22

Hours of downtime

17

Weekends worked by on-call teams

3

Security personnel

1100

Known compromised to accounts

F5 Distributed Cloud Bot Defense & Account Protection

Jon Hine Major Account Manager

Keith Pasley Solutions Engineer

October 2022

Agenda

- Today's threat landscape and how it is affecting state agencies
- The unique challenges Agencies are having fighting off bots and manual fraud
- The benefits of F5 Distributed Cloud Bot Defense & Account Protection

Fraud occurs when criminals act like legitimate users

Users
(criminals mixed in with good users)

"Hackers don't break in, they log in" – Fortune 50 CISO

Typical large enterprises lose >$25M / year to criminals who act like users

Bots cause harm across your organization

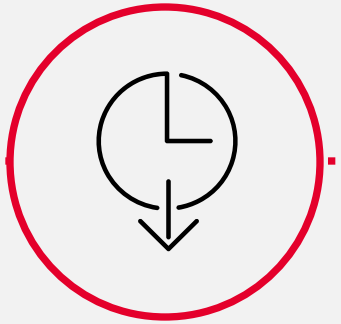
ATO and Fraud

$500k lost annually per organization due to credential stuffing

Manual bot blocking

10k hours manually blocking and clean up bots per year

Downtime



80% of traffic potentially unwanted automation

Poor customer experience

4 out of 5 global brands suffer churn due to bots

The Threat Landscape – Economic

Scaled Manual Attacks

- Human "Click Farms"
- Suspicious human behaviors
- High value/high cost

Professional Automation

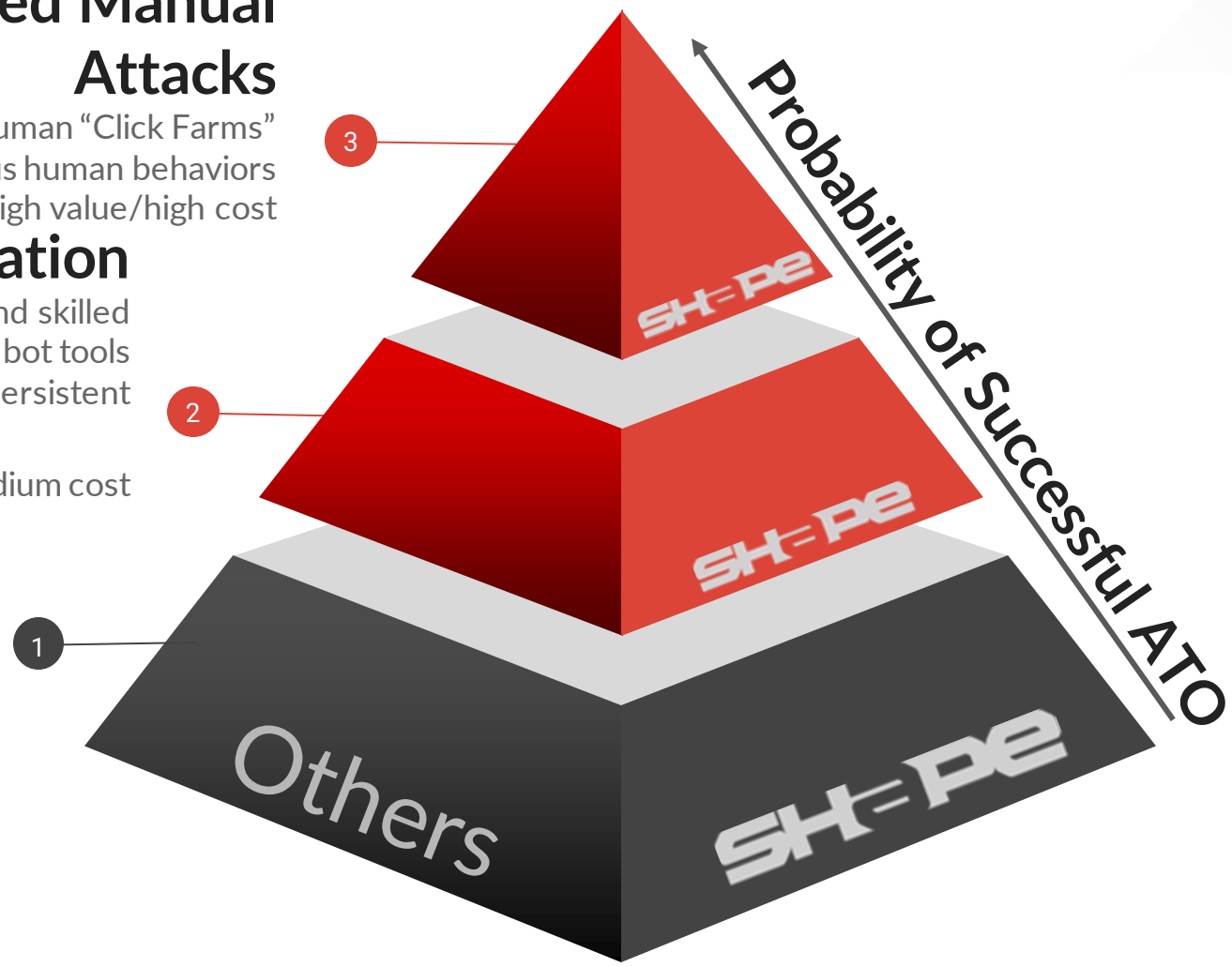
- Highly motivated and skilled
- Customized bot tools
Persistent

- medium value/medium cost

Amateur Automation

- Less motivated and skilled
- Off-the-shelf tools

- Low value/low cost



1 2 3 **Shape**

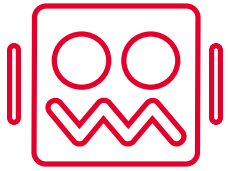
1 ○ ○ **Other Solutions**

Modern attacks begin with breaches and end with fraud

BREACHES, FRAUD, AND ABUSE HAVING GREATER BUSINESS IMPACT

#1

Credential attacks leading cause of extreme financial loss over past 5 years ($10BN)



78%

of orgs reported increase in customer complaints or churn due to **bot attacks** since start of pandemic

1 in 3

global consumers have experienced **fraud** in past 3 months

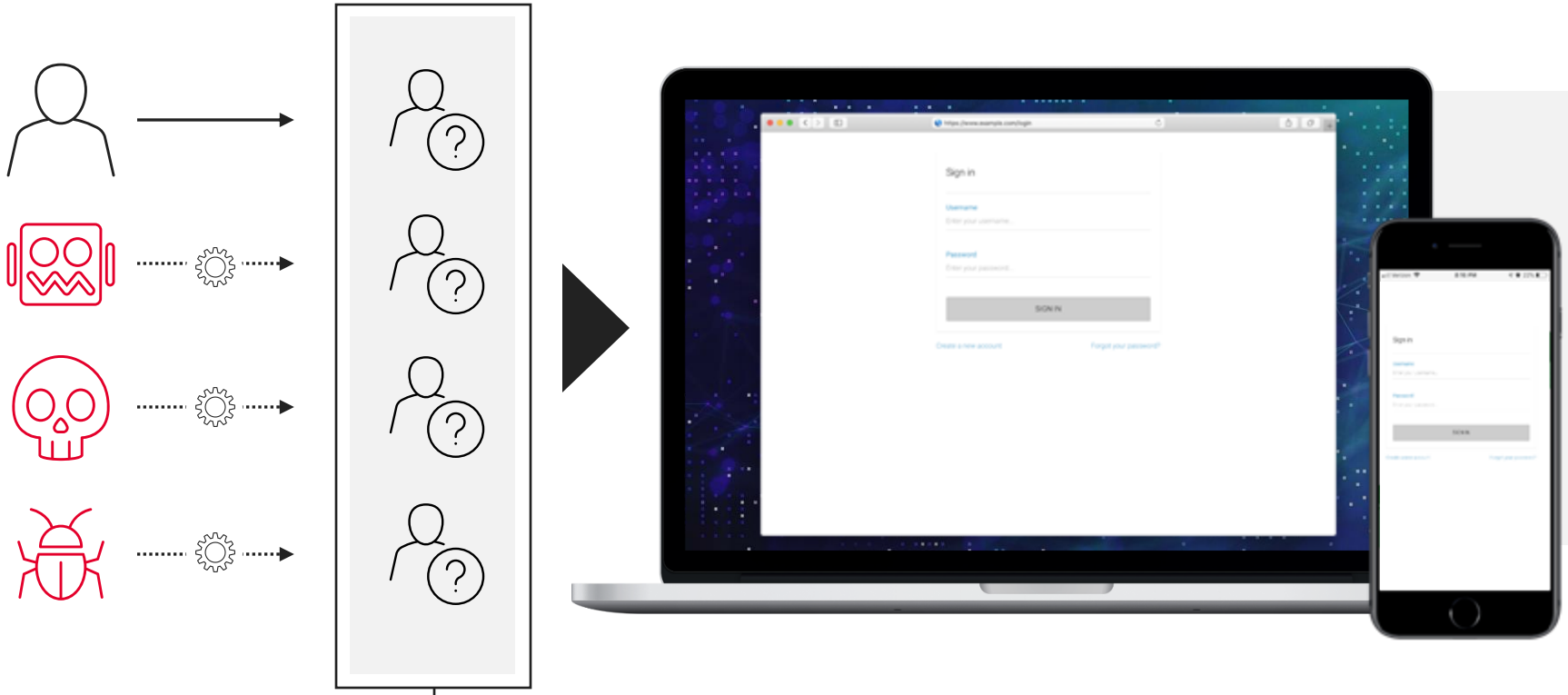
Churn

Fines

Revenue Loss

Theft

Bots are a fundamentally different type of threat



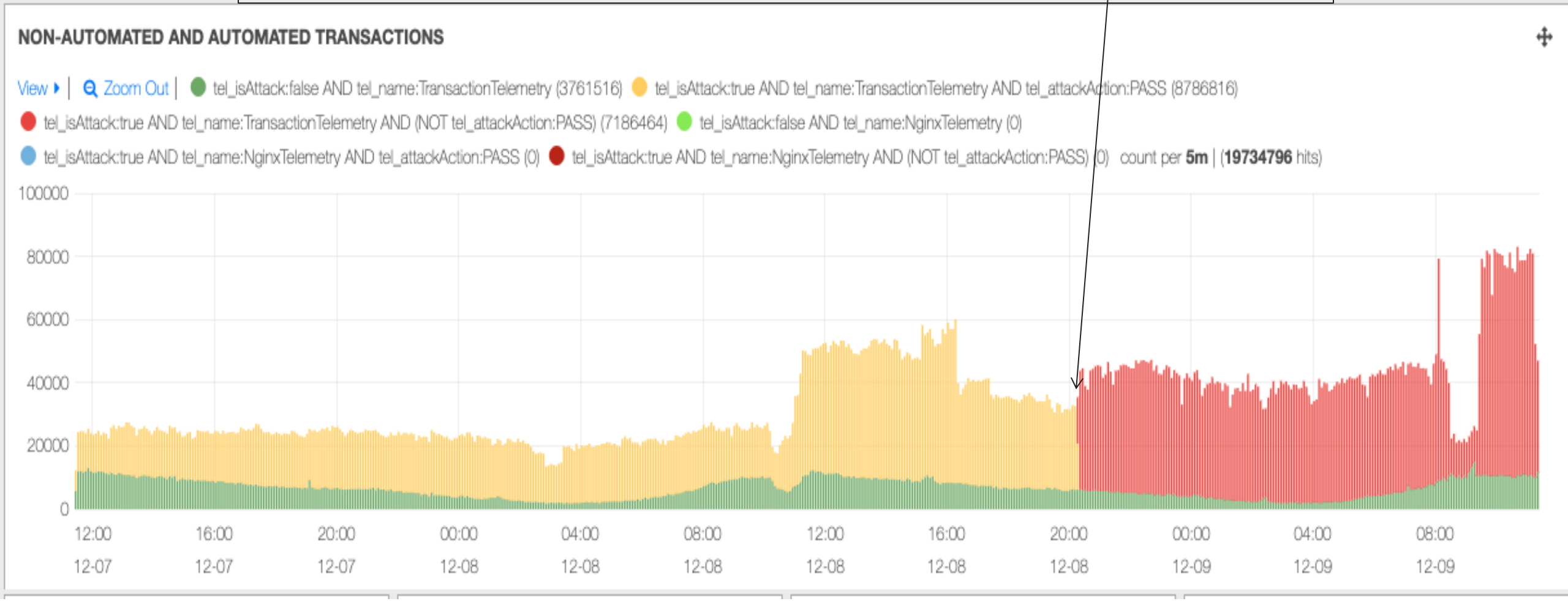
Bots look like customers and abuse inherent app functionality

> **Using our WAF and traditional firewalls** to manually block IP addresses was a **horribly ineffective** way to mitigate the very real threat posed by bots.
>
> —CISO, Major US Retailer

XC Bot Defense: Examples and Use Cases

Attack on State Agency:

XC Bot Defense was implemented on 12/08/2020 at 08:20PT

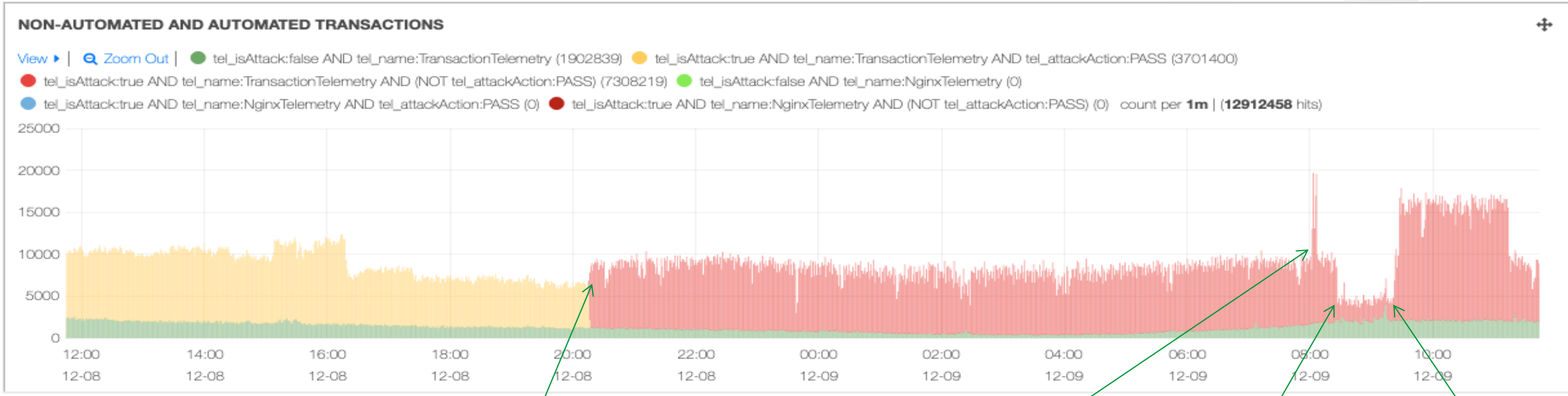


Yellow indicates automated traffic not blocked

Red indicates traffic blocked

Green indicates legitimate human connections

Attack on State Agency:

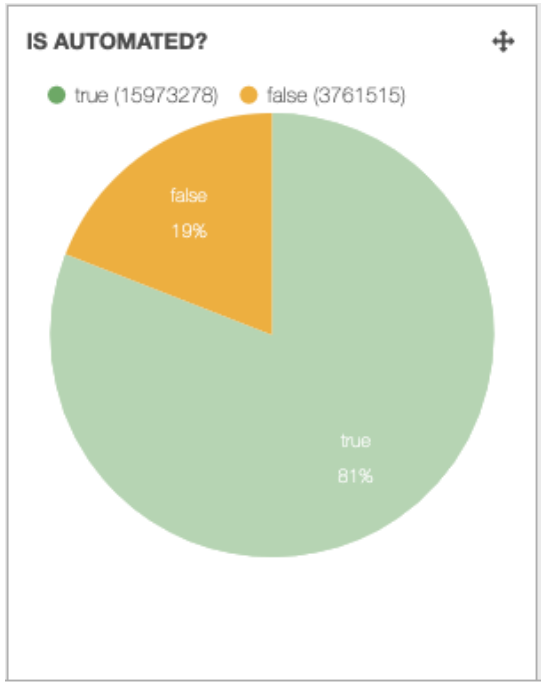


Immediately after XC Bot Defense was implemented the attacker increased the volume of the attack

The attacker attempted to incorporate a brief ddos attack

Attacker retools, then attempts new attack parameters

Attack on State Agency:



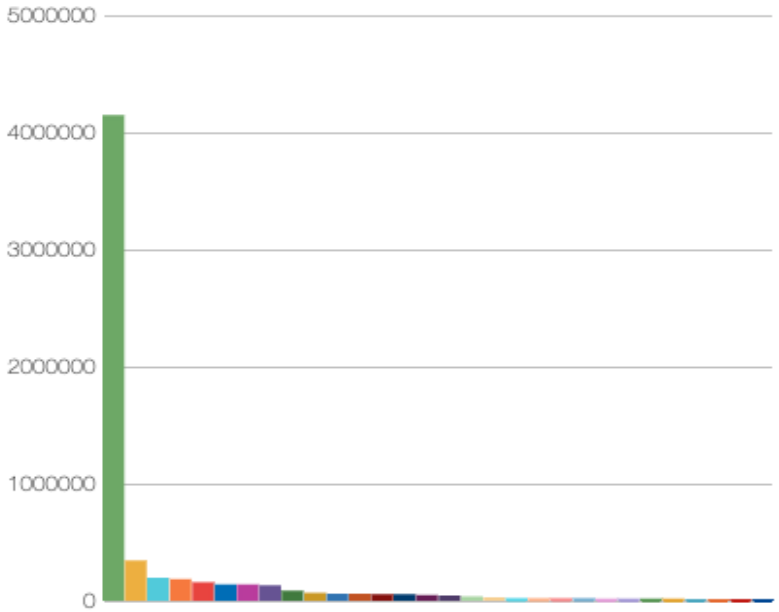
81% of connections are automated, with a peak of 95%

The top target Authentication login

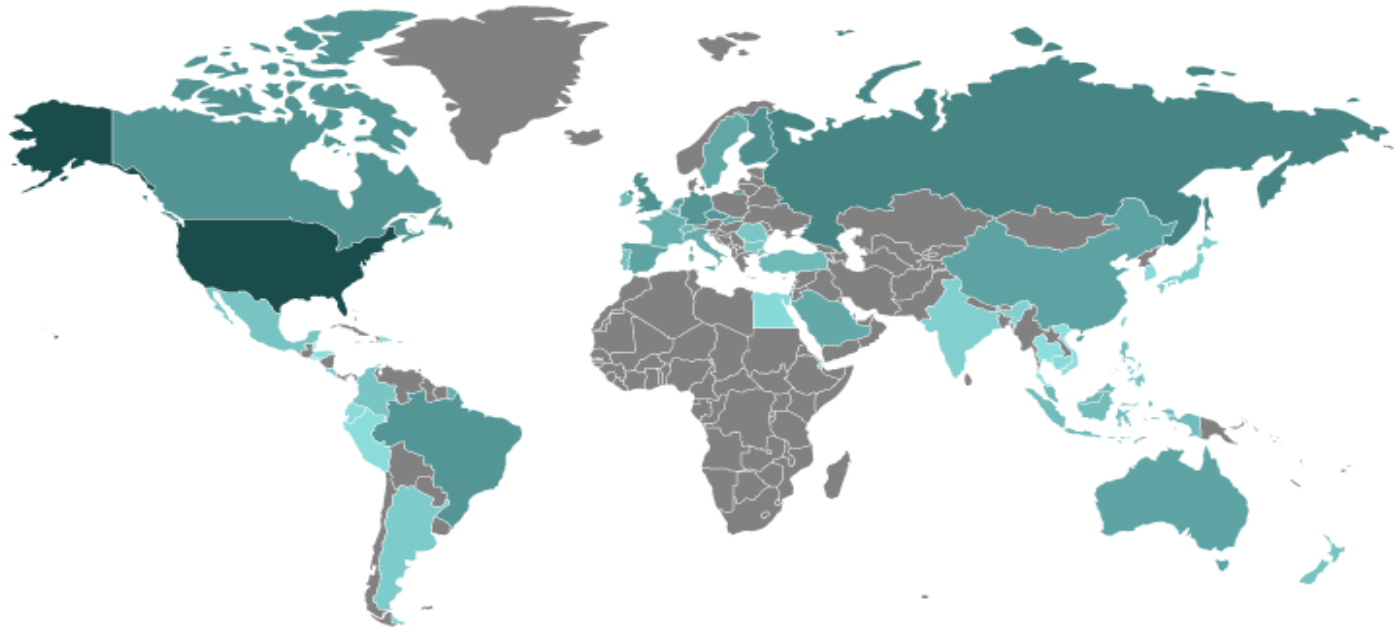
Past 24 hours

TOP COUNTRIES

United States (4131513) Russia (329536) Finland (180837)
United Kingdom (169359) Canada (144669) Brazil (125890)
Germany (125441) Czechia (117185) Netherlands (70162)
Israel (51922) Spain (46886) China (45149) Slovakia (42895)
Australia (41855) Sweden (35397) Saudi Arabia (30408)
Italy (22649) France (16949) Switzerland (9349)
Belgium (7636) Malaysia (6704) Turkey (6070) Ireland (5074)
Indonesia (3955) Portugal (3133) Philippines (2410)
New Zealand (1700) Mexico (1421) Colombia (1286)
Bulgaria (1090)



IP ADDRESS MAP



Attack traffic is coming from all over the globe

Macro Trend: Convergence across functional areas

Are you human?

Are you good or bad?

Are you who you say you are?

The XC Bot Defense Platform

Bot Defense

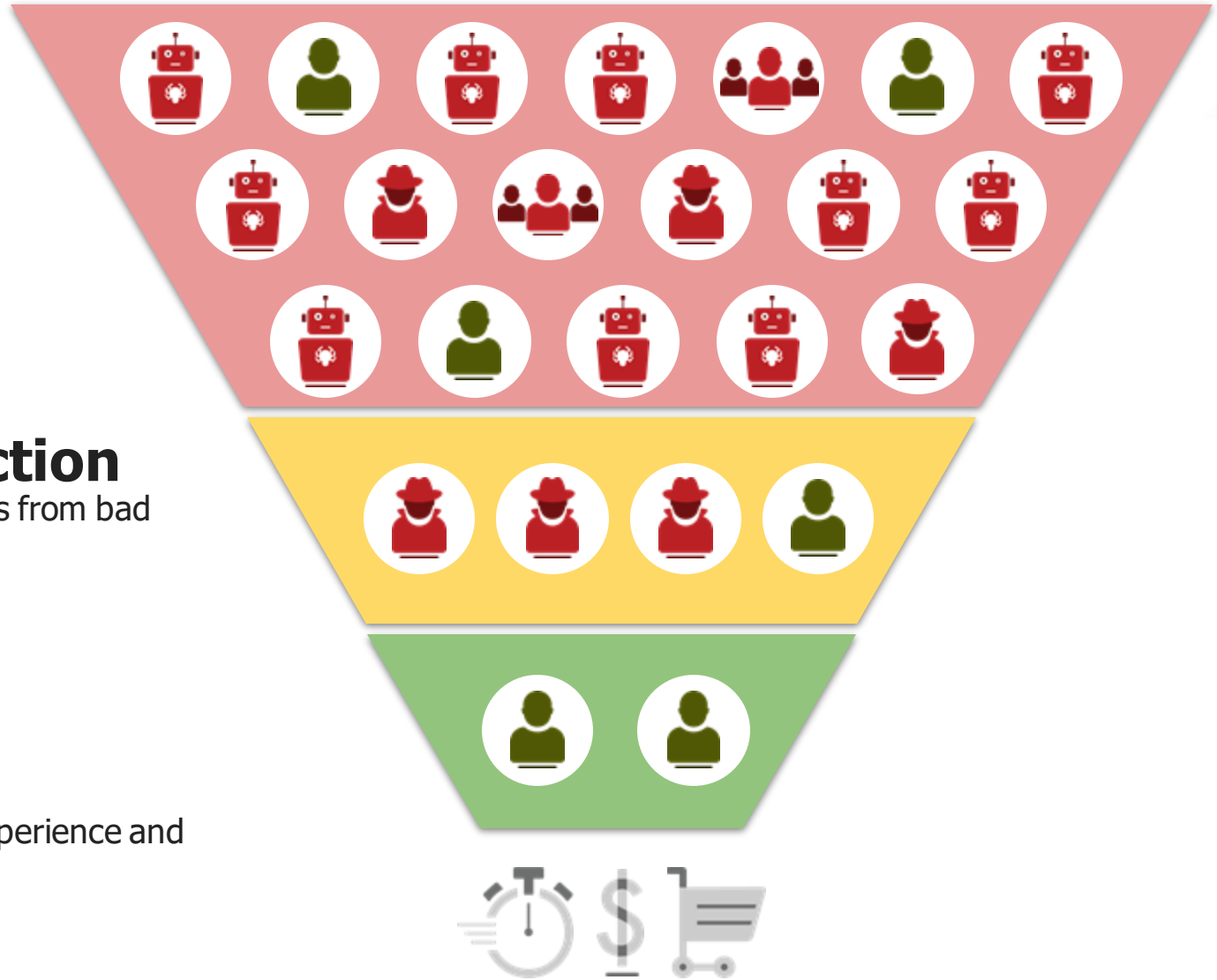
Identify and mitigate unwanted traffic

Account Protection

Differentiate good customers from bad customers

Authentication Intelligence

Create a friction free user experience and increase revenue



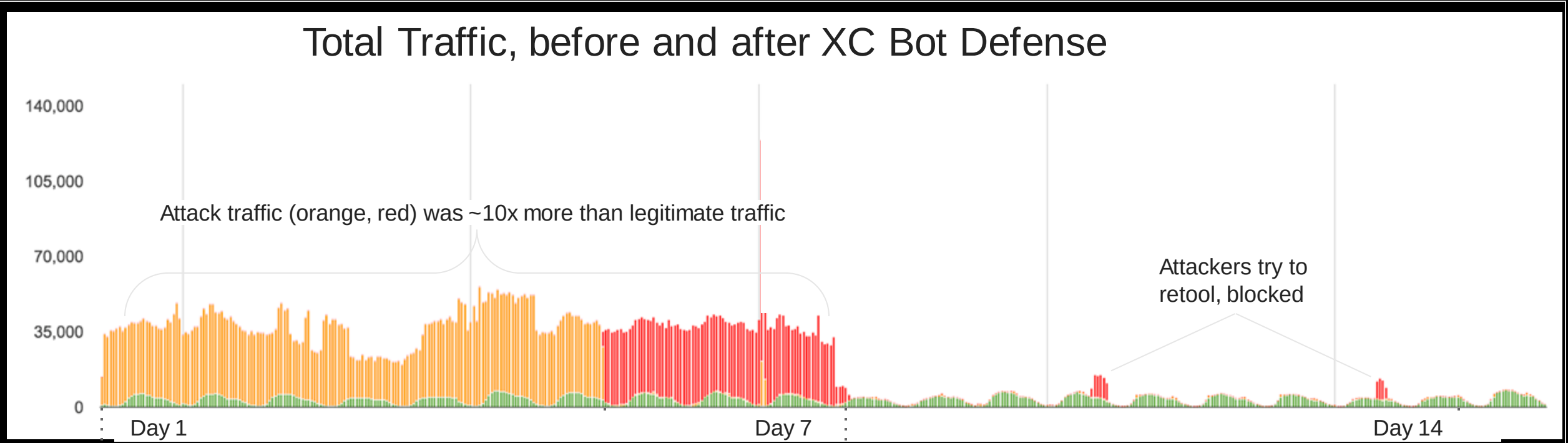
Bots

Human Clickfarm

Fraudsters and Criminals

Good Customers

Current customer: Sustained 99% effectiveness (3+ years)



XC Bot Defense inline, monitoring mode only, observes 92% of traffic as malicious

XC Bot Defense begins blocking attacks

Major attacks stop

Attackers give up

Bots have significant impact on the Organizations.

Account takeover

Carding

Gift Card Fraud

Inventory Hoarding

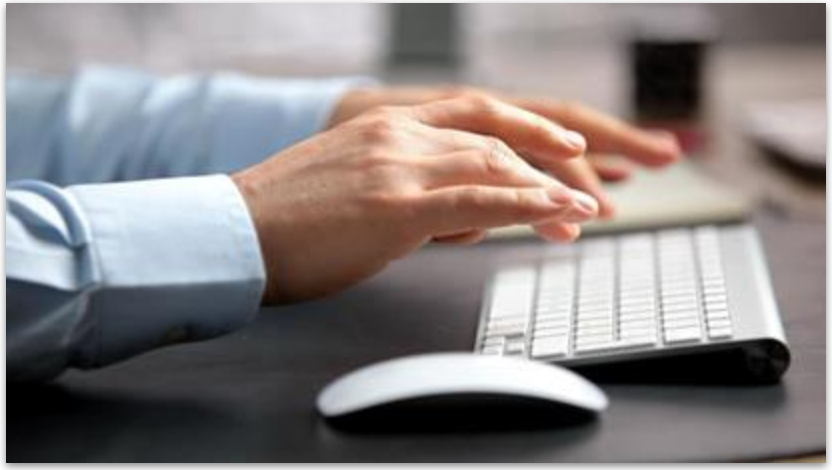
Scraping

The XC Bot Defense Signals

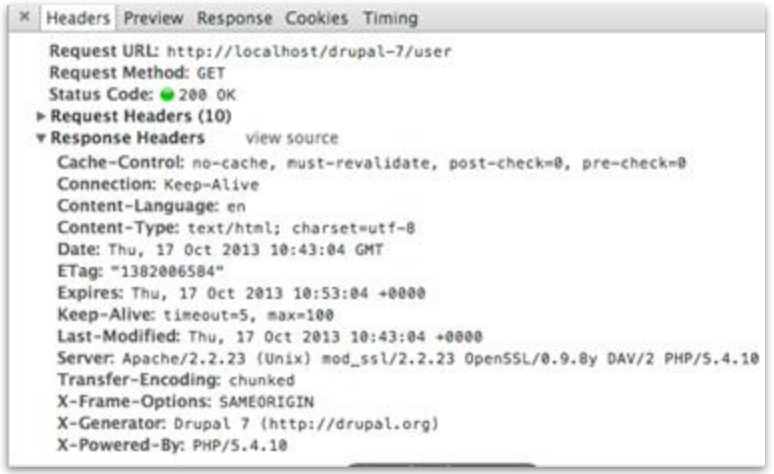
Bot Detection

XC Bot Defense analyzes three categories of signals to identify illegitimate traffic

Environment



Behavior

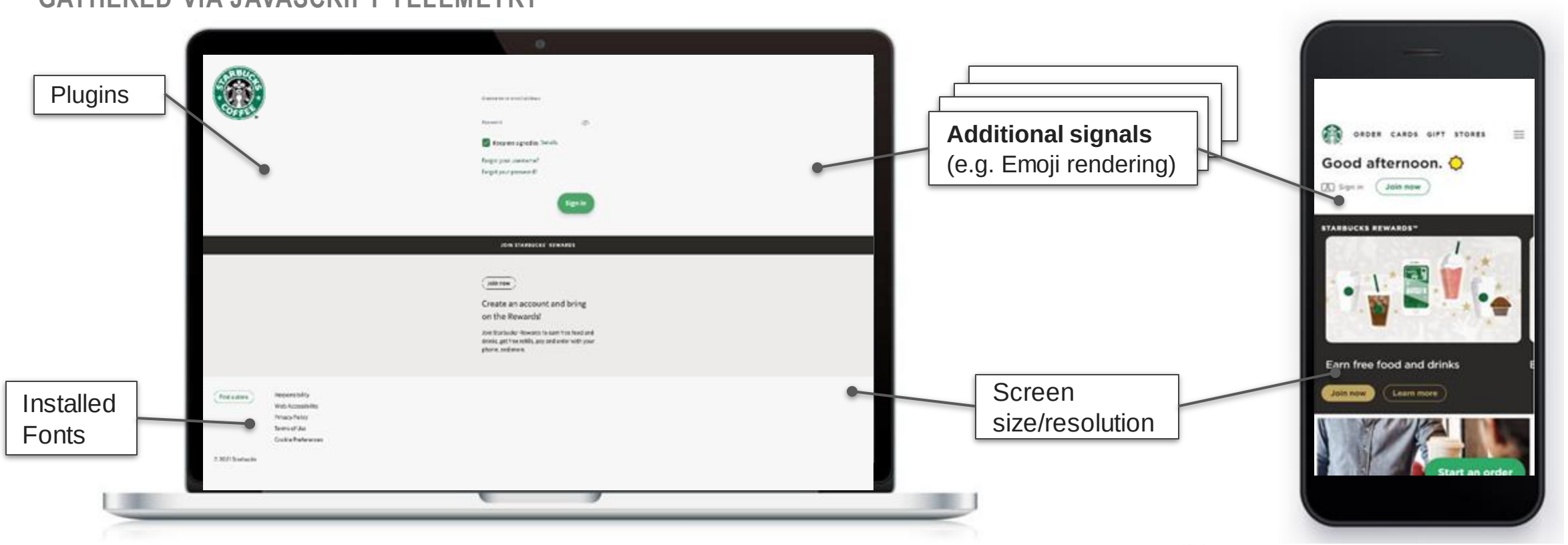


Network

28

Browser Environment Signals (Web & Mobile Web)

GATHERED VIA JAVASCRIPT TELEMETRY

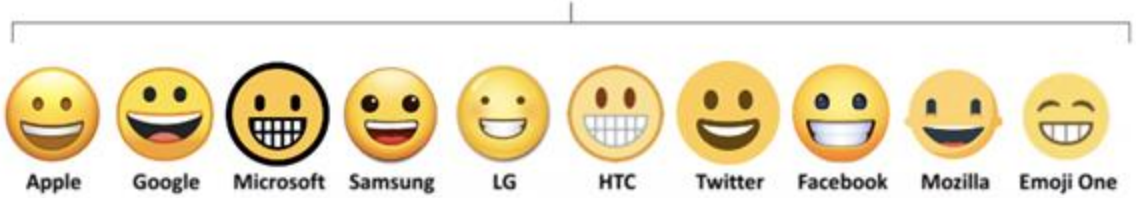


0xFFFFFFFFFFFFBFF

=

18,446,744,073,709,552,000
18,446,744,073,709,550,000
18,446,744,073,709,550,591

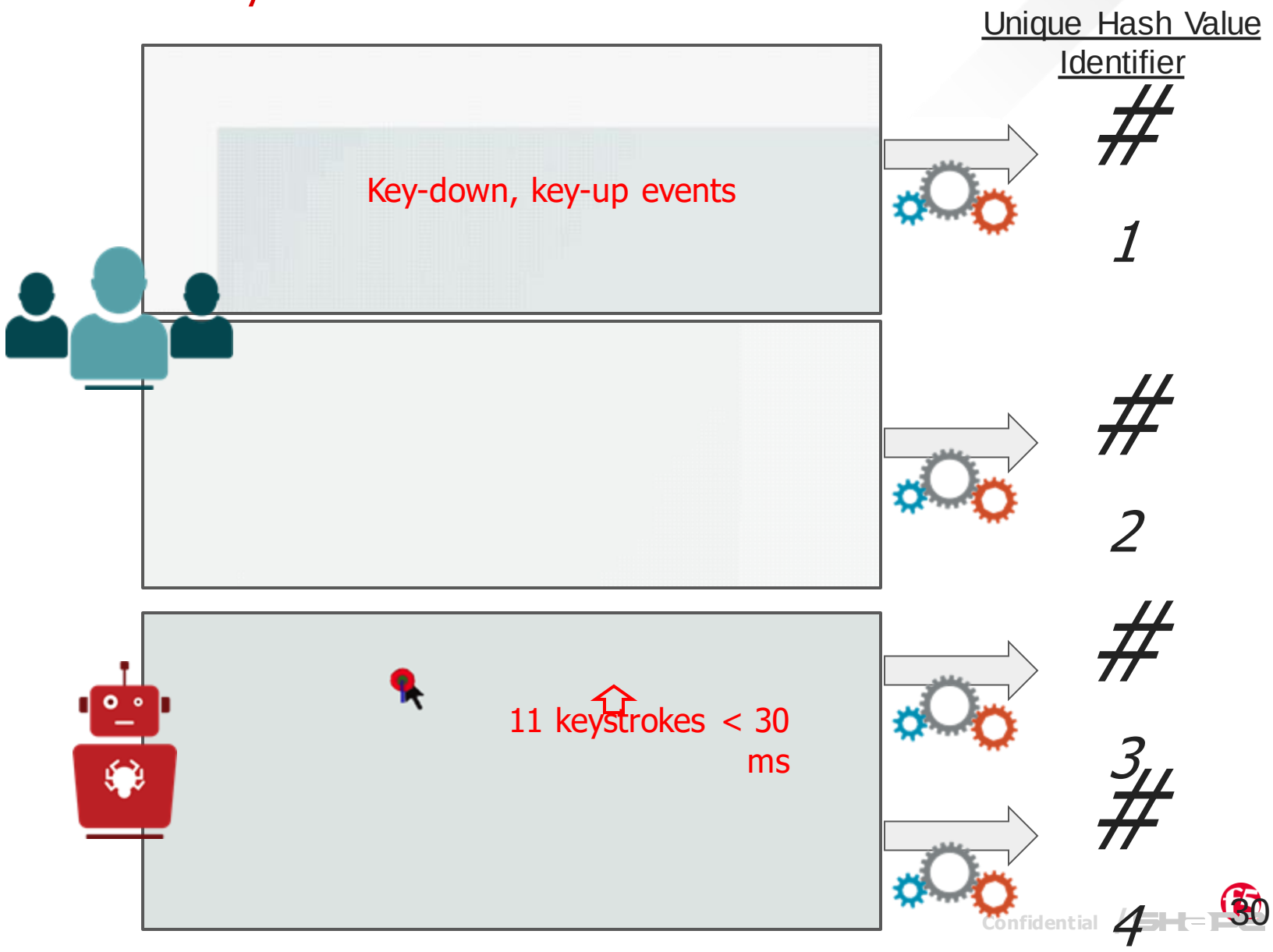
:D



Behavior Signals

Gathered via JavaScript & SDK Telemetry

Blue Bar	Key-down.
Orange Bar	Key-up.
Red Circle	Mouse-click.
Green Tick	Captured mouse event.
Dashed Line	High speed movement between two points.
Brown Square	Long pause.
Grey Line	Transition from non-mouse event to mouse event.



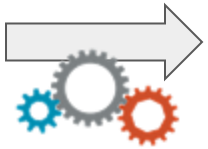
Network Signals

Network Signals + XC Bot Defense's Global Intelligence Enable API Channel Protection

Header field name	Description
Accept	Content-Types that are acceptable for the response. See Content negotiation.
Accept-Charset	Character sets that are acceptable.
Accept-Encoding	List of acceptable encodings. See HTTP compression.
Accept-Language	List of acceptable human languages for response. See Content negotiation.
Accept-Datetime	Acceptable version in time.
Authorization	Authentication credentials for HTTP authentication.
Cache-Control	Used to specify directives that *must* be obeyed by all caching mechanisms along the request-response chain.
Connection	Control options for the current connection and list of hop-by-hop request fields.[8]
Cookie	An HTTP cookie previously sent by the server with `Set-Cookie` (below).
Content-Length	The length of the request body in octets (8-bit bytes).
Content-MD5	A Base64-encoded binary MD5 sum of the content of the request body.
Content-Type	The MIME type of the body of the request (used with POST and PUT requests).
	The date and time that the message was originated (in "HTTP-date"

Known Bad True Client IP & ASN Example

AS #	IP	CC	Registry	Allocated	AS Name
48817	185.156.73.21	RU	ripencc	2016-06-15	RELDAS-NET, RU



Indicators in the HTTP Header, such as header field order, can reveal crafted requests and signs of automation

Threat actors & attack campaigns can be profiled by source:

- Foreign & Bulletproof Hosting Services
- AWS / GCP / Azure Hosting
- Residential ISPs
- Shape-tracked Known Bad ASNs

Mobile Environment Signals (Native Mobile Apps)

GATHERED VIA SHAPE MOBILE SDK TELEMETRY

- Operating System
- **Device Information**
- App Versioning
- **Battery Information**
- Processor
- Localization Information
- **Physical Sensor Data**
- Epoch Timestamp
- WebView Data
- Emulator Detection
- Rooted Device Detection

Screen resolution
Screen brightness
Hardware

Temperature
Capacity
Technology

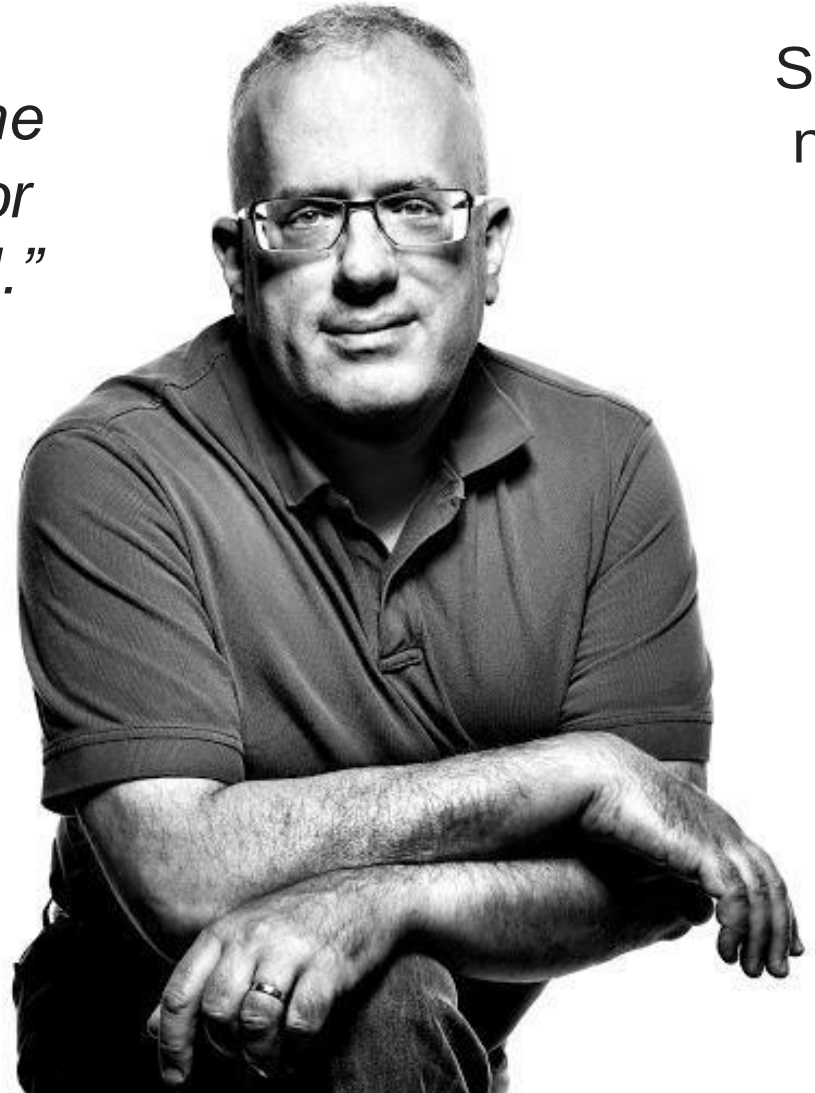
Altitude
Orientation
Gyroscope

Shape's Mobile SDK is currently deployed on over **1 billion** mobile devices worldwide

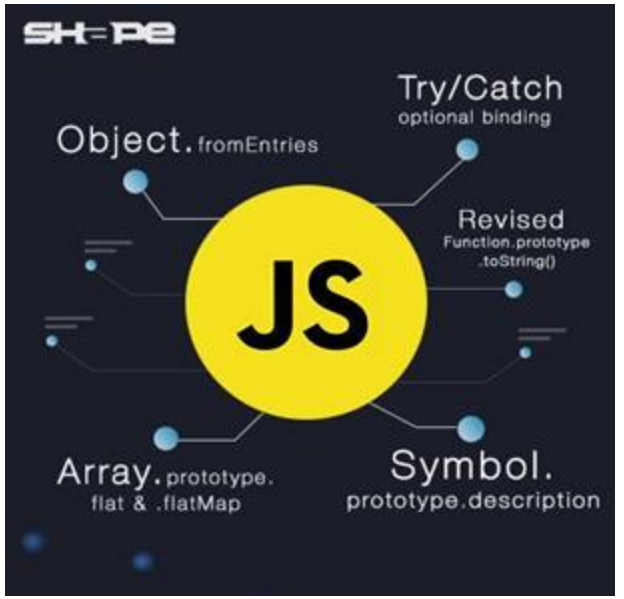
“Shape (XC Bot Defense) understands web browsers and mobile devices in a way nobody else in the industry does”

“Today, Shape is by far the most influential contributor to JavaScript in the world.”

***Brendan Eich**,*
Creator of JavaScript
Founder of Mozilla/Firefox



Shape invented 5 of the 9 total new official features added to JavaScript in the last year



Spoof-proof JavaScript

JS EXPERTISE AND SECURITY PATENTS CREATE THE HIGHEST QUALITY TELEMETRY AND EFFICACY

Competitor JavaScript

```
function(h) {
    function e(e) {
        if (!e) throw new Error("messageBus param must be defined");
        this._requireParseFields = new h.Map, this._requireParseFields.set(h.ConfigurationFiel
            logLevel: h.Logger.LOG_LEVEL.INFO,
            orientationEventsSamplePeriod: 300,
            orientationEventsThreshold: 1,
            stateChangeEnabled: !1,
            accelerometerEventsSamplePeriod: 0,
            dataQPassWorkerInterval: 500,
            gyroEventsSamplePeriod: 0,
            gyroEventsThreshold: .3,
            isContextPropsFeature: !0,
            isEnabled: !0,
            isResetEveryLoad: !1,
            isScrollCollect: !0,
            isUnsupportedReport: !0,
            isVMDetection: !0,
            isAudioDetection: !0,
            isHistoryNavigationEvent: !1,
            wupStatisticsLogIntervalMs: 3e4,
            resetSessionApiThreshold: 2e4,
            wupMessageRequestTimeout: 3e3,
            logMessageRequestTimeout: 3e3,
            forceDynamicDataWupDispatchSettings: !0,
            dataWupDispatchRateSettings: h.ConfigurationDefaultTemplates.defaultDynamicWupDisp
            logWupDispatchRateSettings: {
                type: "constant",
                initialRateValueMs: 2500
            },
            serverCommunicationSettings: {
                sendRetryRate: 1e3,
                queueLoadThreshold: 100
            },
            ipDetectorTimeout: 2e3,
            collectKeyRegionValue: !1
        }, this._cid = "", this._messageBus = e, this.updateConfiguration(this.configDefault)
    }
```

- Static, single obfuscation model
- Easily reverse engineered
- Easily spoofed
- Re-used between customers

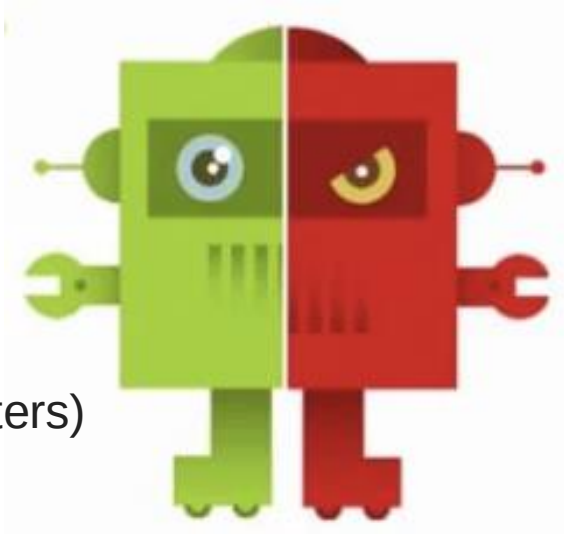
Shape JavaScript

```
, function(vd) {
    vd.V[vd.V.length - 2] = vd.V[vd.V.length - 2] === vd.V[vd.V.length - 1];
    vd.V.length -= 1
}
];
function Qh(vn, vY, vQ, vG) {
    "use strict";
    var va = B[vn];
    return vR(vY, vQ, vG, va.E, va.b, va.C, va.Z, va.q, va.h)
}
;var Rj = n;
var dq = M("JgV7XBgPAQduSwCTBc5GrNoC_FMAdQBGaQReGaL2AykAAcgCBLQvNQ8CH9cAAnUJqQEg
tDMc7gAcAAXIAgW0R-ruAJQABsgCALQ1JO4CPwAHyAIAtPTuDwM1UwB1CEZpAV7OsukC4tcACXUIXvN3
qQEq_MYAWe4ANww7NwCxOJUJAU0ADcgCBbThrg8BClMAdQ5GaQReepXpANFTAHUPRmkAXlqO9gDjABDI
yAIDtLqMDwHAUwB1E0ZpAl7aGvYCKQAUyAIBtMfq7gELABXIAgW03m_uAzMAFsgCCekBJmftAlsAF283
Agm0T3APAnzXABp1A6kBEXRwAHoAGzs3ArGN0wkDGwAcyAIItE3tDwIXUwB1HUZpA179N-kAxlMAdR5G
ACDIAgW0-2buAsIAIcgCCLSXge4CQAAiyAIAtO6WDwBLUwB1I0ZpAF7pu-kAE1MAdSRGaQGpAQhDxgCM
AsMAJzs3ArG3d9oA_tcAKHUEXmyL6QKIUwB1KUZpBV7rb-kAP1MAdSpGaQZeC_j2Am8AK8gCA7RMuA8B
AMTXAC51CV6pLekBtVMAdS9GaQFejzb2AaIAMMgCArRYpe4CkAAxyAIJtNCNDwBTUwB1MkZpAl7aNekC
XhD39gCAADXIAgC0tDcPAaxTAHU2RmkAXsc-9gDIADfIAgO05doPAwzXADh1Al6rI_YBYAA5yAIBtHpz
Xo4e6QKB1wA8dQVe3SL2AowAPcgCAOkBGeiYArebAMc-1McFe_j0DwMyUwB1P0ZpAqkBE-twAf8AQDs3
Agm0MiAPAkRTAHVDRmkEXoBB6QGHUwB1REZpAF7qdukC31MAdUVGaQVeixbpAPHXAEZ1CV4ULukC5FMA
6QJ1UwB1SUZpCakBNKpwAv0ASjs3B7G5g9oB39cAS3UJXmGH6QMk1wBMdQmpASdvcALzAE07NwSxq_Ta
vtoAI9cAUHUHqQEwhXAAUgBROzcH5wEeFNsAUABSOzcBsY0M2gE0UwB1U0ZpAqkBKgHGAZ7uADdUOzcB
AHVWRmkGXuhj6QIC1wBXdQVeIibpAlZTAHVYRmkFXpMi6QFv1wBZdQZerUbpAhJTAHVaRmkCXgeb6QAB
DwC21wBddQJet0rpAVFTAHVeRmkIXs196QLcUwB1X0ZpAF4VHukB7lMAdWBGaQReI8H2ABgAYcgCA7QR
Yzs3ALEIAAkB9QBkyAIDtJMxDwIaUwB1ZUZpCV5KxukC6lMAdWZGaQNeFPH2ApwAZ8gCBbQP7g8CmFMA
MVMAdWpGaQKpASaAxgCy7gA3azs3BLH5ugkAKABsyAIJtAh17gAkAG3IAgm0FNoPABdTAHVuRmkFXs32
aQBe7yHpAxlTAHVxRmkJXugr6QDKUwB1ckZpB14_wekASFMAdXNGaQRegqv2ANUAdMgCBrSqdA8A19cA
PlMAdXdGHgBMvmBLSDYBVE8ESwE2AVPmAE8BRBsAUwEXAU_SBEuNNgFATQdrAjlZAcWWWQF8AUQEADAA
rwLOns9ShgYFCZmDowCSAIWvABqefs8GBAQmB09lWQFzRFoGIQMMSAIA0BMBOvIEJ0QGIAfiWQCTBqgB
JgNTAMDuA84Dva8CecgCBLR_WQ8A6XEDAlNpBF5OfekA91MDtwSrWQMPs5MBJQEgiRIBBQMCcEcAJdTH
```

- Unique obfuscation for each telemetry source
- Continuous, revolving obfuscation
- Spoof proof data
- Unique for each enterprise

What Shape JavaScript Does Not Collect

- Security credentials
- Personally identifiable information (PII)*
- POST body (such as html form data)
- Files uploaded or downloaded
- Content in html web pages
- Characters typed by user on web page (e.g. a-z, 0-9, special characters)
- Application-level data beyond standard http headers
- User's geographic location



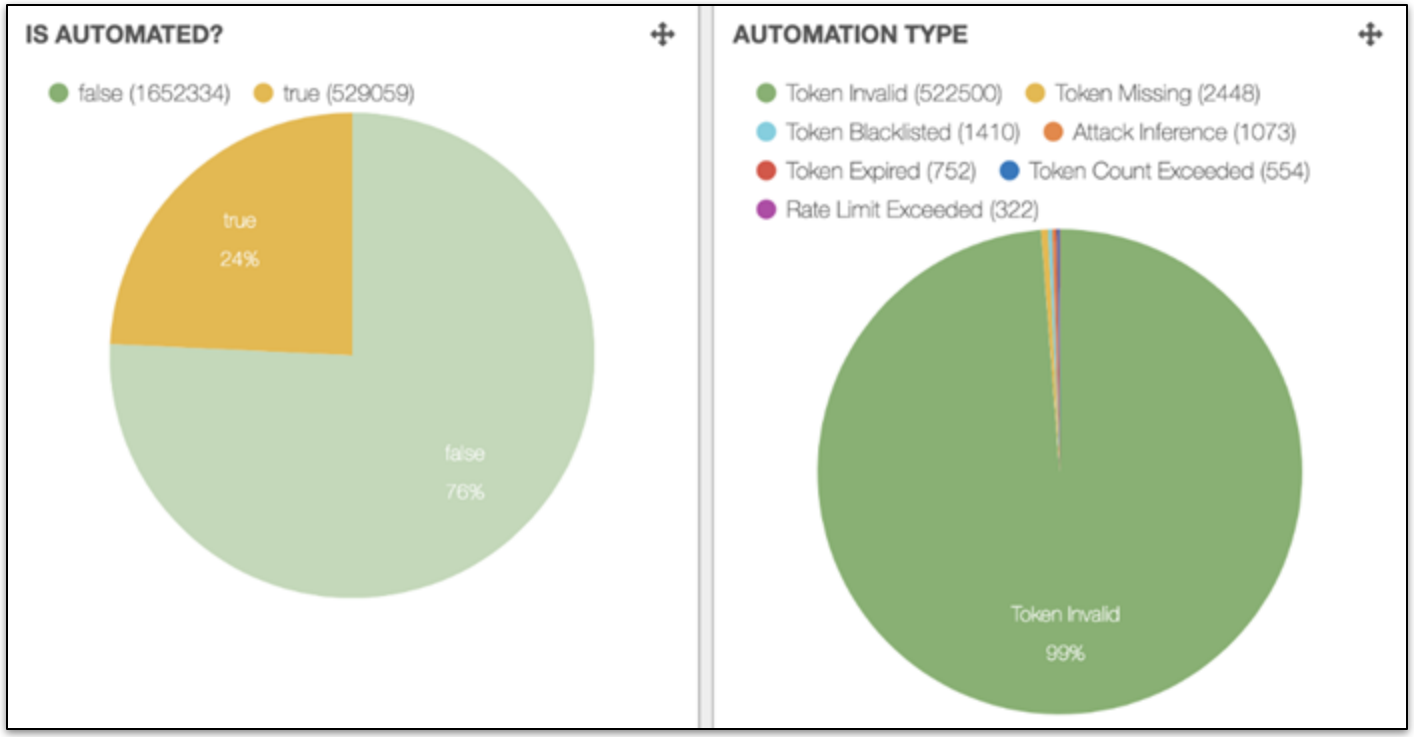
Shape does NOT collect any sensitive user data

* Shape collects the client IP address, which may be considered PII according to some interpretations (e.g. GDPR)

Shape Performs Analysis & Provides Deterministic Results

AS OPPOSED TO RISK SCORING, WHICH PROVIDES ROOM FOR UNCERTAINTY

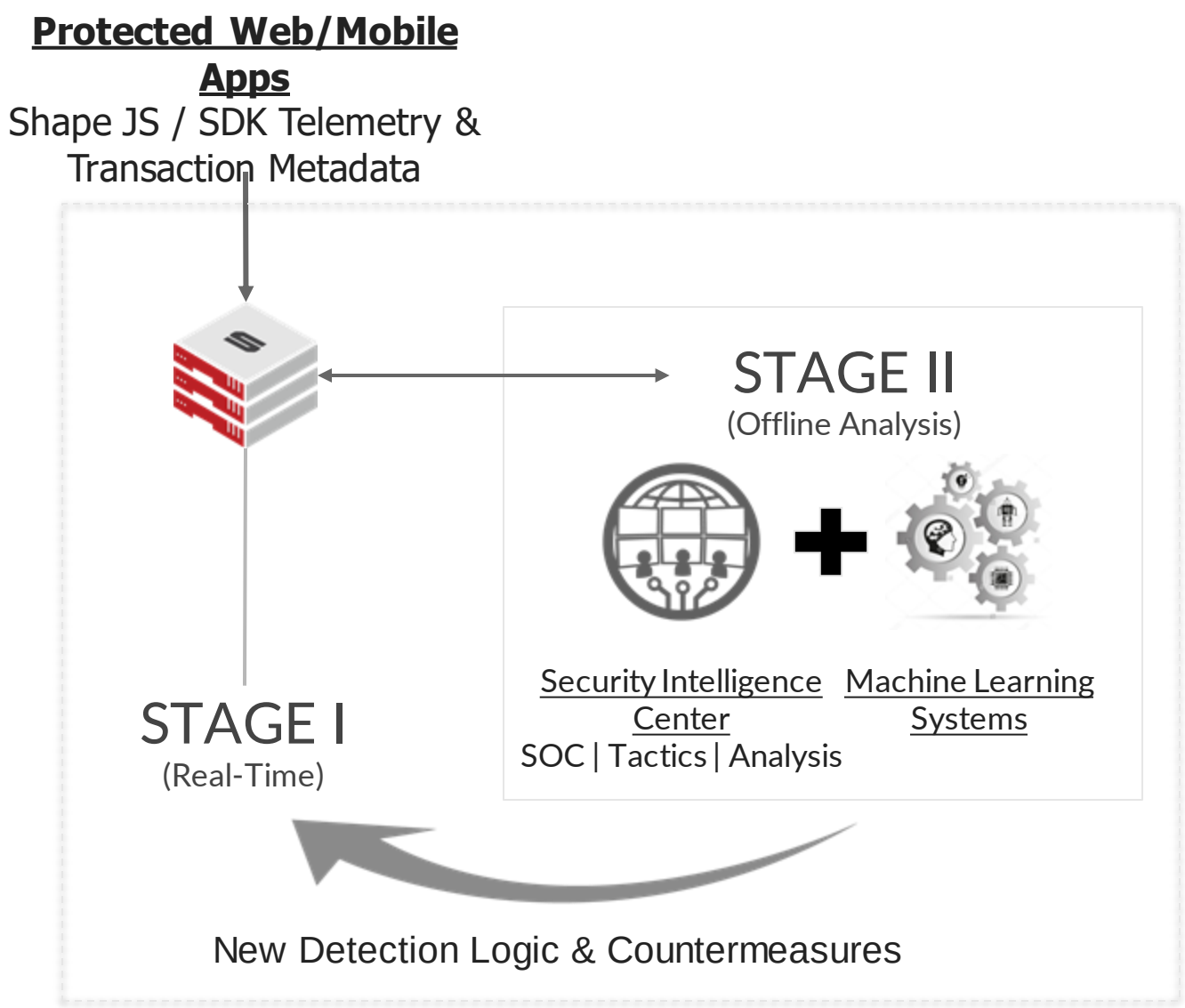
Environmental Signals + **Behavioral Signals** + **Network Signals** = **Automated? Yes / No**



Shape pinpoints fraud using:

- Session ID based on unique interrogation
- User interaction patterns
- HTTP Header indicators
- Input timing and interactions
- Traffic source analysis

Continuous Improvement to Detection & Mitigation



Modes

- Non-Blocking (Observation)
- Blocking (Mitigation)

Stage I

- Advanced Signals Analysis
- Real-time Mitigation
  - Allow
  - Flag
  - Flag & Allow
  - Block

Stage II

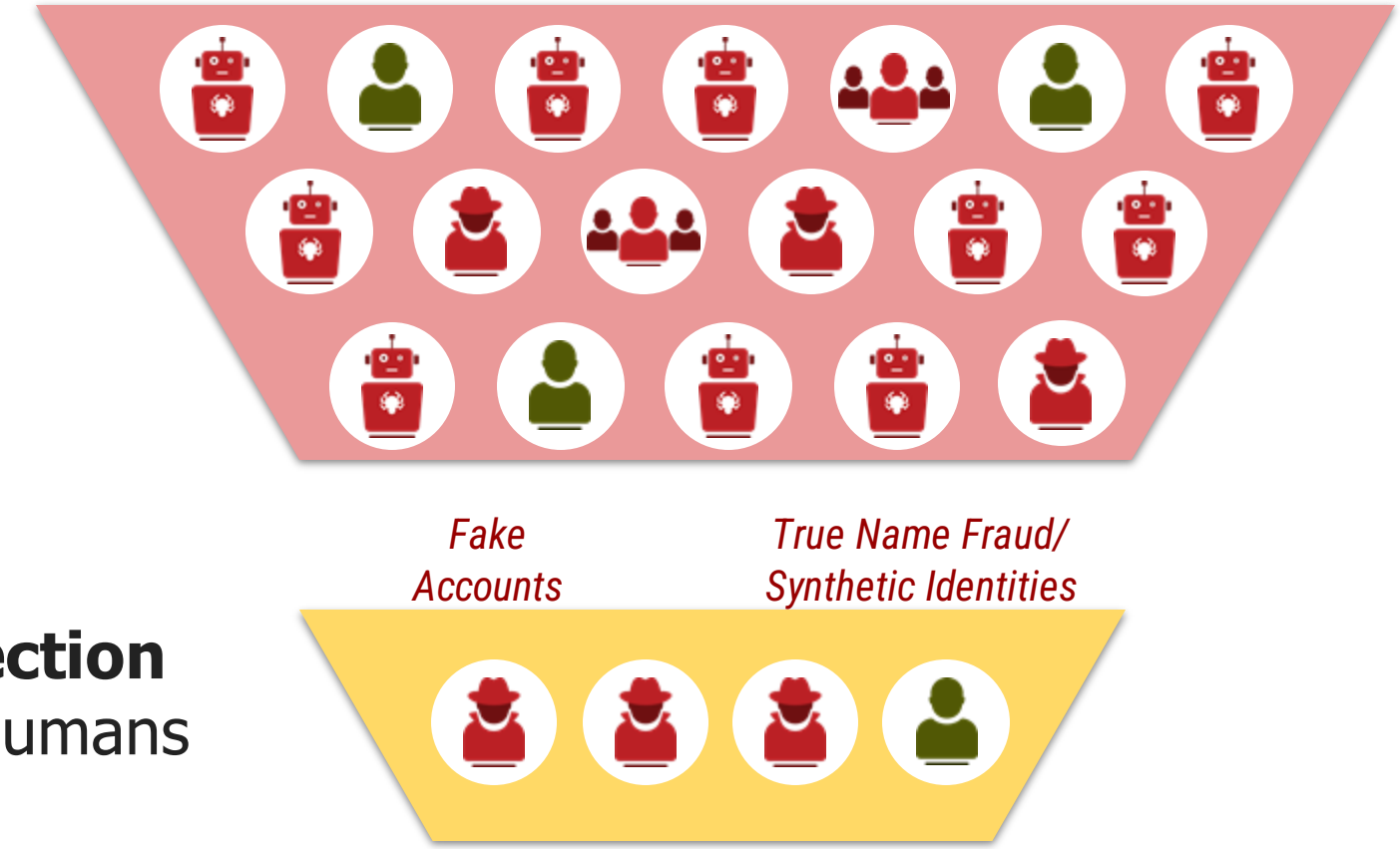
- Artificial Intelligence
- Machine Learning
- Data Scientists
- Investigative Analysts
- 24x7 Threat Mitigation Center

SHAPE SECURITY-AS-A-SERVICE

The XC Account Protection

The Shape Platform

Once synthetic traffic is gone, we focus on identifying the bad organic traffic



Account Protection

Differentiate good humans from bad humans

Account Protection builds on top of battle-tested signals

WHAT

User journey

What high risk actions did this user/device take (logging in, creating account, applying for claim etc.)

HOW

Behavioral insights

Were there any anomalous interaction that indicate fraudulent behavior?

WHO

Environment insights

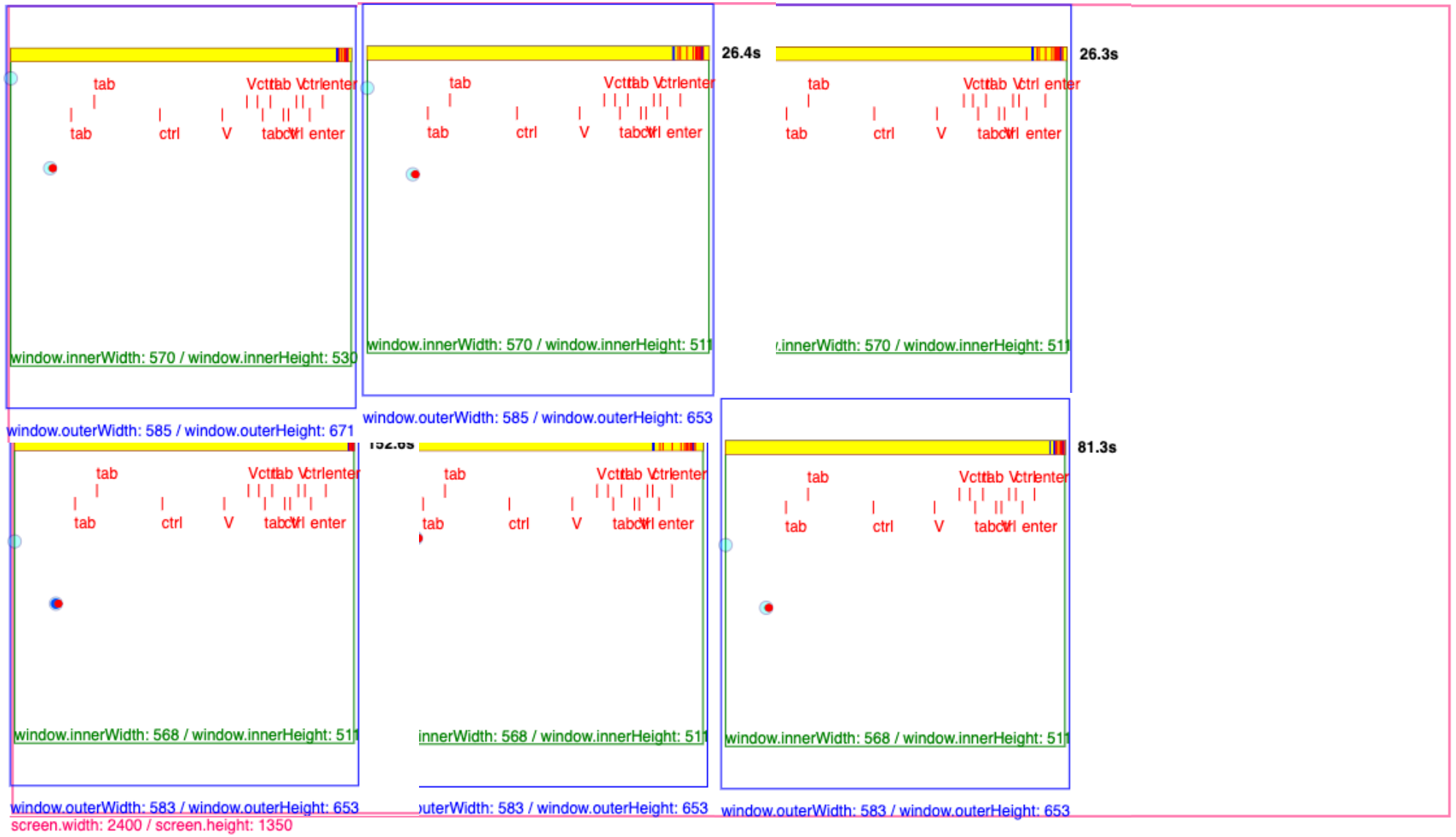
“who” is the browser, device, and network that we’re seeing? Is the environment spoofed or have any inconsistency?

SHAPE NETWORK INSIGHTS

Have we seen this user/device/environment conduct fraud elsewhere within Shape’s network?
Is the traffic profile or originating network strongly indicative of fraudulent behavior?

Live Traffic Replay - Replay of one login from fraudster is suspicious

Screen offset, visibility events, pasting all consistent with fraud at scale



Account Protection Also Collected Additional Fraud Metrics - Illustrating Highly Anomalous Device Behavior

Device
AJofIZI5AQAAM-C_SSgjLa4DdrRgVuKXjgdI-4WI8gB26MxAOAizR0GrkjtU

Device age
23 days

No. of transactions
3859

Login

Login Success
0.85%

Accounts Attempted
2699

Account Access Rate
0.74%

Accounts Succeeded
20

Account Repetition Score
1.4

Anomaly Indicators

- 99.7% pasting events
- 1.6% hosting ASNs
- 0.75% unusual keys
- 99.6% small window
- 0% likely VM
- 99.9% unusual time zones
- 5.3% VPN IPs
- 0% switching in and out
- 0% browser spoofing

Datestrings (1)

Search

GMT+0900 (China Daylight Time)

Pastings (4)

Search

USR_LOGIN_NAME
USR_LTPD_PASSWORD
unknown
USR_LOGIN_NAME

IPs (100)

Search

216.131.81.65
199.244.51.226
199.244.51.74
138.128.245.65
174.139.46.66
138.128.246.36
174.139.137.35
173.213.87.152

Usernames (30)

Search

84c77d726d***
58f2da895c***
c0181c3acc***
4671ef3622***
4518a46f27***
03d1908acc***
3fb28890b2***
2ef1c0091b***

In Conclusion

Globalized network of signals & ML used to catch retooling

Billions of signals analyzed daily

8/10
Top Banking

2/3
Top Hospitality

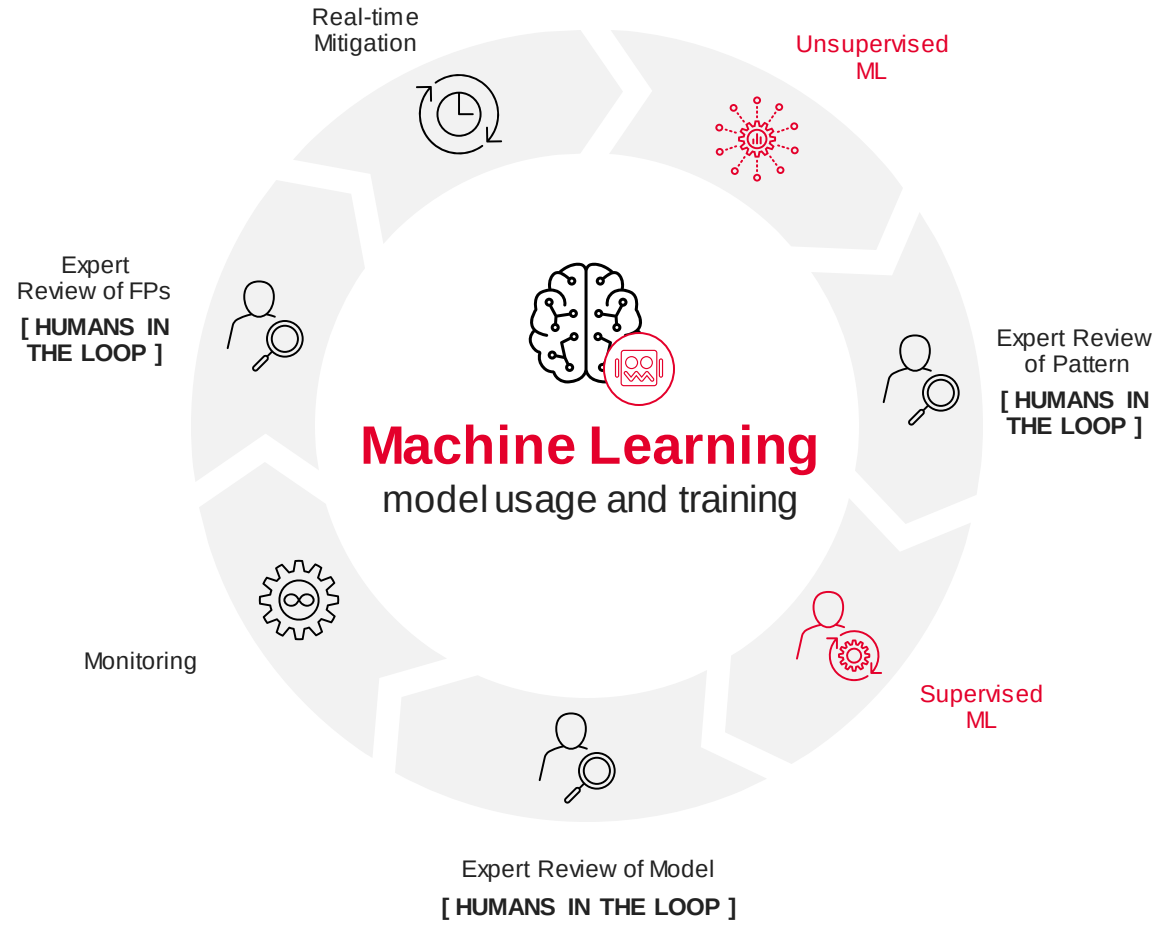
2/10
Top Retail

5/10
Top Credit Cards

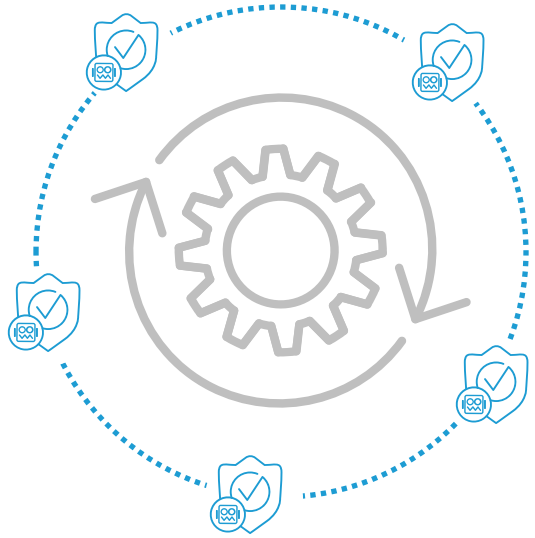
5/10
Top Airlines

2/5
Top Insurance

Rapid intelligent analysis at scale



Dynamically updated mitigation



F5 Reduces Fraud

delivers differentiated outcomes

LESS FRAUD

F5 typically **identifies 2x-5x more fraud per month** than current solutions, while maintaining false positive levels

LESS FRICTION

F5 recommends **up to 90% FEWER MFA challenges** for legitimate users than alternative solutions - less user friction for legitimate users means more revenue

LESS EFFORT

F5 slashes number of transactions that require fraud team review **by more than 50%**

Data 

+ AI 

+ Network