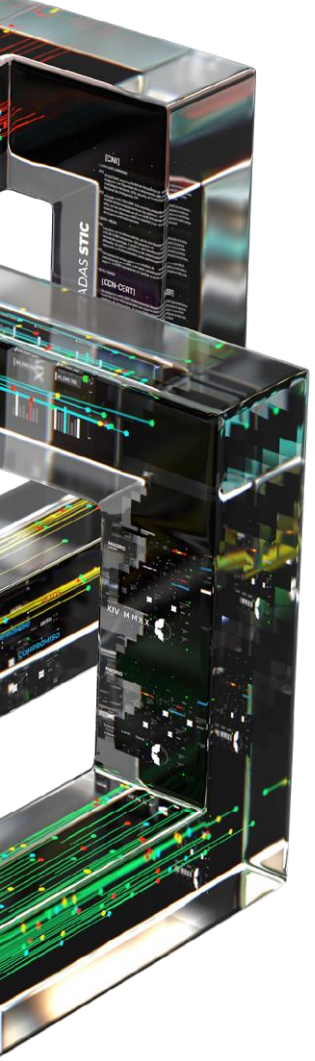
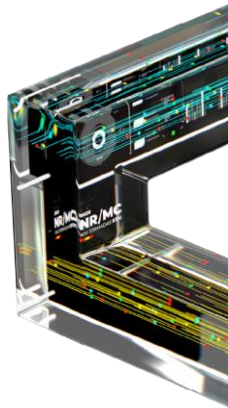


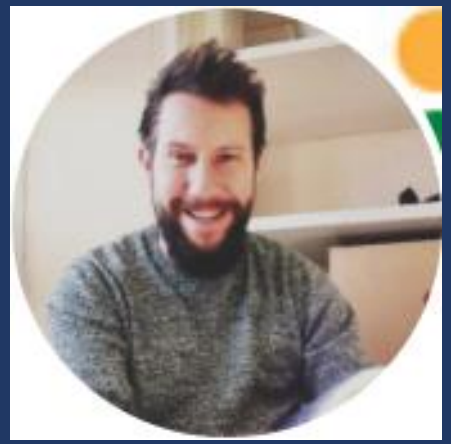
#XIVJORNADASCCNCERT

BAD BOTS:

El 25% del tráfico web está listo para interrumpir su servicio



ccn-cert
centro criptológico nacional



Juan José Navarro

Radware

juann@radware.com

BREAKING NEWS!

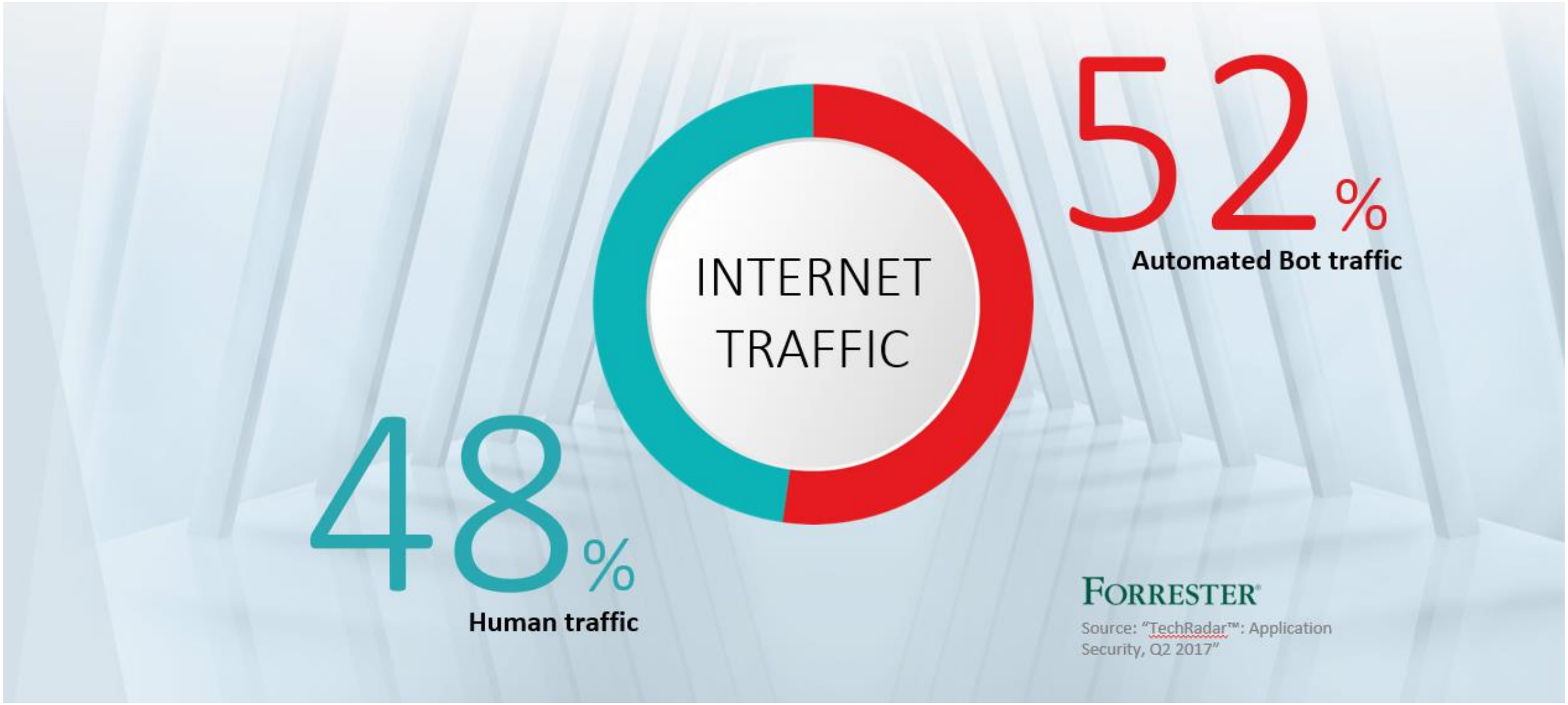
The North Face sufre un ataque de relleno de contraseñas

13 noviembre, 2020 Por Jose Ignacio Palacios Ortega — Leave a Comment

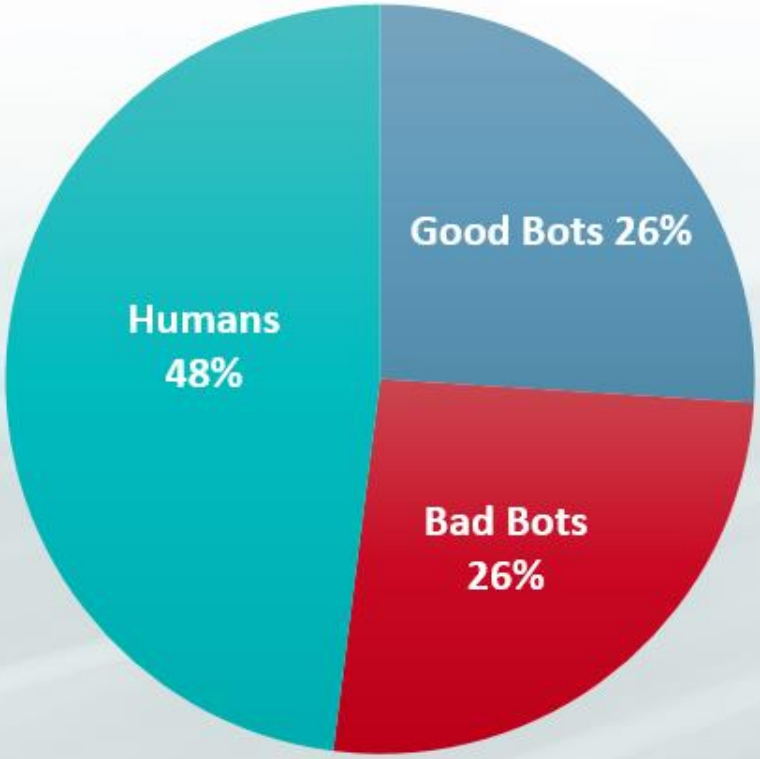
Se ha publicado la noticia de un ataque dirigido a la compañía norteamericana *The North Face* que ha obligado a un restablecimiento de contraseña a sus usuarios.



AUTOMATED BOTS ARE TAKING OVER THE INTERNET



AUTOMATED BOTS ARE TAKING OVER THE INTERNET



26%

Of the internet traffic is generated by bad bots

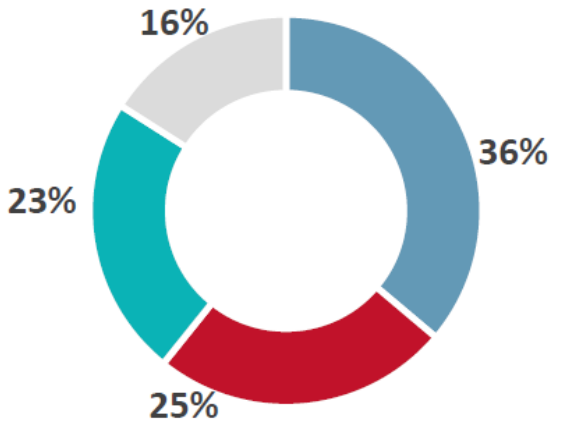
4 in 5

cannot distinguish between 'good' & 'bad' bots

AUTOMATED BOTS ARE TAKING OVER THE INTERNET

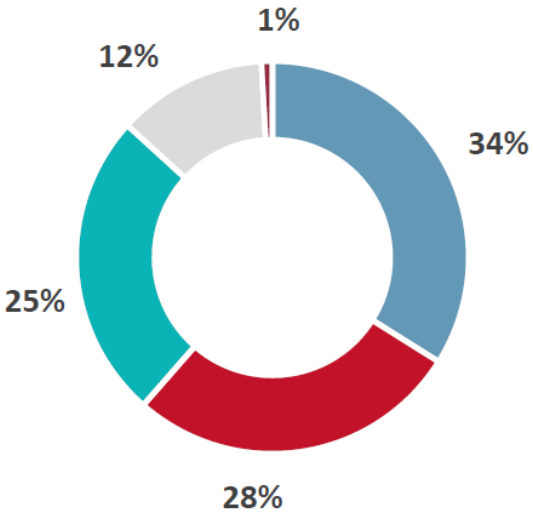
TOP ATTACKED VERTICALS

- ONLINE COMMERCE & GAMING
- HIGH TECH PRODUCTS & SERVICES
- BANKING & FINANCE
- SERVICE PROVIDERS



BAD BOT DISTRIBUTION BY VERTICAL

- Media
- Travel
- Retail
- Banking
- Entertainment



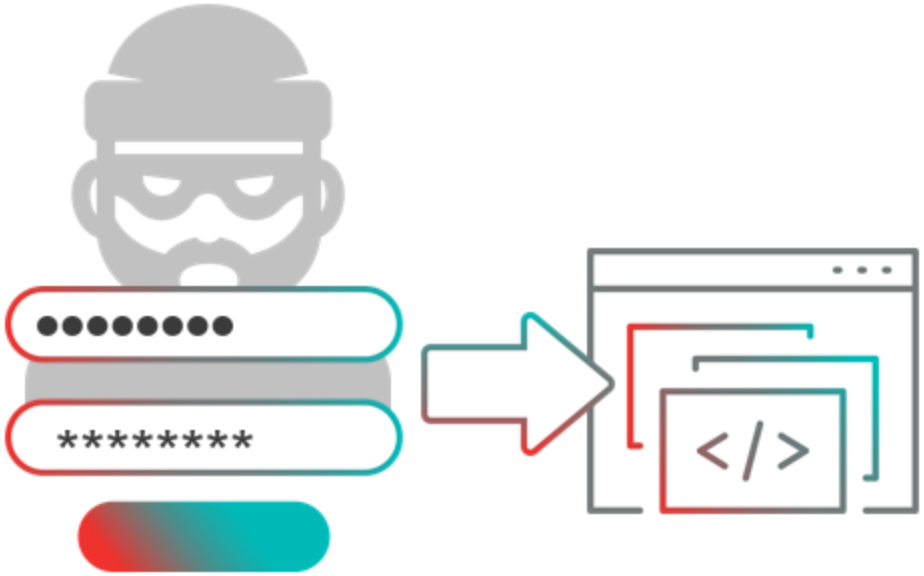
COMMON BOT ATTACKS



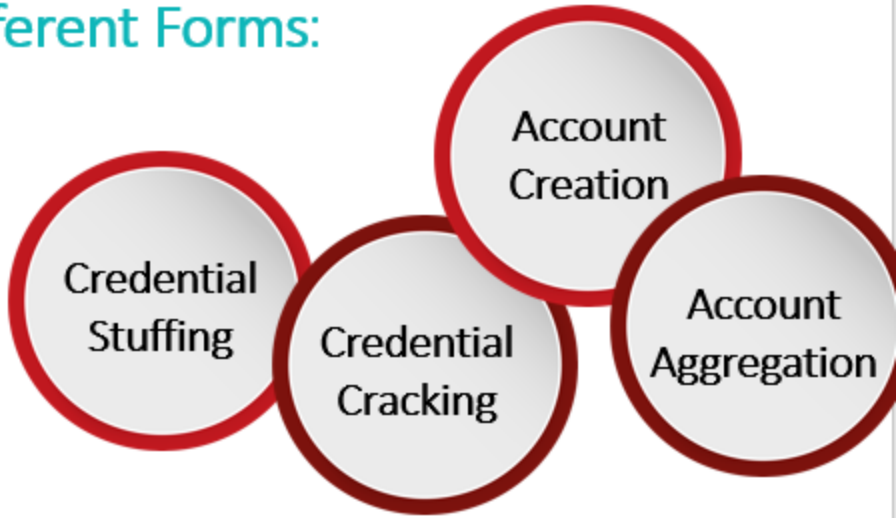
THE RISK: ACCOUNT TAKE OVER

Using another person's account info to obtain products & services

How Does it Work?



Different Forms:



Data Theft

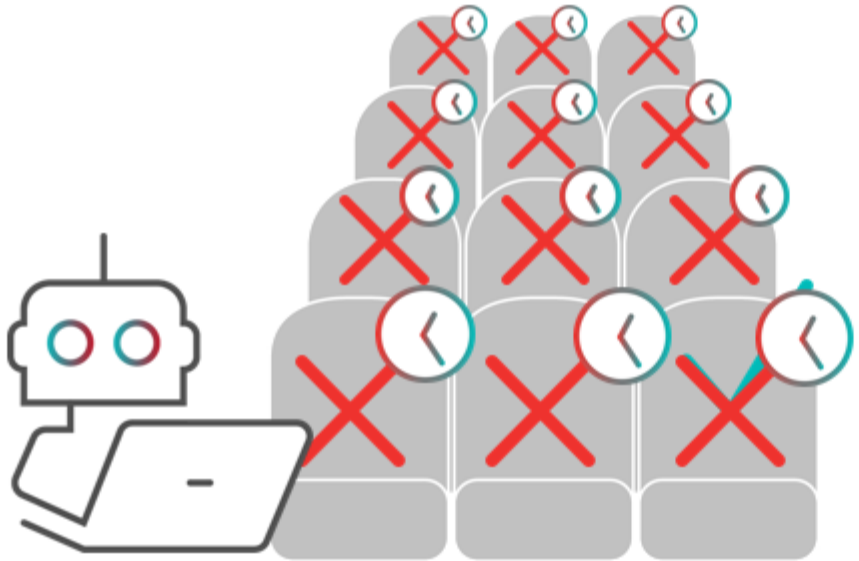
Loss of Reputation

Financial Loss

THE RISK: DENIAL OF INVENTORY

Deplete goods or services stock without ever completing the purchase or committing to the transaction

How Does it Work?



45% Experienced inventory hold-ups*

32% Suffered inventory depletion*

Loss of Users

Loss of Reputation

Loss of Revenue

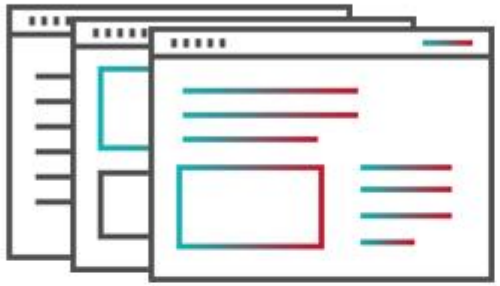
*Source: Radware Research: Web Application Security in a Digitally Connected World, Nov 2017

THE RISK: WEB SCRAPING



Data scraping used for extracting data from websites

How Does it Work?





87% web scraping is a significant threat

40% suffer weekly from web scraping

Data Loss

Loss of Revenue

THE EVOLUTION OF BOTS



BOTS

L1: Script Bot

```
C:\Windows\system32>curl -v localhost
* Rebuilt URL to: localhost/
*   Trying ::1...
* TCP_NODELAY set
* Connected to localhost (::1) port 80 (#0)
> GET / HTTP/1.1
> Host: localhost
> User-Agent: curl/7.55.1
> Accept: */*
>
< HTTP/1.1 200 OK
< Date: Mon, 18 Feb 2019 14:19:52 GMT
< Server: Apache/2.4.34 (Win64) PHP/7.3.2
< Content-Length: 1951
```

TECHNOLOGY

Blacklists

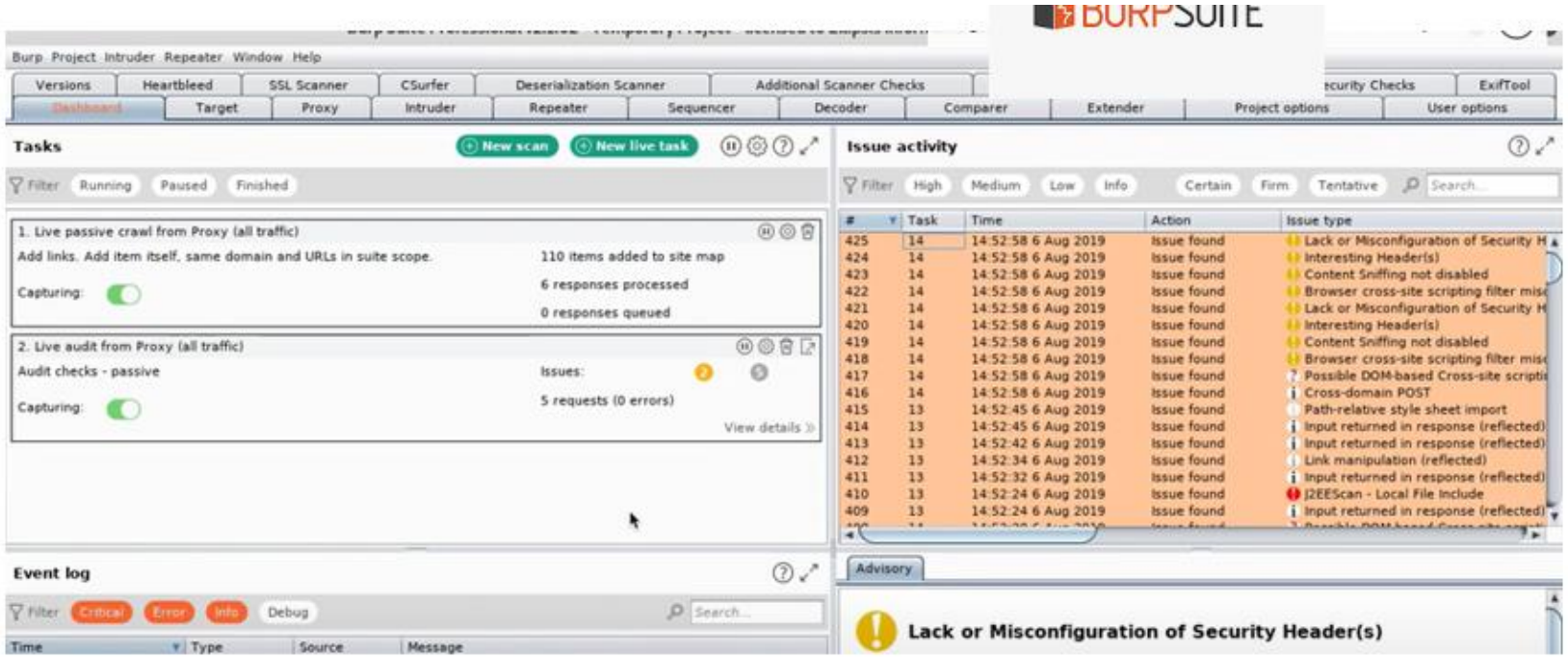
IP, User Agent

THE EVOLUTION OF BOTS

BOTS



L2: Headless Browser Bot



TECHNOLOGY

Device/Browser

Cookie, JS,
Fingerprinting

THE EVOLUTION OF BOTS



BOTS

L3: Human-Like Bot



TECHNOLOGY

Interaction (shallow)

Mouse movement & keystrokes anomalies

User Behavioral Analysis

THE EVOLUTION OF BOTS



BOTS

L4: Distributed Bot

TECHNOLOGY

Intent (deep)

Correlation in intent signatures across devices

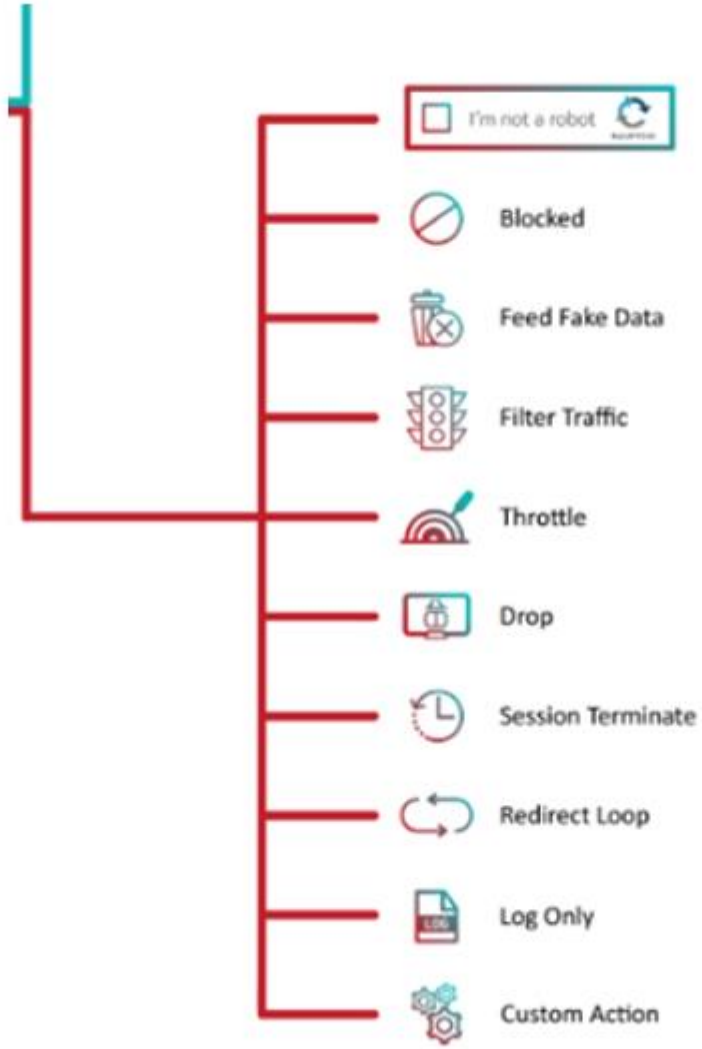
User Behavioral Analysis

¿Cómo funciona Kolotibablo?

El funcionamiento es muy simple. En pocos segundo, tras una pequeña configuración necesarias estarás resolviendo captchas y ganando dinero por ello. Para comenzar a trabajar deberás dirigirte al menú **Captchas » Empezar a trabajar**. Una vez dentro encontrarás un panel como el que verás a continuación



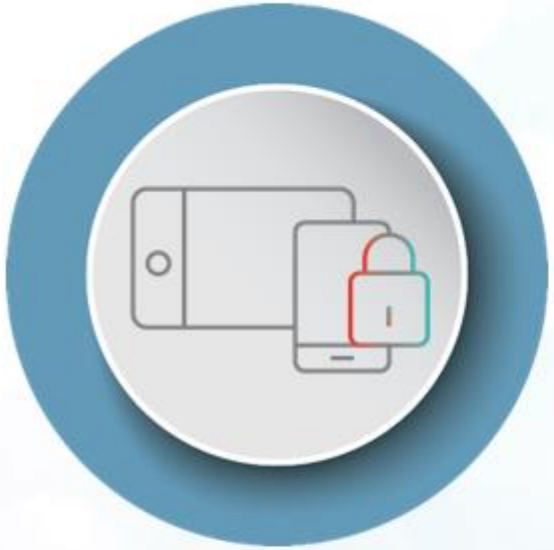
¿DEBEMOS BLOQUEAR SIEMPRE LOS ATAQUES?



BOTS TARGET ALL CHANNELS



WEBSITES



MOBILE APPS



API

SOLUTION REQUIREMENTS



ALL ATTACKS



ALL GENERATIONS



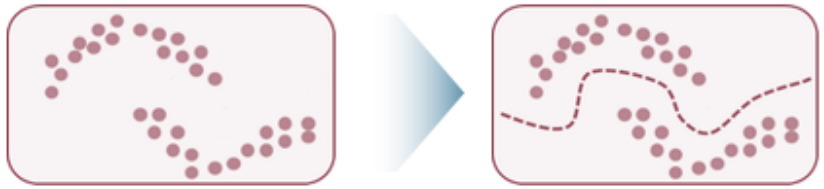
ALL CHANNELS



MINIMUM FALSE POSITIVES

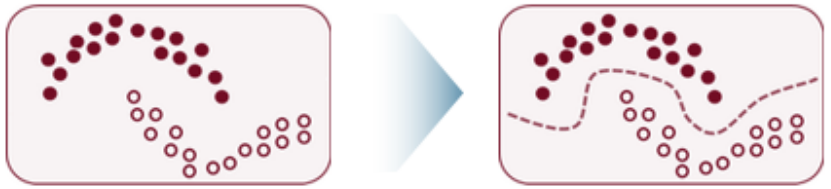
SEMI-SUPERVISED MACHINE LEARNING

Unsupervised Machine-Learning



- Clustering by commonalities
- No direction on good vs. bad
- Risk –> High **False Positives**

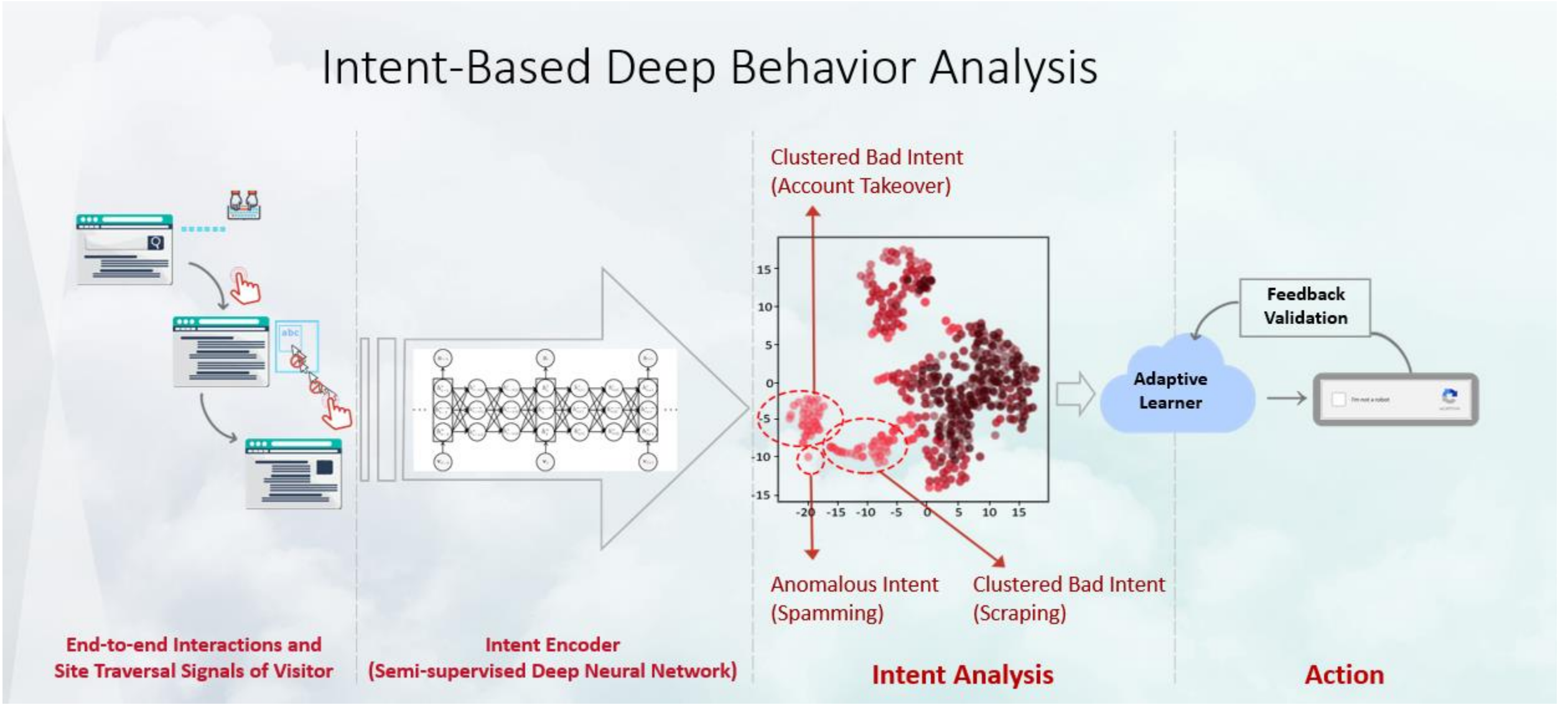
Supervised Machine-Learning



- Guided classification based on past
- New data samples create noise
- Risk –> High **False Negatives**

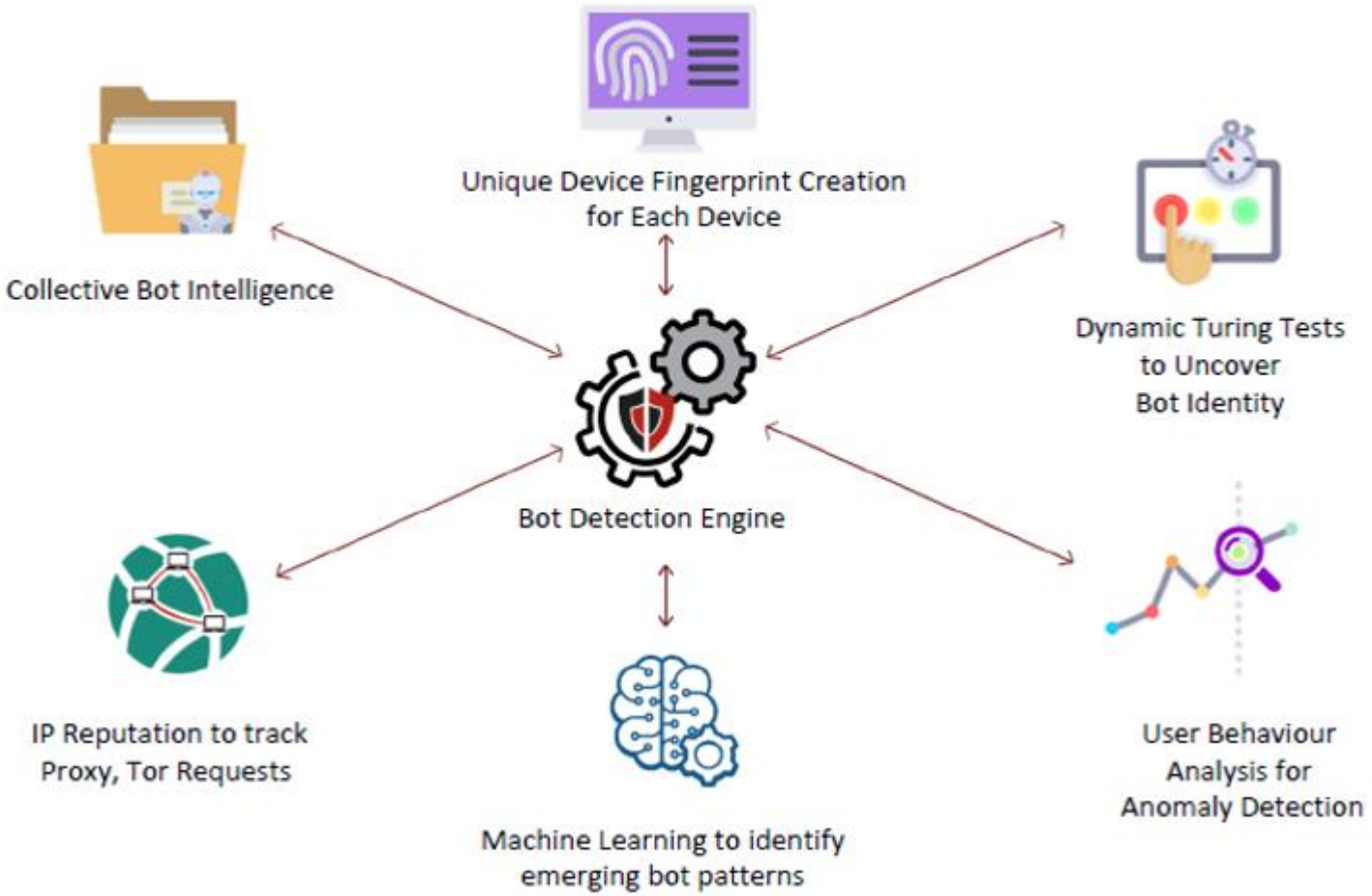
Semi-Supervised: *combined approach yielding highest precision*

AUTOMATED THREATS: GOOD vs. BAD BOTS

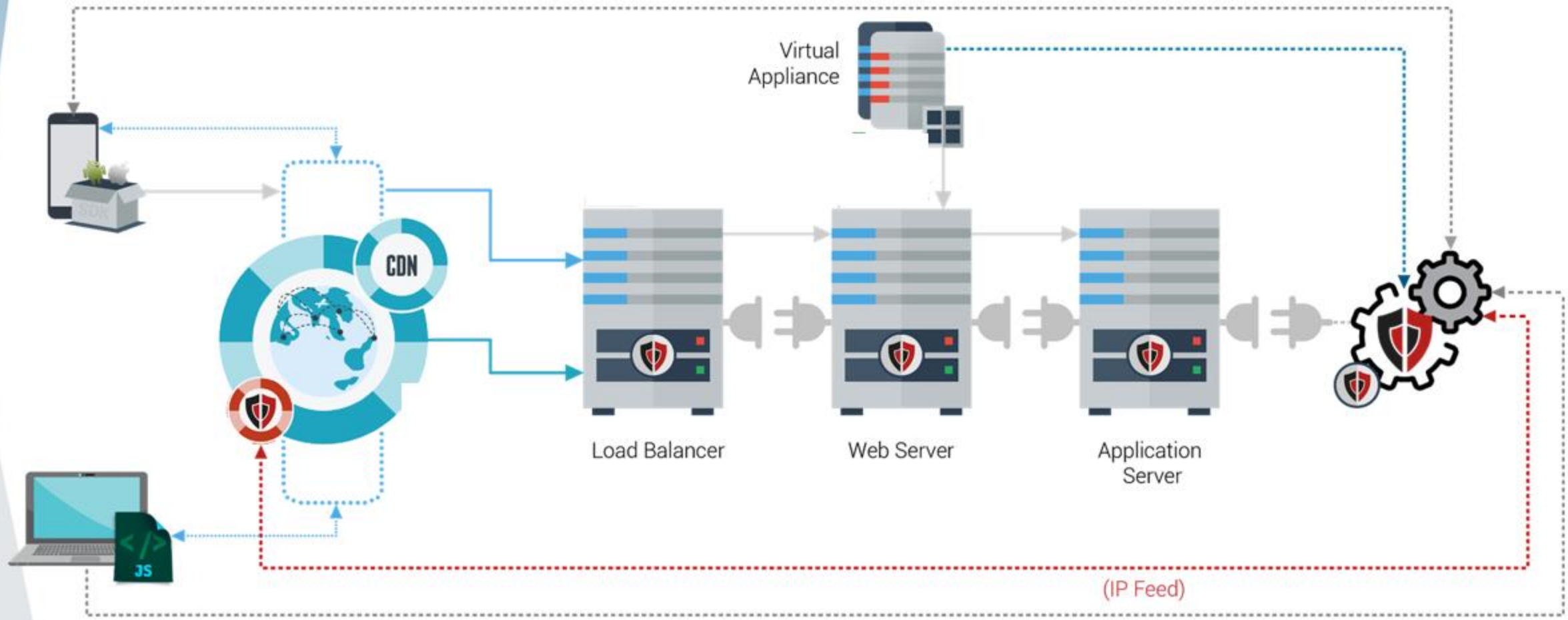


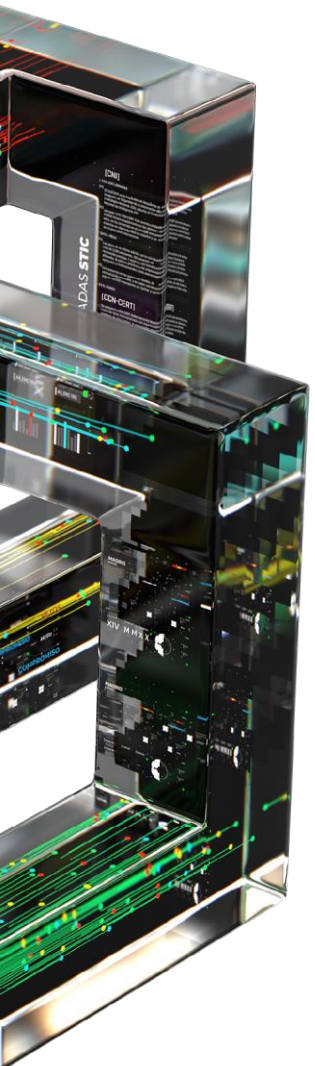
BOT DETECTION ENGINE

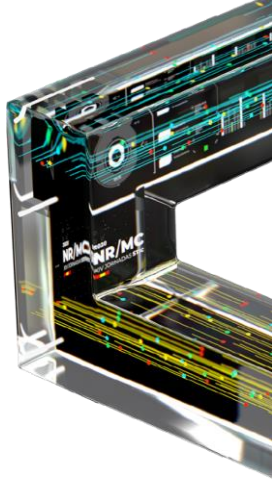
Multiple identification and tracking mechanisms for highest accuracy



INTEGRATION WORKFLOW







MUCHAS GRACIAS

#XIVJORNADASCCNCERT