
Barracuda
TECHSUMMIT19
BARRACUDA TECHNICAL SUMMIT
WAF – Advanced Bot Protection
Deep Dive

Agenda

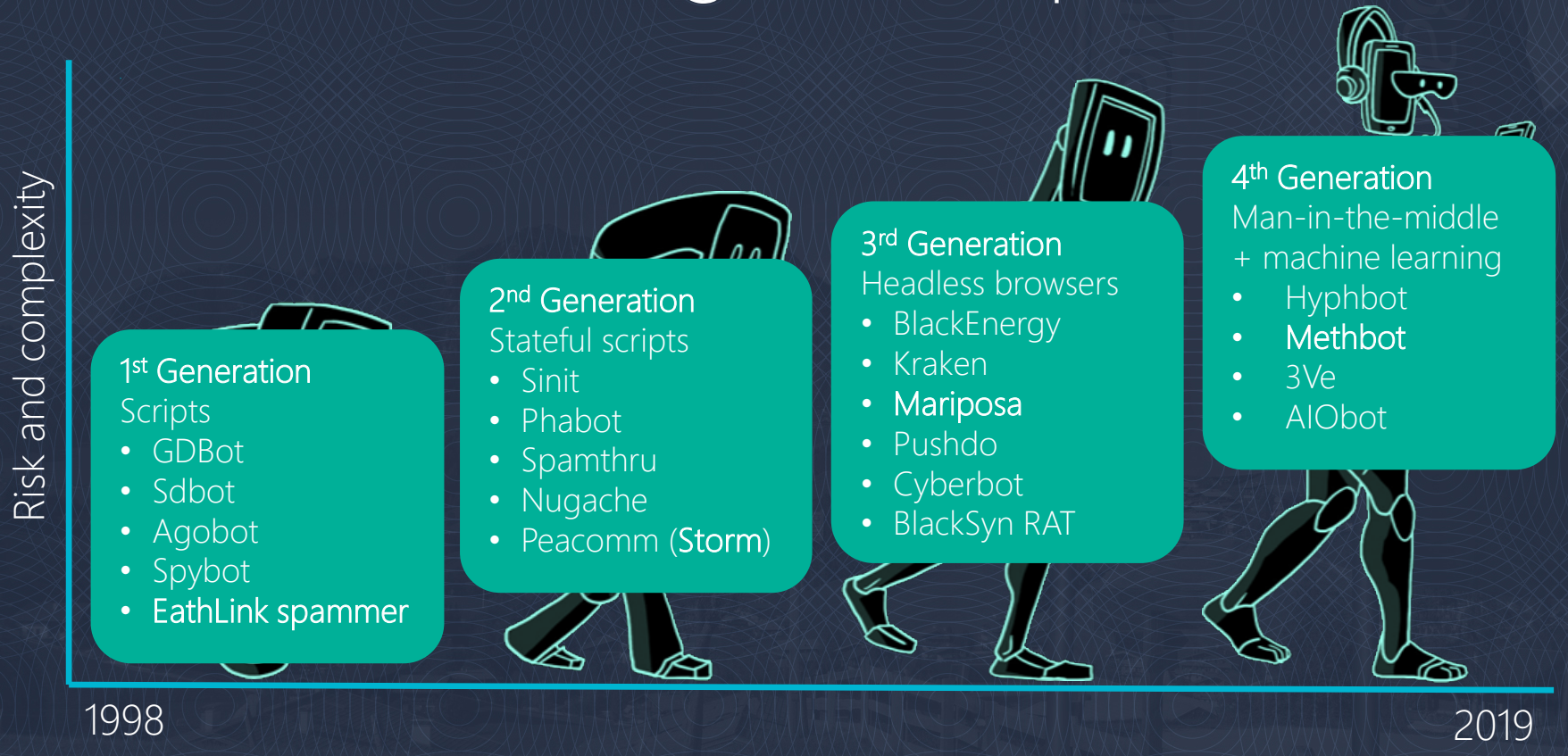
Bots & botnets – a short history

The bot problem - Industry impact

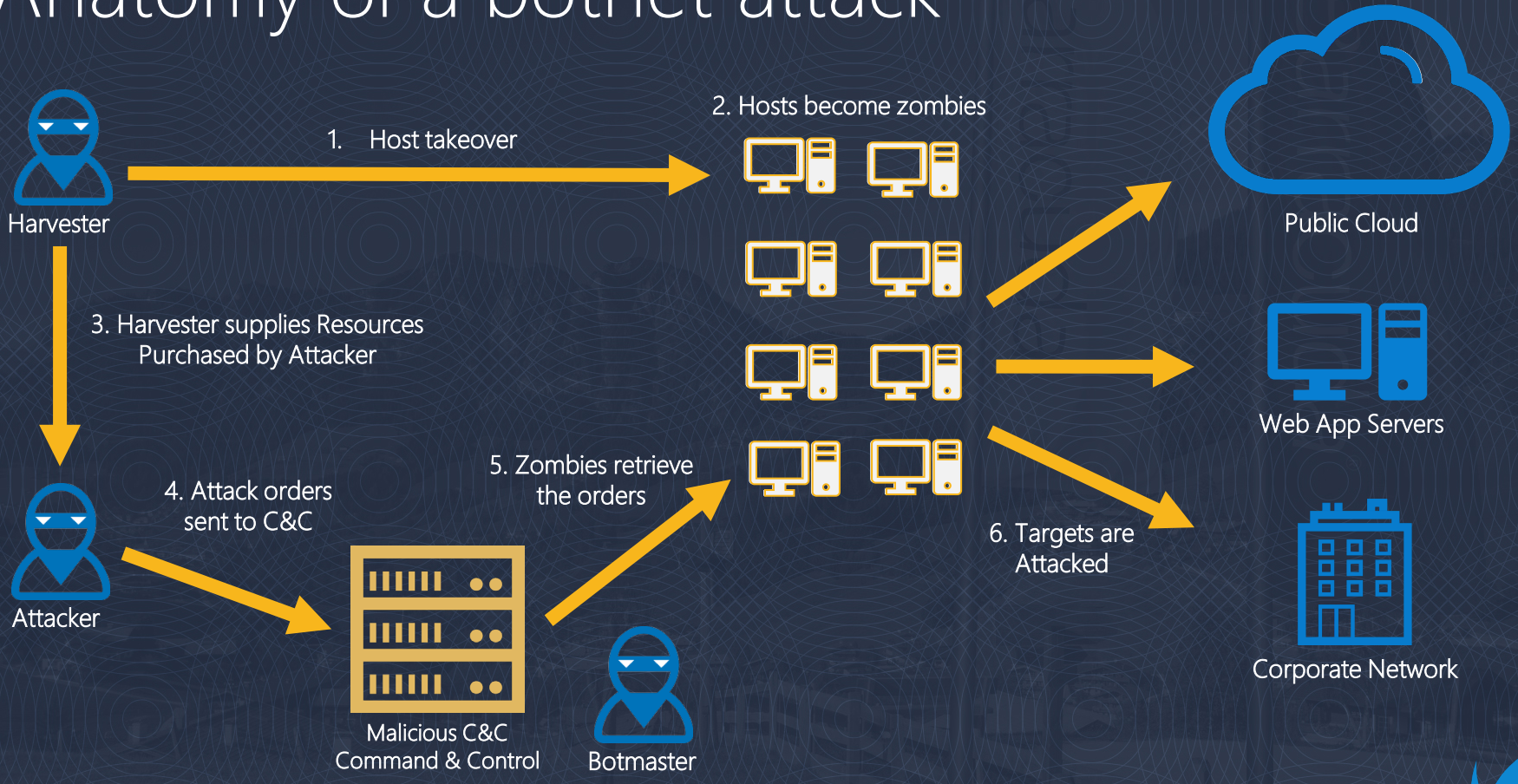
The Barracuda solution

A Short history of bots

Bots are becoming more sophisticated



Anatomy of a botnet attack



The BOT problem

Compromised Credentials

LinkedIn – 117 million account (2012)

Yahoo – 3 billion accounts (2013)

eBay – 145 million accounts (2014)

Talk Talk – 157 thousand accounts (2015)

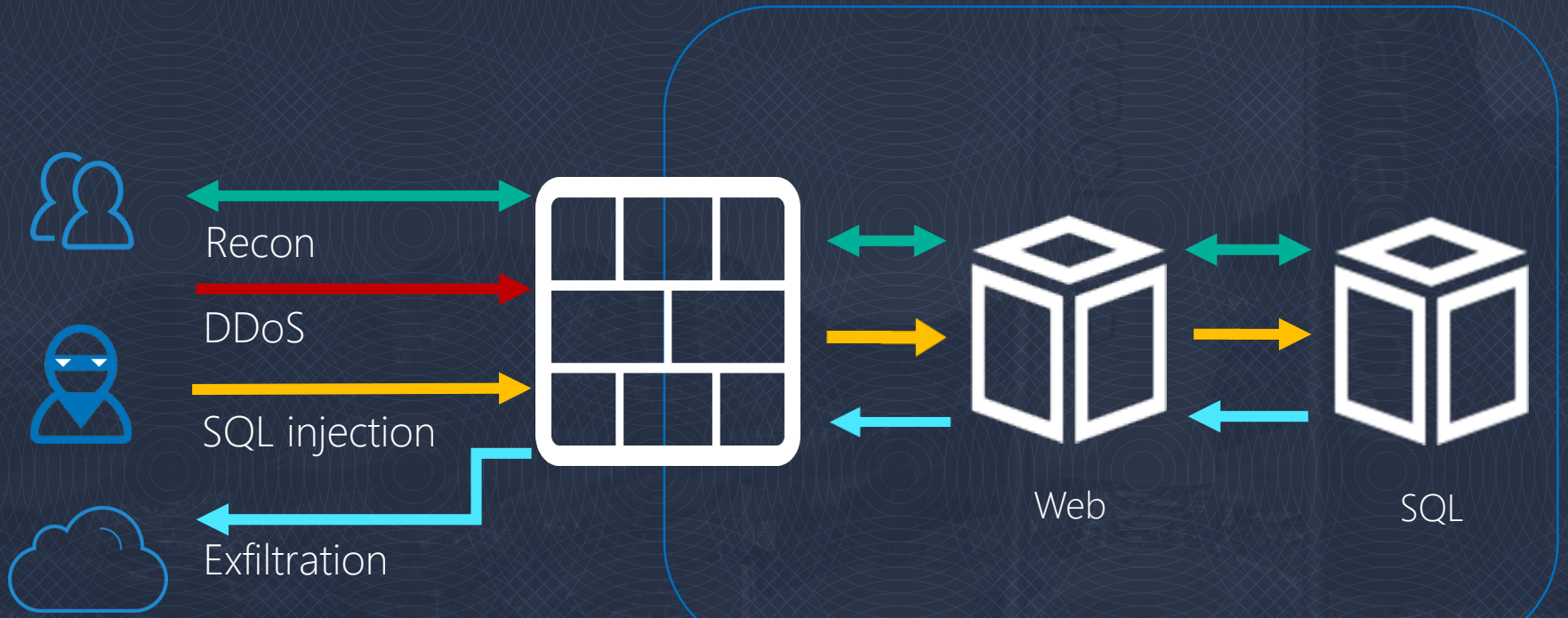
Uber – 57 million accounts (2016)

Equifax – 189 million accounts (2017)

Marriott International – 500 million accounts (2018)

https://haveibeenpwned.com/

TalkTalk 2015



157,000 user accounts compromised

OWASP Top 21 automated attacks

OAT-001 Carding	OAT-002 Token cracking	OAT-003 Ad fraud	OAT-004 Fingerprinting	OAT-005 Scalping	OAT-006 Expediting
OAT-007 Credential cracking	OAT-008 Credential stuffing	OAT-009 CAPTCHA defeat	OAT-010 Card cracking	OAT-011 Scraping	OAT-012 Cashing out
OAT-013 Sniping	OAT-014 Vulnerability scanning	OAT-015 Denial of service	OAT-016 Skewing	OAT-017 Spamming	OAT-018 Foot printing
OAT-019 Account creation	OAT-020 Account aggregation	OAT-021 Denial of inventory			

Industry specific use cases

eCommerce	Media	Travel	Government
Classifieds	Finance	Ad networks	Social networks

eCommerce

Account Takeover

- Hack into accounts using credentials purchased on dark web

Carding

- Hackers testing 1000s of stolen credit cards

Web Scraping

- For content, pricing and inventory information

Scalping

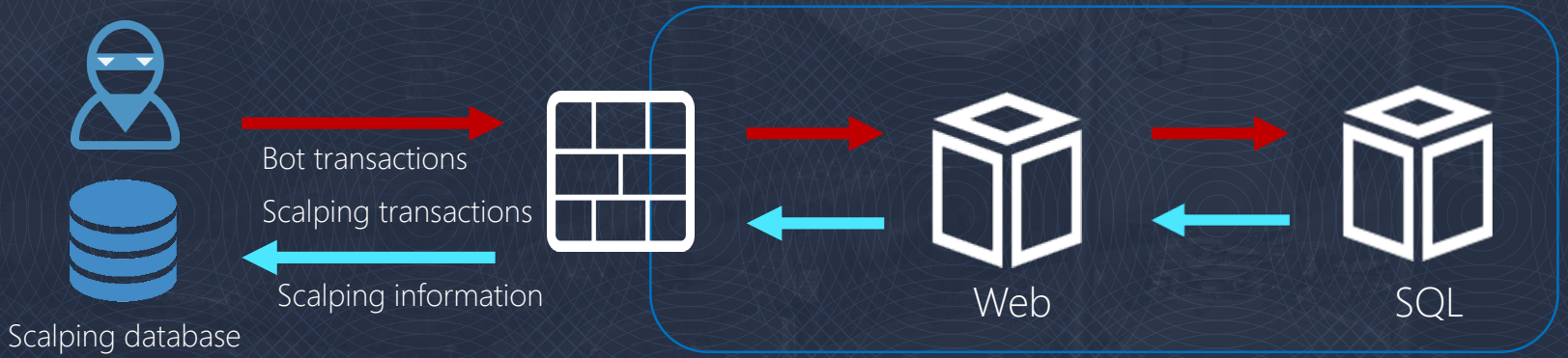
- Automated purchases for black market sales

Cart Abandonment

- Add 100s of items to shopping cart and abandon, cause inventory exhaustion

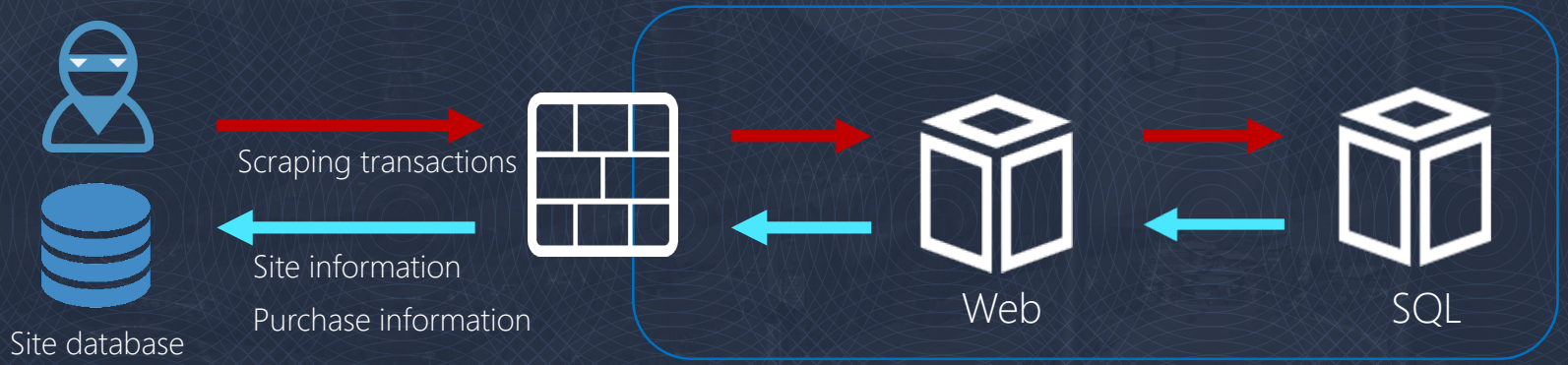
Scalping

Bots take advantage of their speed vs human purchasers to buy a rare resource and then sell at an inflated price



Web scraping

Bots copy data from a website for nefarious purposes such as price fixing, site impersonation, etc.



Finance

Credential stuffing

- Trying 1000s of stolen user credentials

Web scraping

- For content, pricing and inventory information

Application DDoS

- Use layer 7 attacks to DDoS the online service

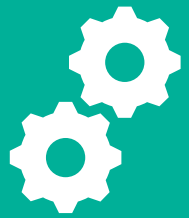
Account aggregation

- Collect user credentials to access

Government

Comment spamming

- Injecting bad links in comments and review forms



API misuse

- Repeated calling of APIs, loading servers

Application DDoS

- Use layer 7 attacks to DDoS the online service

Account takeover

- Hack into accounts using credentials purchased on dark web

Barracuda Advanced Bot Protection Solution

Solution requirements

Solution requirements : Monitor & track

What WAF had …

- Web firewall log
- Access logs

Limitations for this task …

- Number of logs stored
- Limited information about client headers
- Ability to group and corelate logs in sessions

Enhancements …

- Cloud based storage and analysis engine
- Important information like Header order etc. now captured for analysis

Solution requirements : Detect

All detections in the WAF were inline

- Features like Brute Force protection requires simple counters

Bot protection requires inline protection &
out of band analysis

Solution Requirements : Detect (inline)

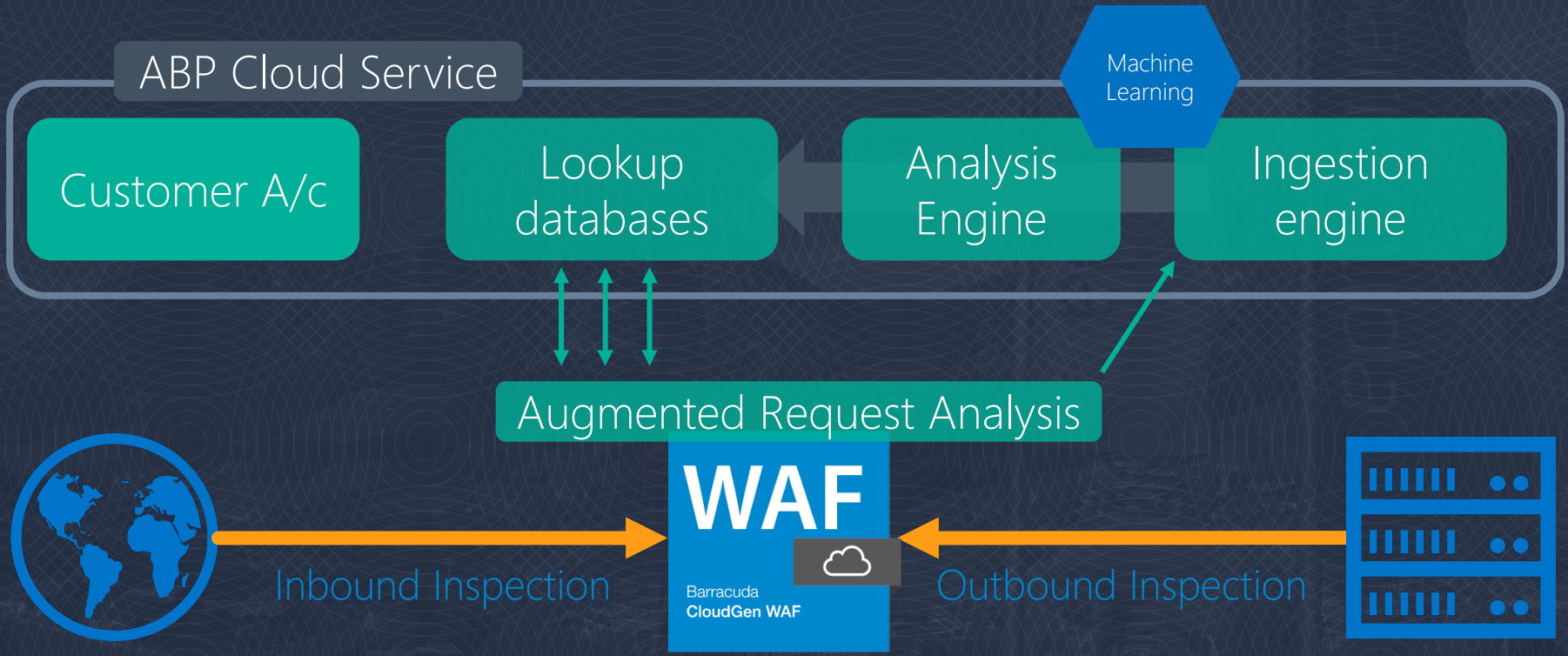
What WAF had …

- Brute force prevention
- Web scraping
- Good bot validations
  - rDNS checks
  - IP ranges
- Slow client protection
- Heavy URL protection
- User agent-based tests
- Honey traps using robots.txt

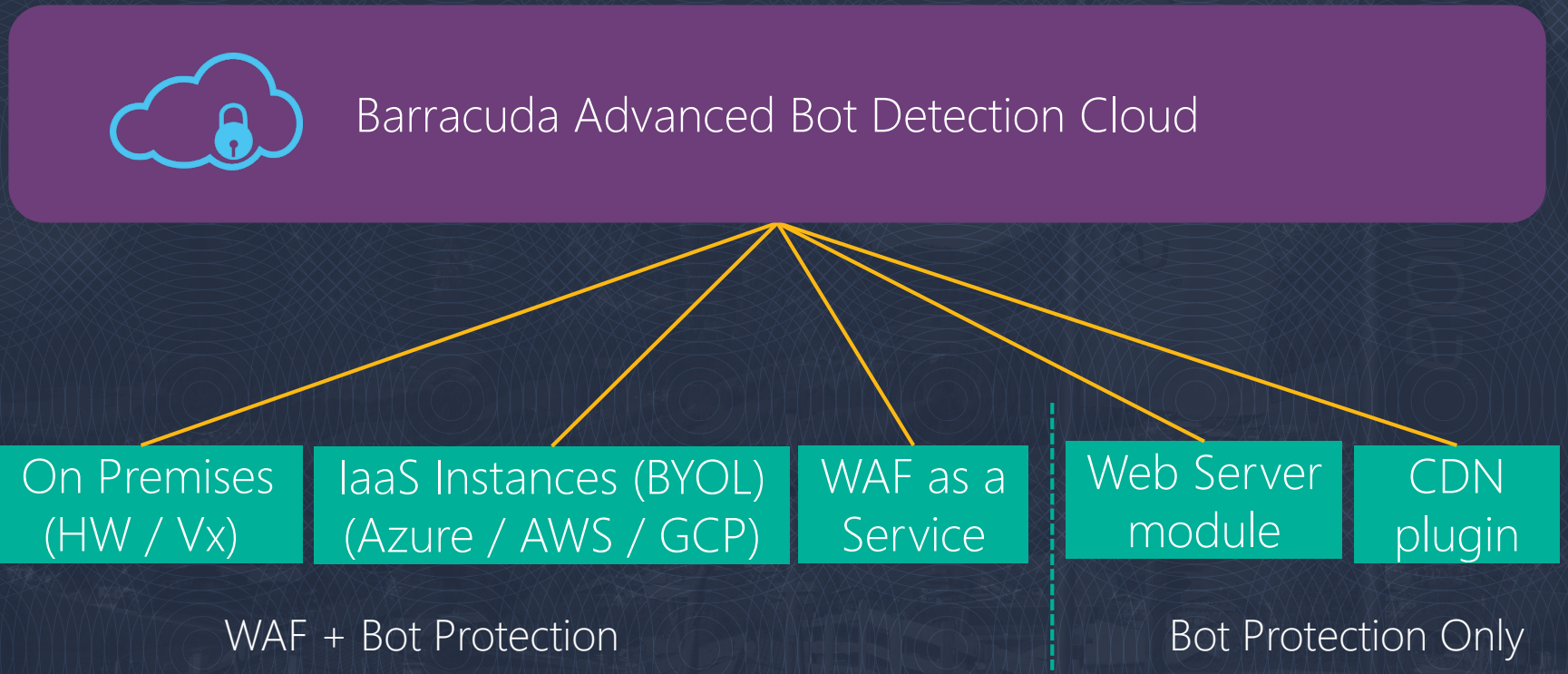
Enhancements …

- Client Fingerprinting
  - Browser / Headless Browsers / Command-line utilities
  - SSL Fingerprints
- Comment & referrer spam
- Bot signature database

Multi-layer approach for advanced protection



Deployment modes



Solution Requirements : Detect (out of band)

What WAF had …

- Nothing

Enhancements …

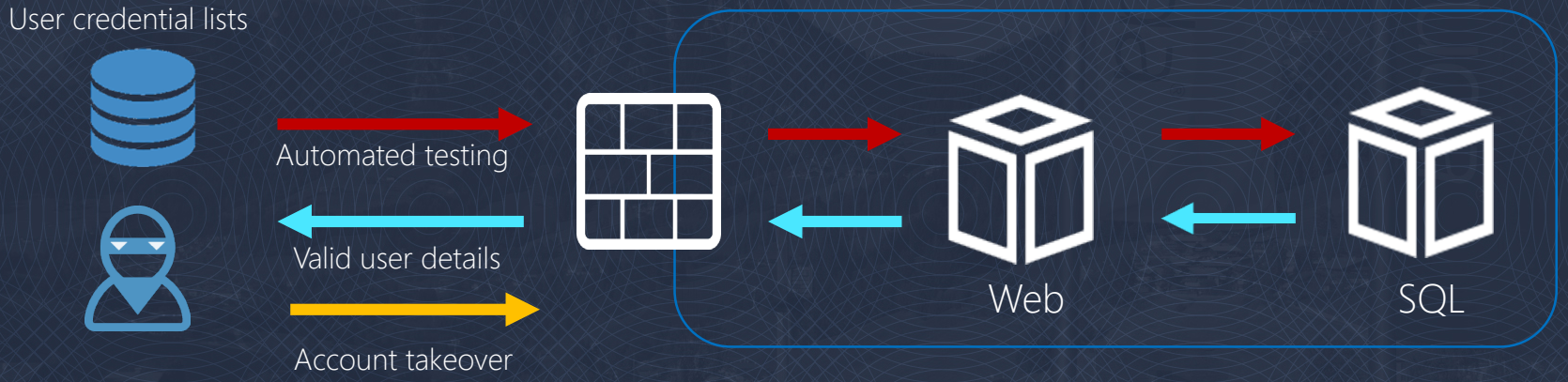
- Credential stuffing service
- Data ingestion engine
- Data augmentation
- Analytics for client risk scoring

Road Ahead …

- Integration with InfiSecure bot engine
- Refining machine learning models for detecting advanced bots

Credential stuffing

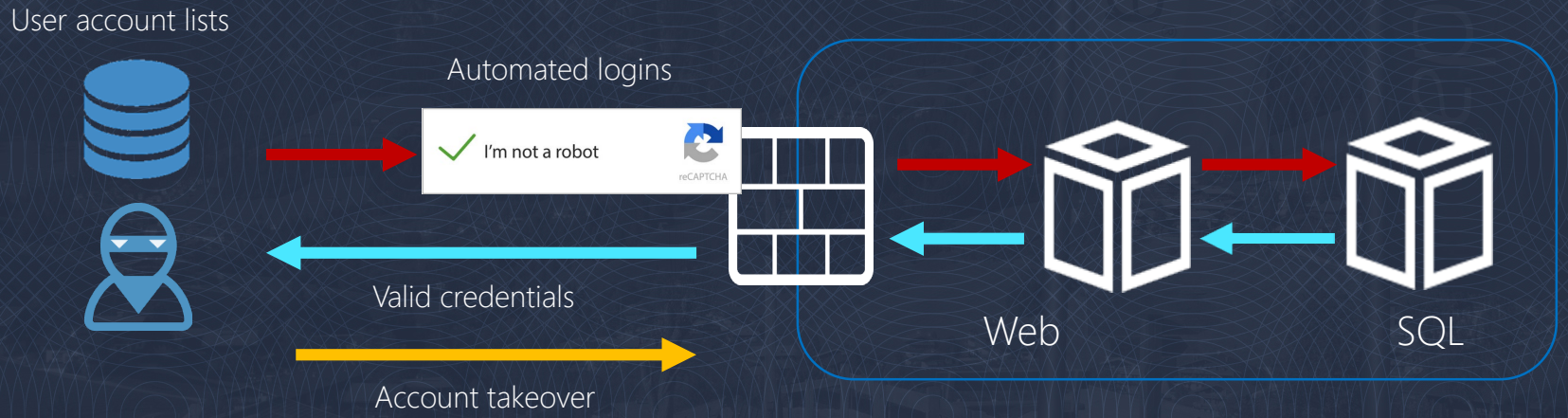
Lists of authentication credentials stolen from elsewhere are tested against the application's authentication mechanisms to identify whether users have re-used the same login credentials



Credential cracking (With CAPTCHA defeat)

Identify valid login credentials by trying different values for usernames and/or passwords.

Additional automation required to defeat CAPTCHA



Solution requirements : Respond & remember

What WAF had …

- Terminate connections
- Block client IP
- CAPTCHA

Limitations …

- Blocking IP means blocking all NAT'ed clients
- CAPTCHA can be solved using scripts

Enhancements …

- Blocking devices based on device fingerprints
- Lock out device fingerprints
- Integrate with reCAPTCHA v2
- Maintain client history

Solution requirements

Reporting

What WAF had …

- In box security & traffic reports

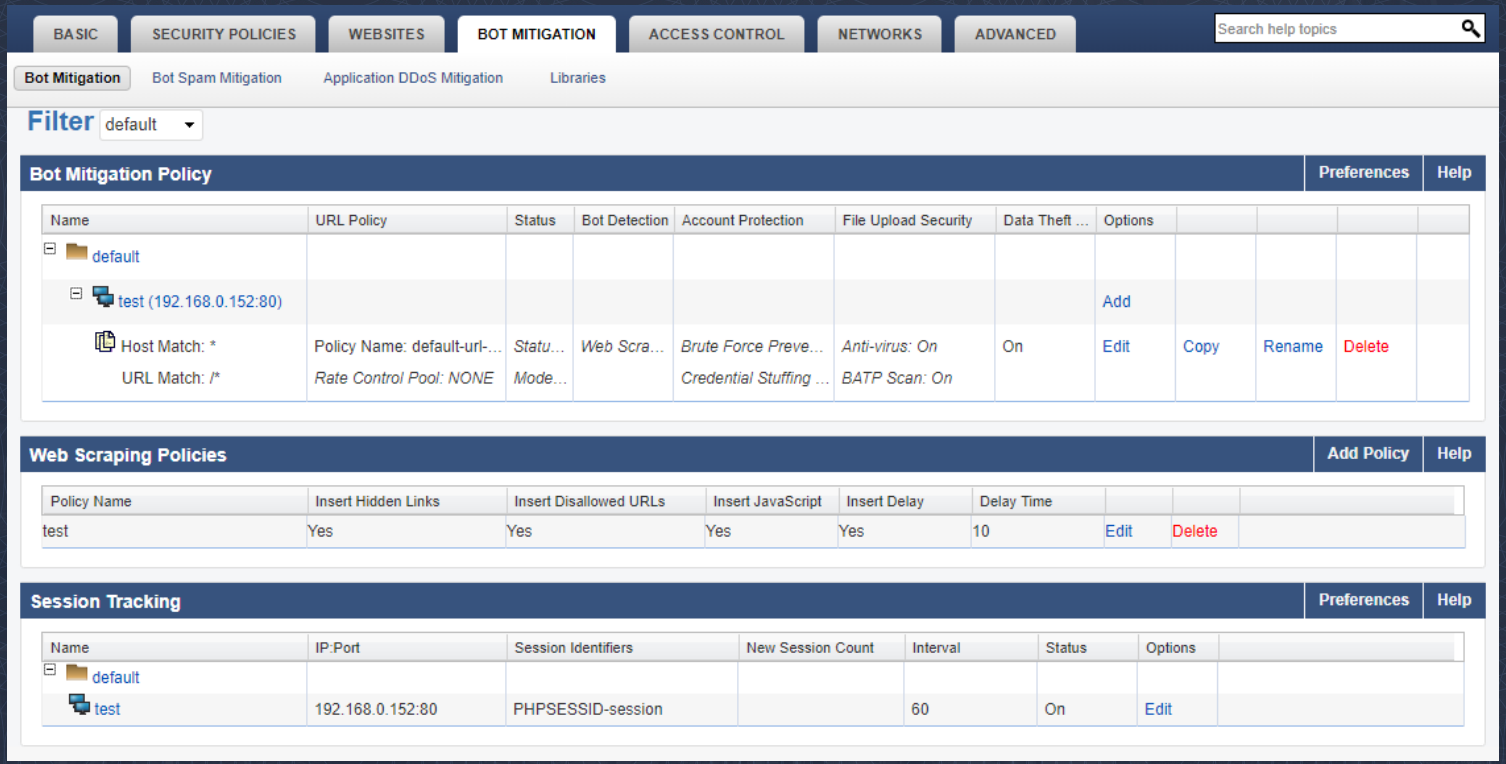
Enhancements …

- Built in reports on WAF
- Bot traffic module on the WAF dashboard

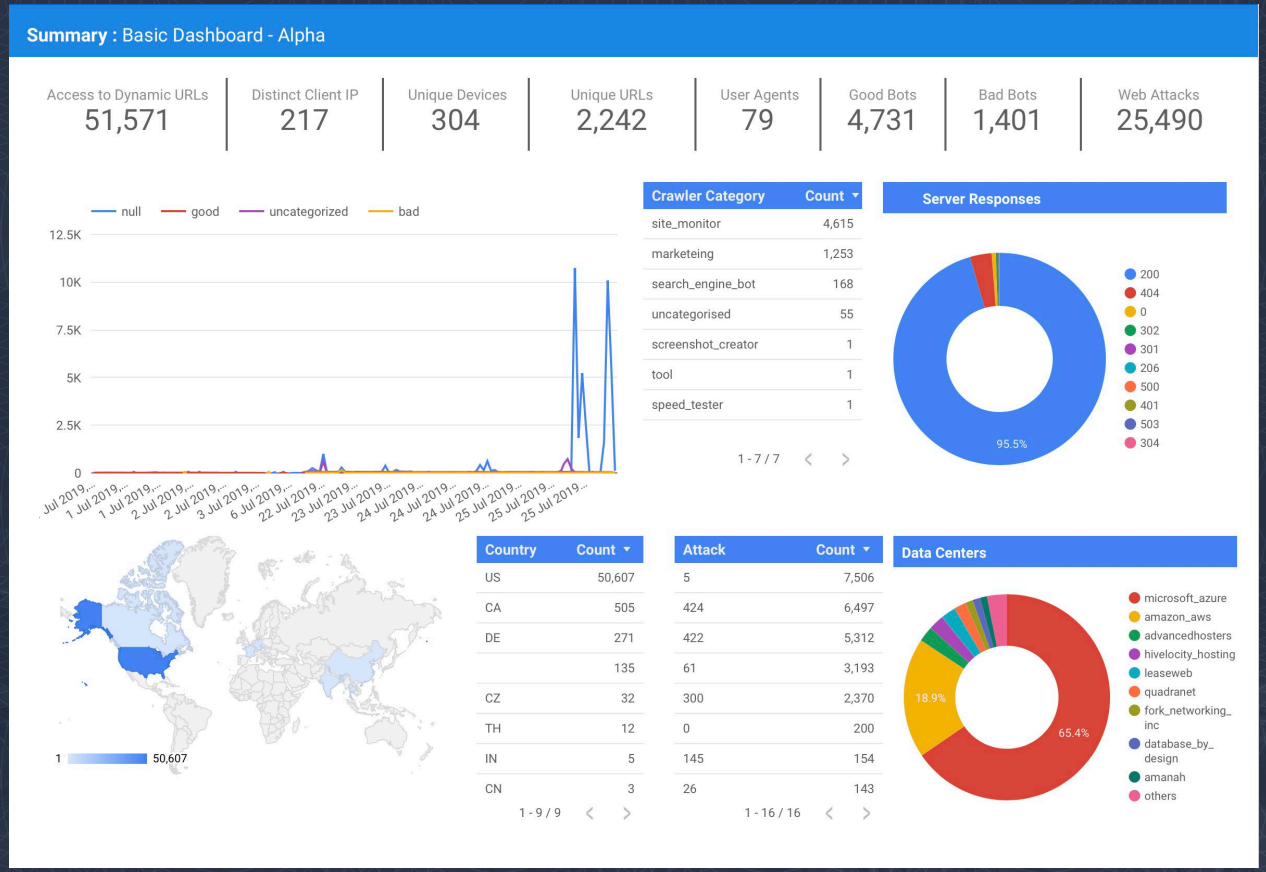
Road Ahead …

- Enhanced cloud bot activity tracking dashboard
- Advanced analytics for application traffic

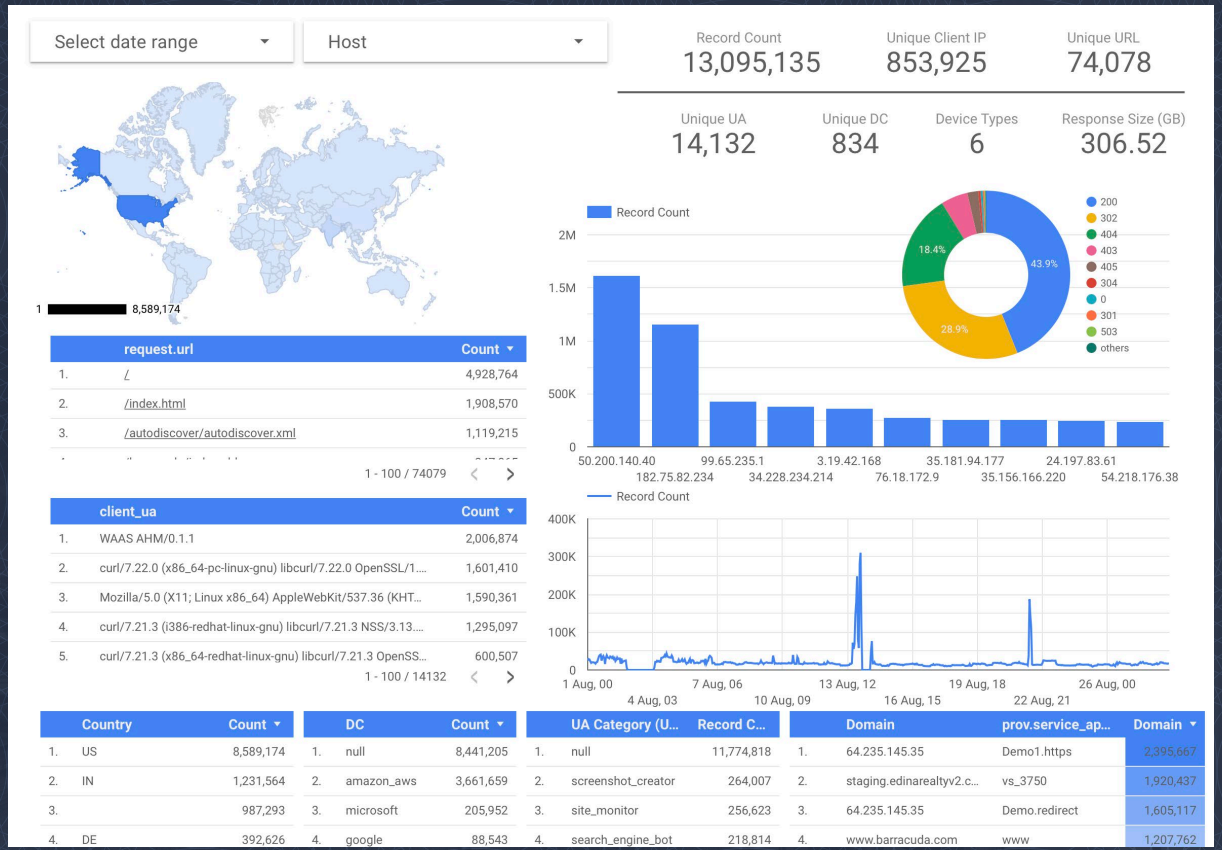
UI : Bot mitigation tab



Cloud-based analysis



Cloud-based analysis



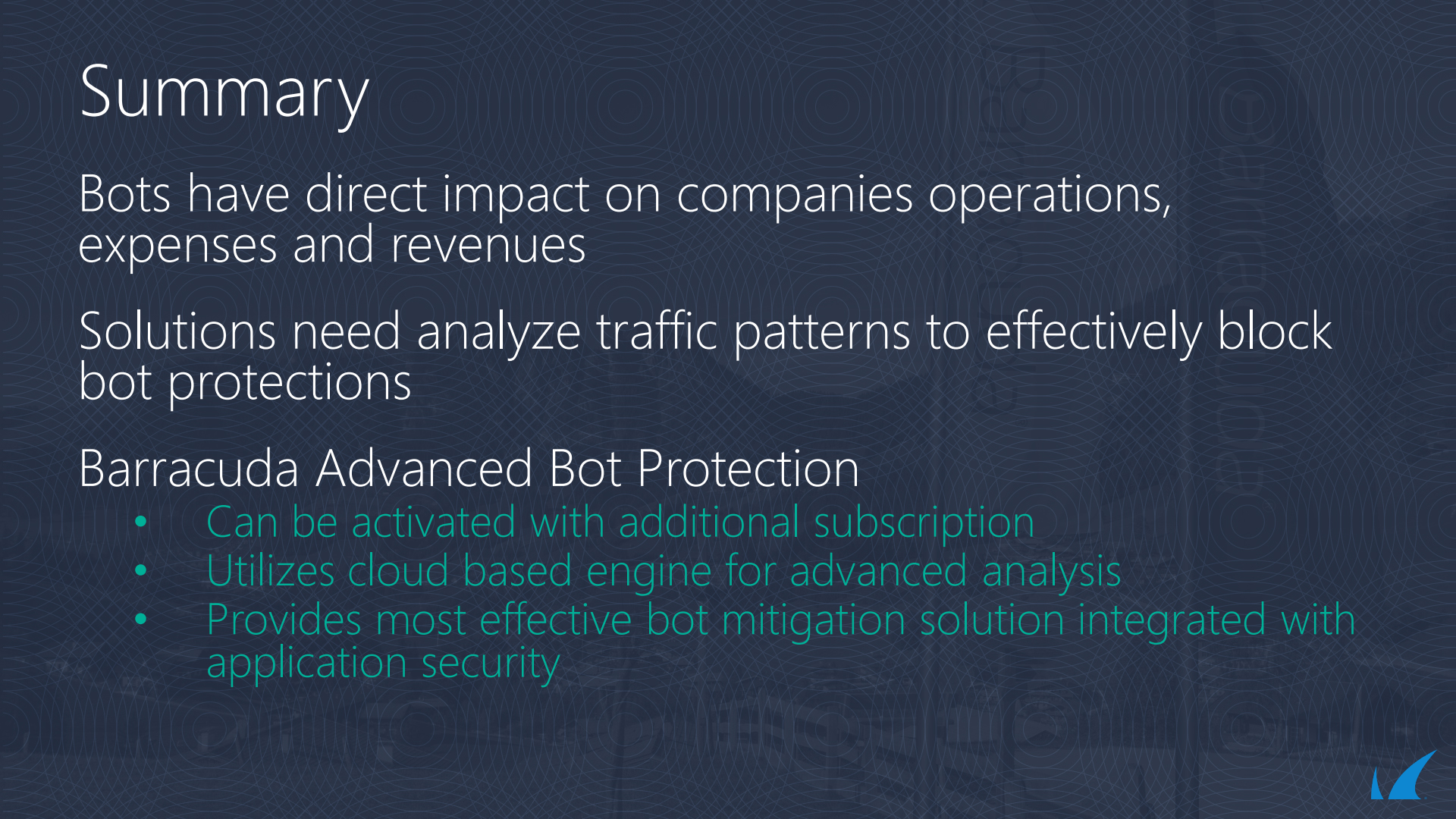
Summary

Bots have direct impact on companies operations, expenses and revenues

Solutions need analyze traffic patterns to effectively block bot protections

Barracuda Advanced Bot Protection

- Can be activated with additional subscription
- Utilizes cloud based engine for advanced analysis
- Provides most effective bot mitigation solution integrated with application security




Thank you
Barracuda
TECHSUMMIT19
BARRACUDA TECHNICAL SUMMIT