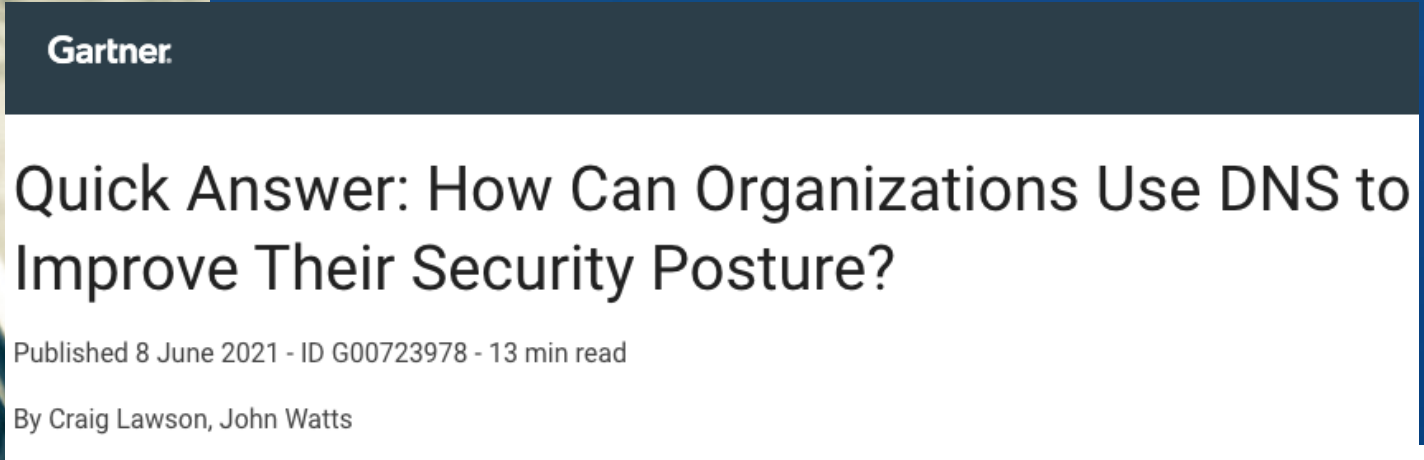
“Hostile” DNS Server

INFOBLOX PROTECTION FROM DATA THEFT



5. AI PROTECTION

Threat Defense AI+ML identify data added to DNS queries and block



Gartner

Quick Answer: How Can Organizations Use DNS to Improve Their Security Posture?

Published 8 June 2021 - ID G00723978 - 13 min read

By Craig Lawson, John Watts

A Forrester Consulting
Thought Leadership Paper
Commissioned By Infoblox

July 2020

Accelerate Threat Resolution With DNS

Leverage DNS As A First-Level Security Control To Detect, Block, And Investigate Attacks

The Total Economic Impact™ Of Infoblox BloxOne® Threat Defense

Cost Savings And Business Benefits Enabled By BloxOne Threat Defense

AMENAZAS CONSTANTES

Email links

- Sites hosting malicious Domains/IPs (Phishing, Spear Phishing, etc.)

Command and Control traffic

- Malicious code from communicating to attacker CnC/C2 networks

Ransomware attacks

- Blocking clients connecting to control networks

Malware downloads

- Domains/IPs known to be hosting malware

IoT/OT compromise

- Non-human managed devices connecting to attacker control servers

¿PORQUÉ DEBEMOS ASEGURAR EL DNS?

DNS is an “ignored” protocol

- Most other security platforms “ignore” the content of DNS

Malware is leveraging DNS

- Newer advanced malware attacks leverage DNS as a communications channel

DNS Encryption

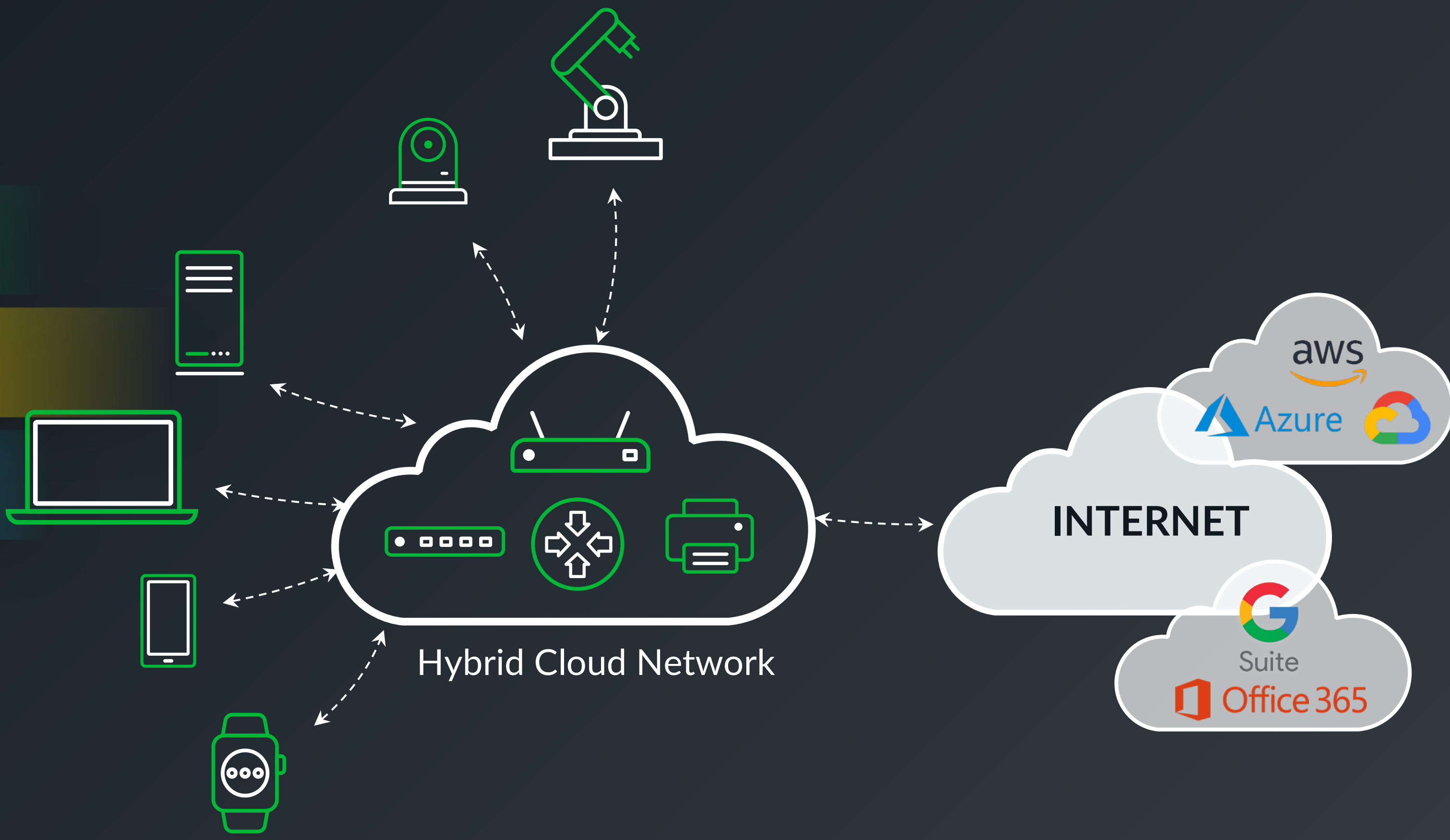
- Attacker communications can be hidden in encrypted DNS, circumventing all other detection tools

VALUE OF DNS IN SECURITY

Spans entire organization

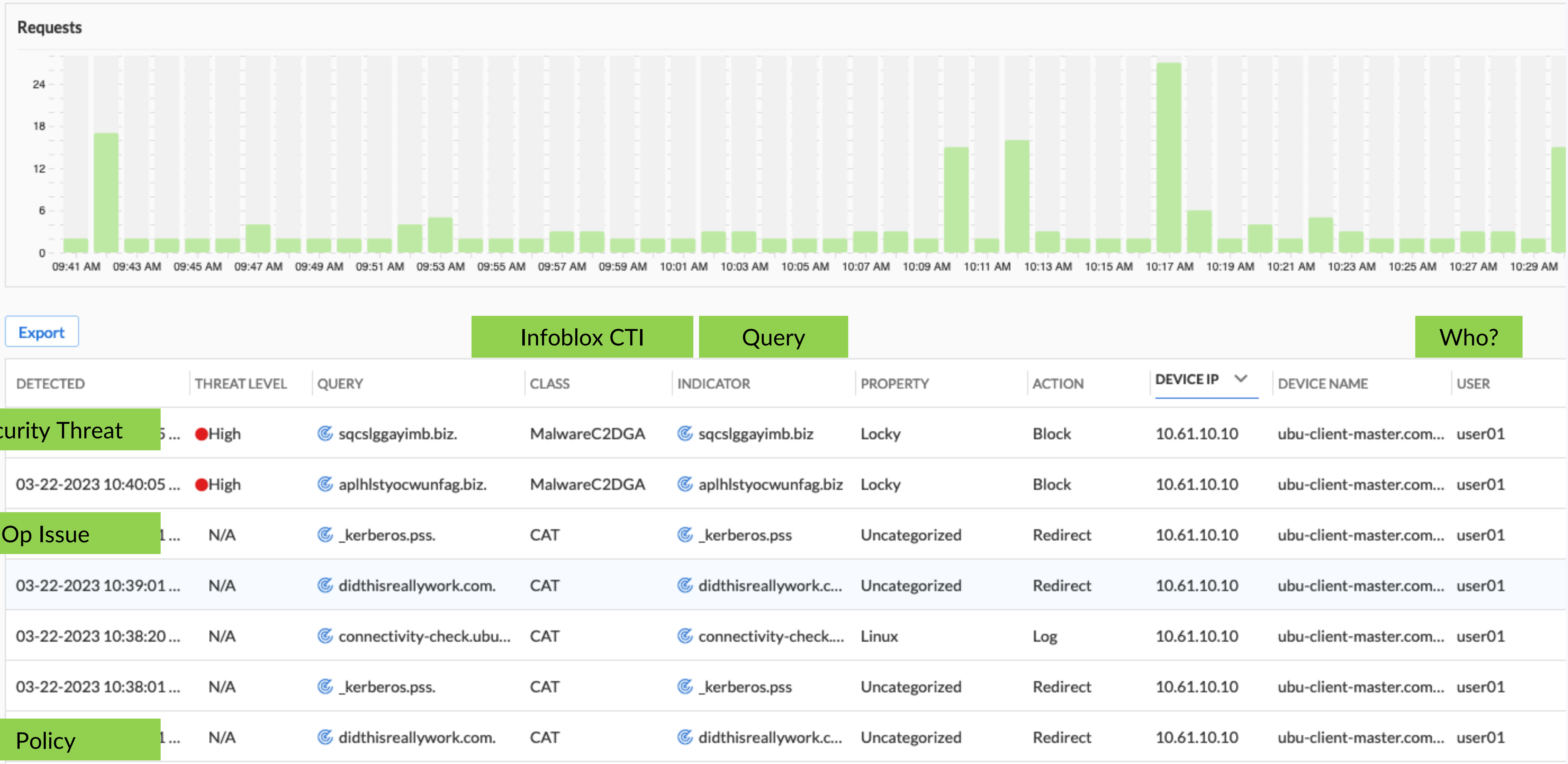
Rich source of telemetry

Closest to Endpoints



infoblox

INFOBLOX CLOUD PORTAL



Infoblox CTI

Query

Who?

Security Threat

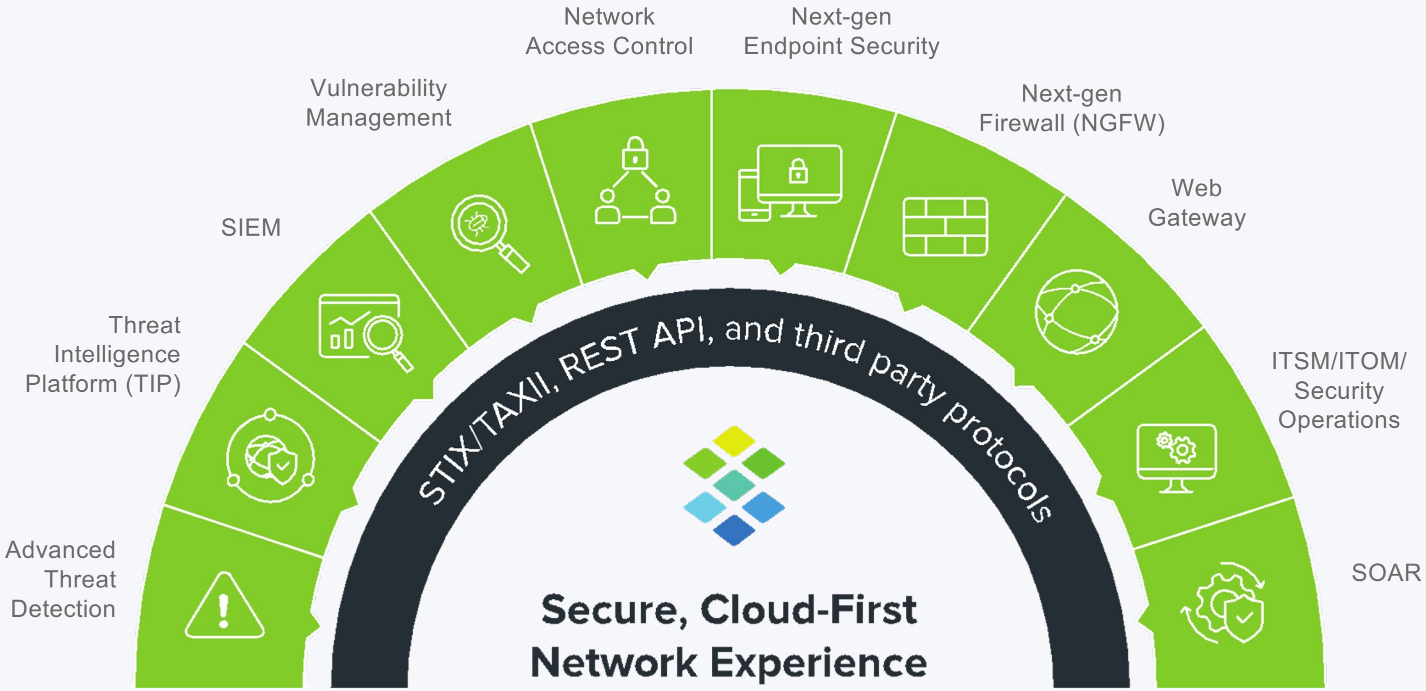
Op Issue

Policy

DETECTED	THREAT LEVEL	QUERY	CLASS	INDICATOR	PROPERTY	ACTION	DEVICE IP	DEVICE NAME	USER
5 ...	●High	sqcslggayimb.biz.	MalwareC2DGA	sqcslggayimb.biz	Locky	Block	10.61.10.10	ubu-client-master.com...	user01
03-22-2023 10:40:05 ...	●High	aplhlstyocwunfag.biz.	MalwareC2DGA	aplhlstyocwunfag.biz	Locky	Block	10.61.10.10	ubu-client-master.com...	user01
1 ...	N/A	_kerberos.pss.	CAT	_kerberos.pss	Uncategorized	Redirect	10.61.10.10	ubu-client-master.com...	user01
03-22-2023 10:39:01 ...	N/A	didthisreallywork.com.	CAT	didthisreallywork.c...	Uncategorized	Redirect	10.61.10.10	ubu-client-master.com...	user01
03-22-2023 10:38:20 ...	N/A	connectivity-check.ubu...	CAT	connectivity-check....	Linux	Log	10.61.10.10	ubu-client-master.com...	user01
03-22-2023 10:38:01 ...	N/A	_kerberos.pss.	CAT	_kerberos.pss	Uncategorized	Redirect	10.61.10.10	ubu-client-master.com...	user01
1 ...	N/A	didthisreallywork.com.	CAT	didthisreallywork.c...	Uncategorized	Redirect	10.61.10.10	ubu-client-master.com...	user01

Cybersecurity Ecosystem

- Automatically notify ecosystem of events in real time
- Trigger remediation action
- Share network context


Advanced Threat Detection
Threat Intelligence Platform (TIP)
SIEM
Vulnerability Management
Network Access Control
Next-gen Endpoint Security
Next-gen Firewall (NGFW)
Web Gateway
ITSM/ITOM/ Security Operations
SOAR
STIX/TAXII, REST API, and third party protocols
Secure, Cloud-First Network Experience

SECURITY ORCHESTRATION

- Faster remediation
- Improve ROI of ecosystem
- Bridge silos

Why Infoblox

MISSION

Empowering organizations to manage their continuously evolving growing networks simply and securely.

OFFERINGS

Core Network Services, Cybersecurity, Secure Edge Services

12,000+ CUSTOMERS

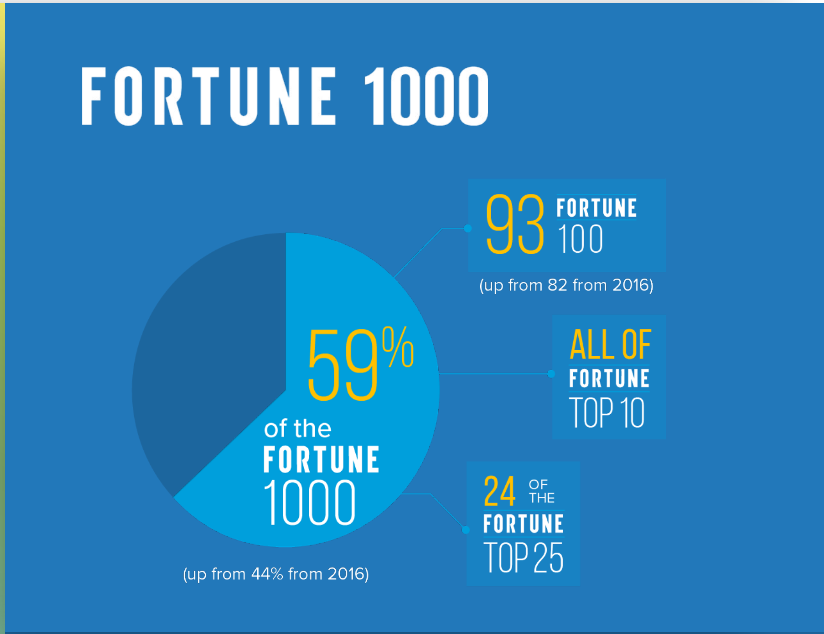
50% MARKET SHARE

133 COUNTRIES

1000+ PARTNERS

53.4 NPS

95.4 CUSTOMERS SAT.



FORTUNE 1000

59% of the FORTUNE 1000

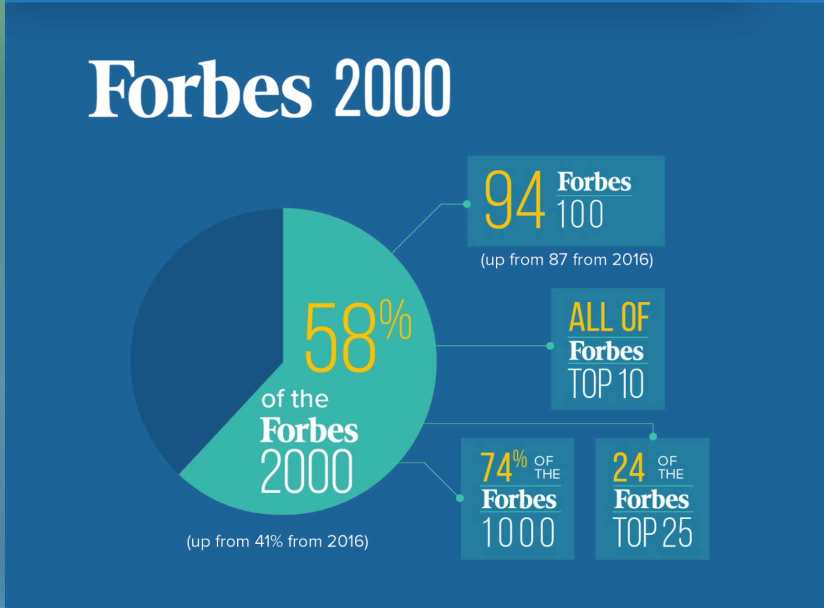
(up from 44% from 2016)

93 FORTUNE 100

(up from 82 from 2016)

ALL OF FORTUNE TOP 10

24 OF THE FORTUNE TOP 25



Forbes 2000

58% of the Forbes 2000

(up from 41% from 2016)

94 Forbes 100

(up from 87 from 2016)

ALL OF Forbes TOP 10

74% OF THE Forbes 1000

24 OF THE Forbes TOP 25

OUR WAY TO PROTECT

- Block threats at earliest point of connection
- Protect any app/device anywhere and IoT/OT
- Hybrid cloud visibility and related compliance
- Close security gaps using threat hunting
- Automate cybersecurity stack

infoblox®

¡GRACIAS!