
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

PRT019

SPONSORED BY F5

Protecting your application from bot attacks

Dan Woods

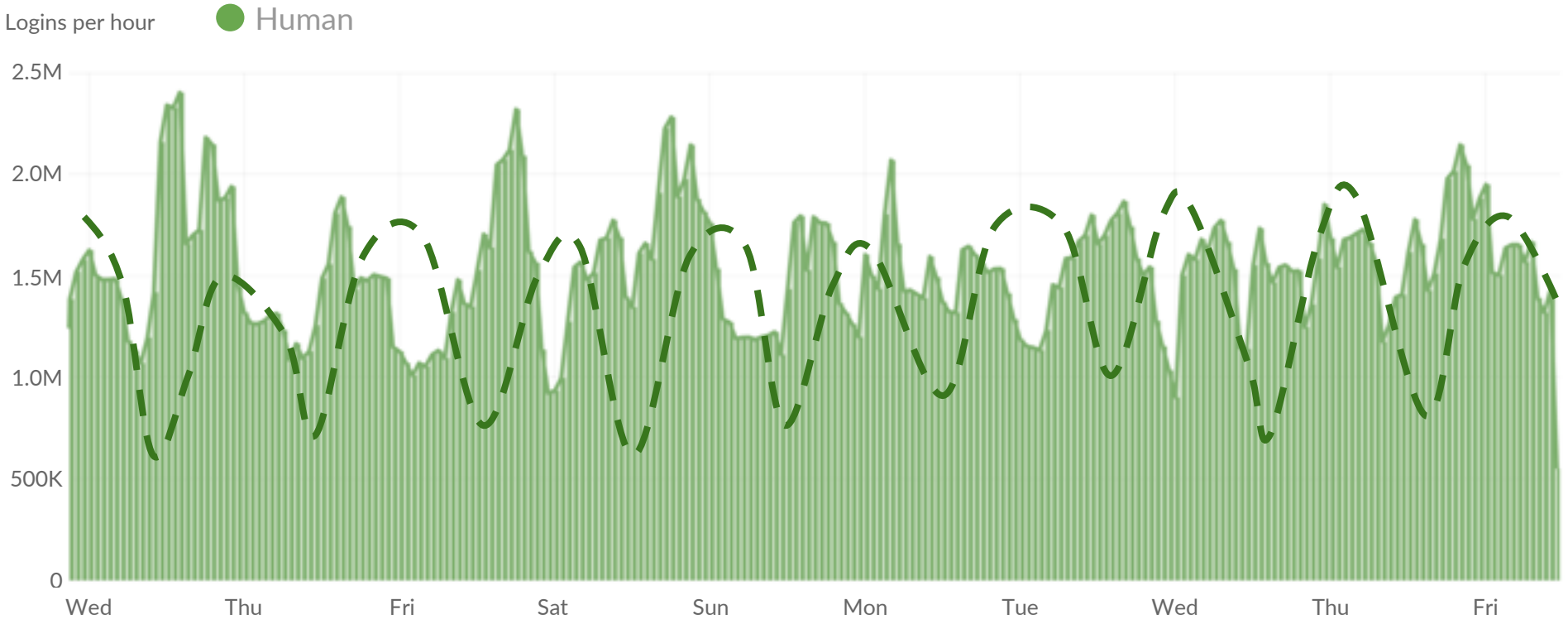
Global Head of Intelligence
F5

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

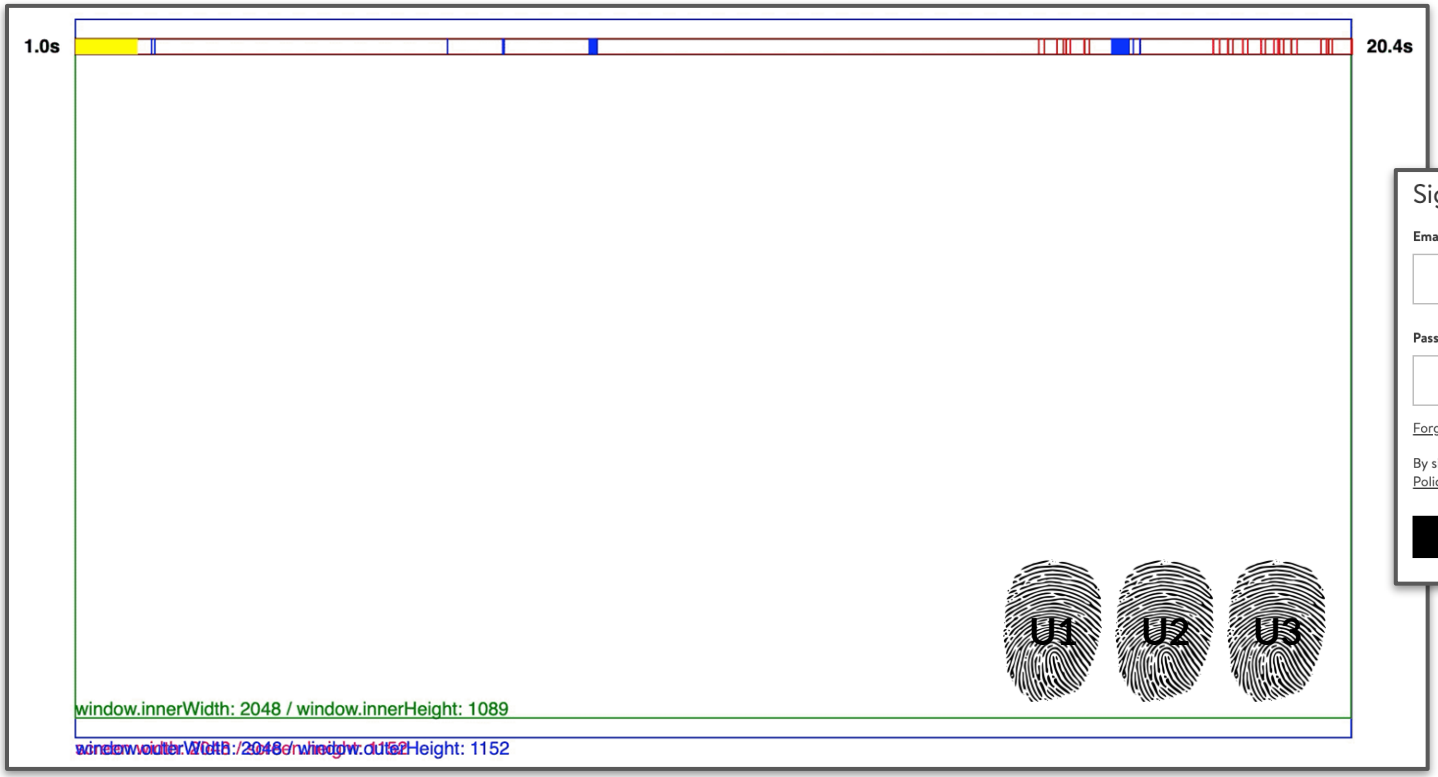
Login traffic at F100 F5 customer

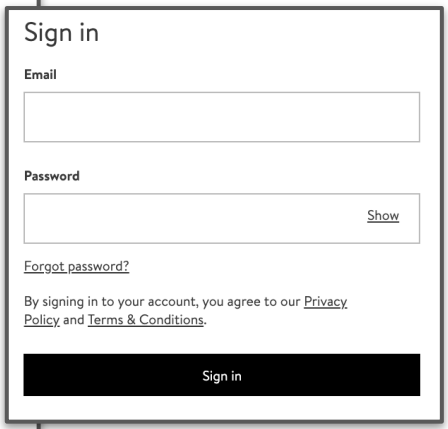
Prior to the application of client-side signals



Visualization of human interaction

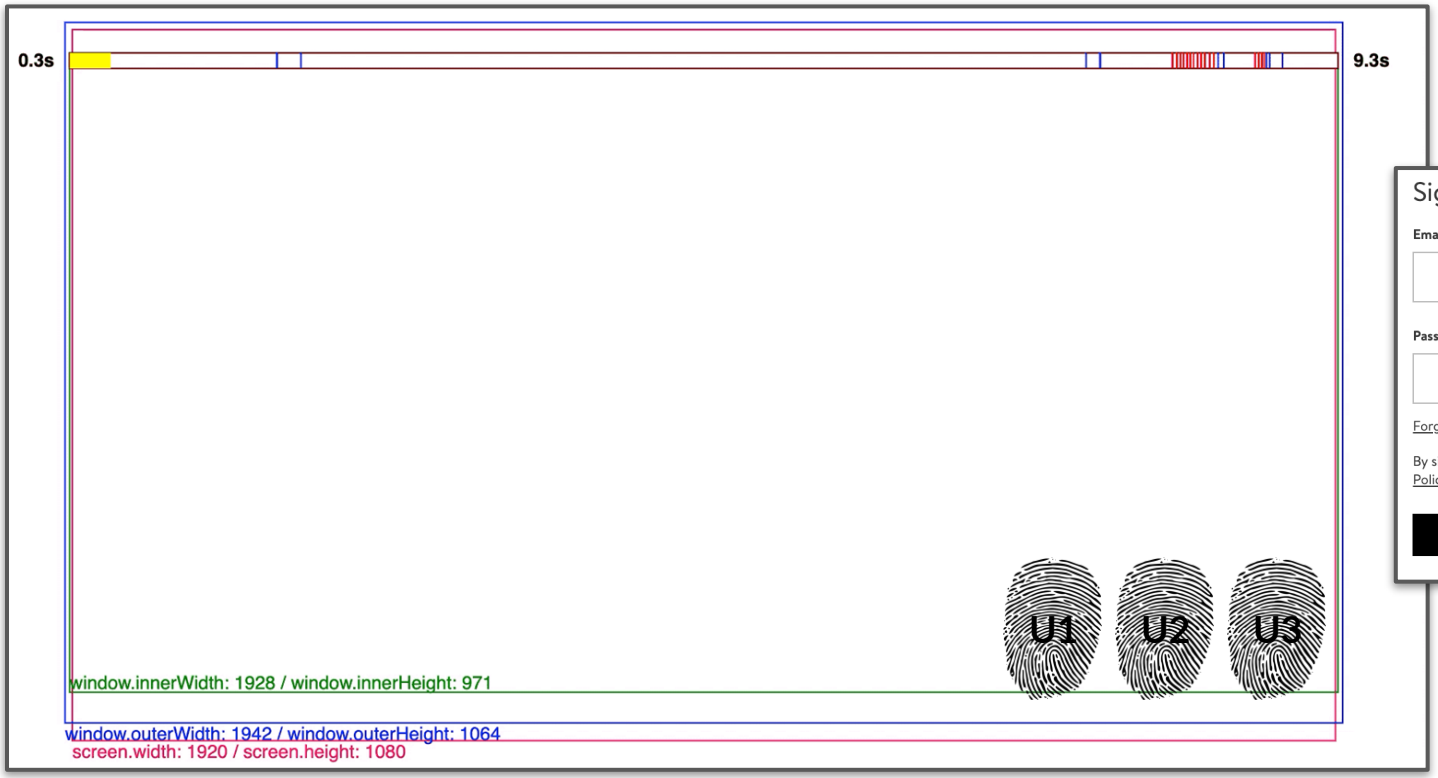
Humans are sometimes clumsy and inefficient in their interaction

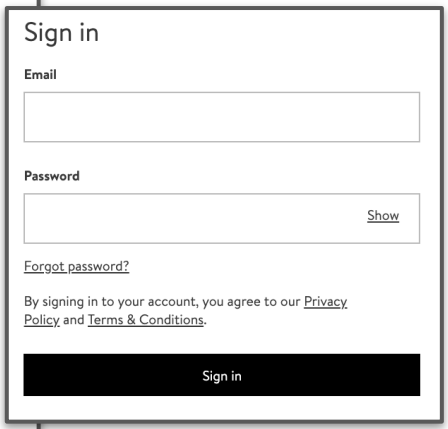




Visualization of automated interaction

Consistent & predictable delays consistent with amateur programmer





Signals can identify anomalous interactions

Detects unauthorized use or account sharing



1.1 to 1.3 seconds

Three separate instances of the customer typing in her password

Signals can identify anomalous interactions

Detects unauthorized use or account sharing



1.1 to 1.3 seconds

Three separate instances of the customer typing in her password

Signals can identify anomalous interactions

Detects unauthorized use or account sharing



1.1 to 1.3 seconds

Three separate instances of the customer typing in her password

Signals can identify anomalous interactions

Detects unauthorized use or account sharing



1.1 to 1.3 seconds

Three separate instances of the customer typing in her password

Signals can identify anomalous interactions

Detects unauthorized use or account sharing

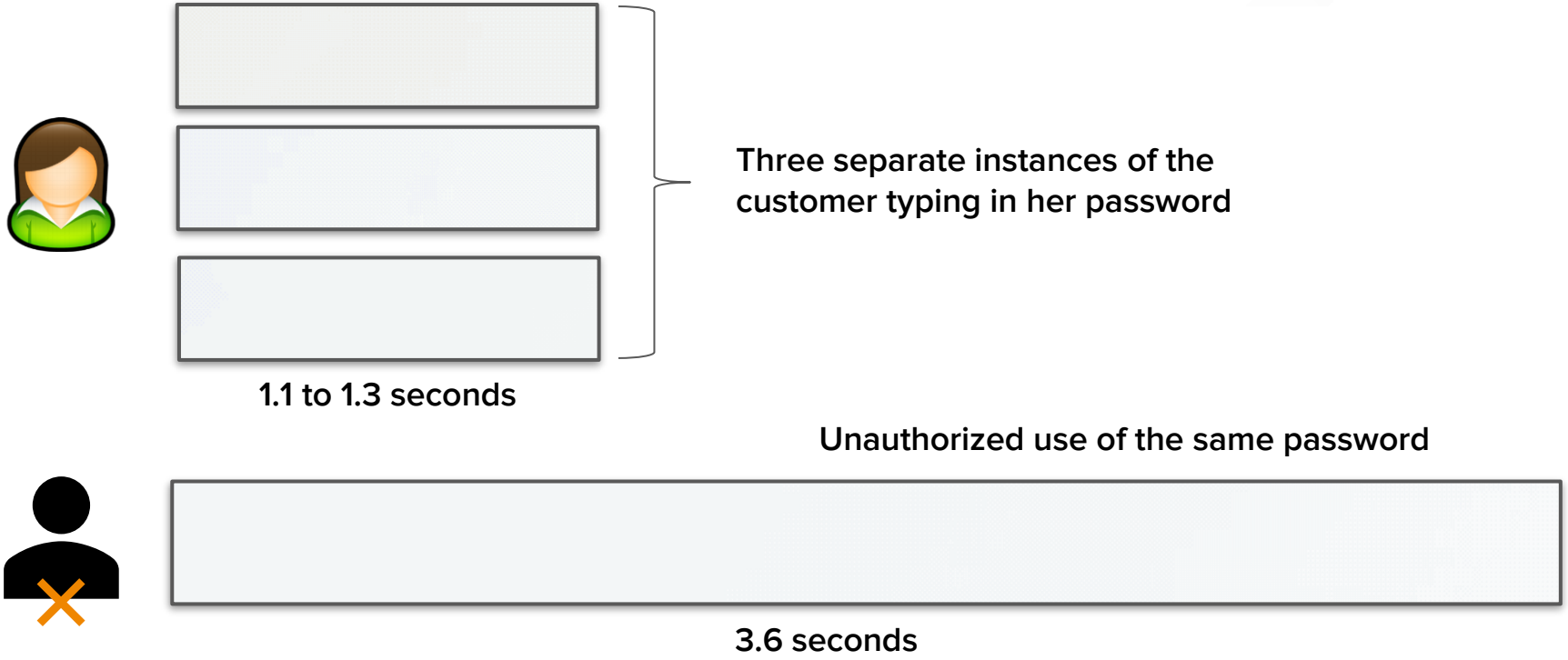


1.1 to 1.3 seconds

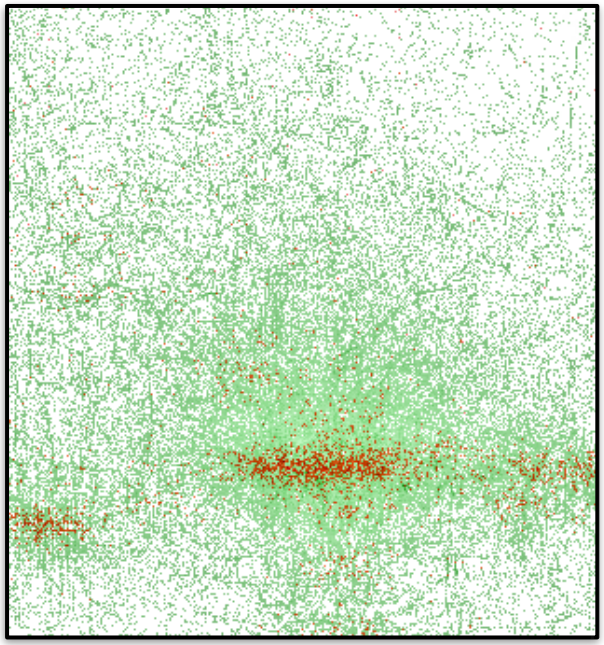
Three separate instances of the customer typing in her password

Signals can identify anomalous interactions

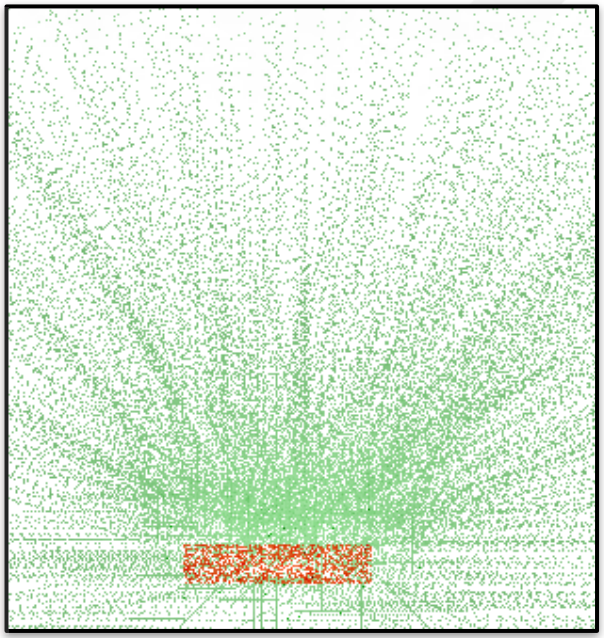
Detects unauthorized use or account sharing



Unauthorized activity is typically very efficient



Humans engaged in unauthorized *manual* activity



Customers

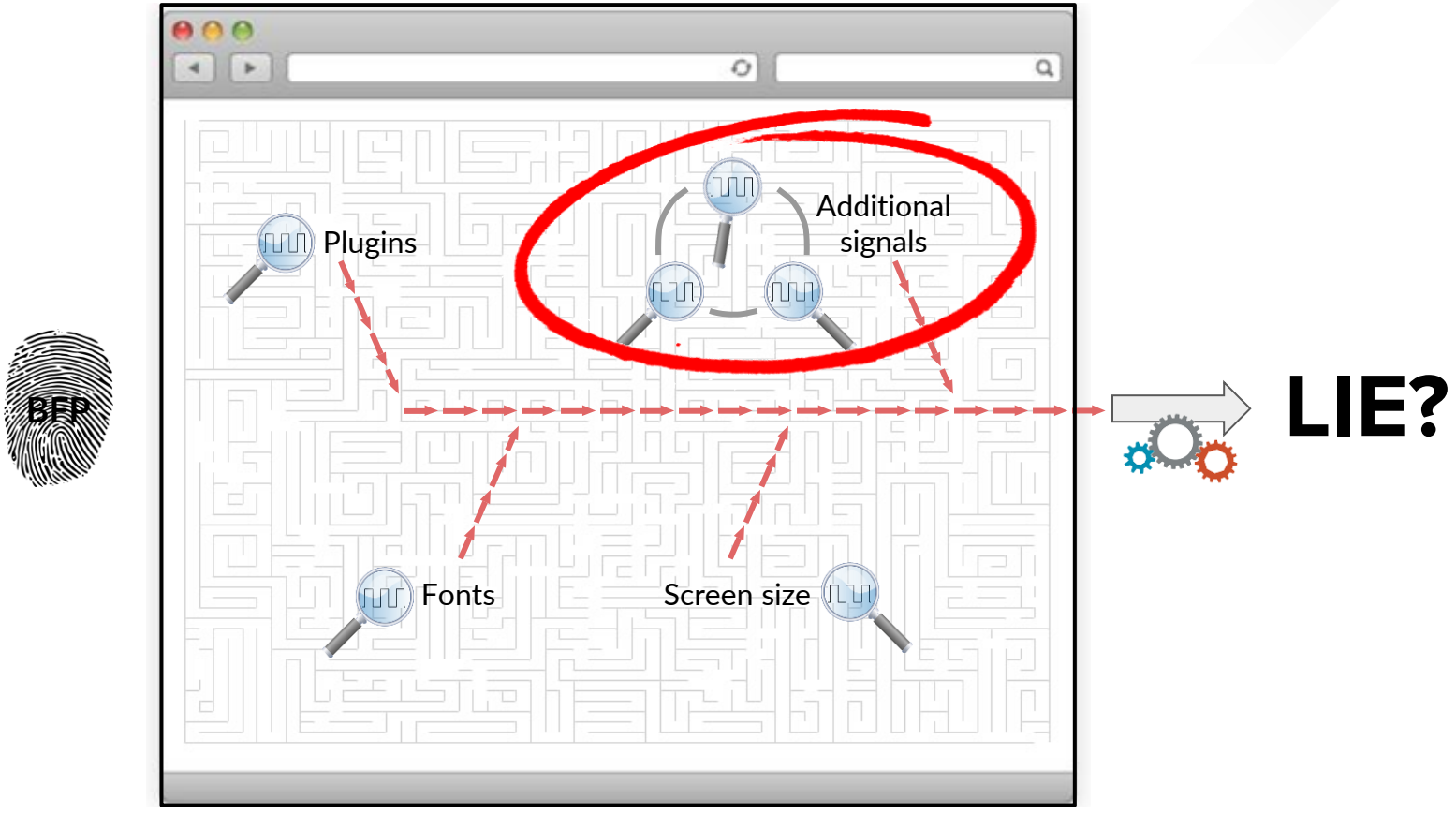
Bots

Increasing speed of navigating workflows

Mouse move Mouse click

Unauthorized users need to spoof signals

Client-side signals identify users who are lying about something



Emojis render differently in different environments

:-)





Really big numbers convert differently on different platforms

0xFFFFFFFFFFFFBFF

=

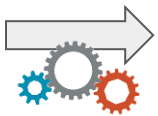
18,446,744,073,709,552,000
18,446,744,073,709,550,000
18,446,744,073,709,550,591

Even the HTTP header contains useful signals

Unauthorized users struggle to spoof everything correctly



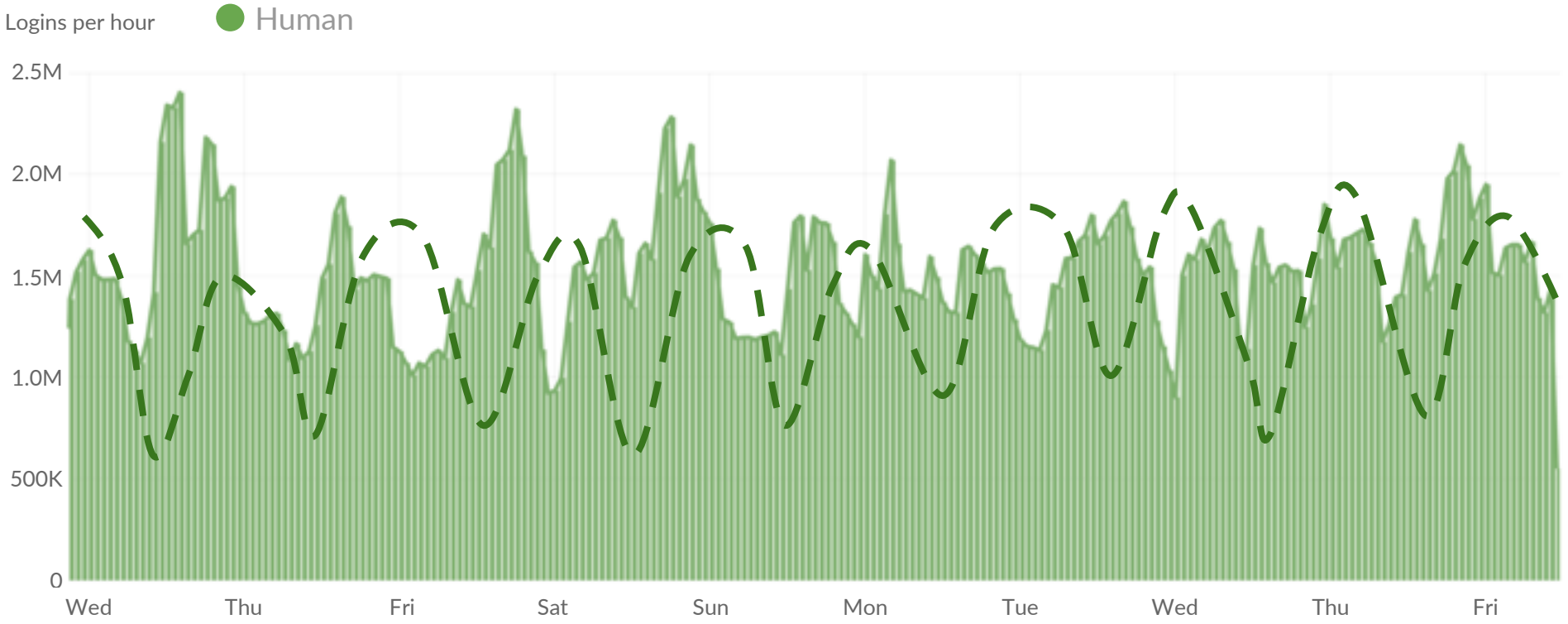
Header Field	Description	Example
Accept	Content-Types that are acceptable for the response. See Content negotiation.	`Accept: text/plain`
Accept-Charset	Character sets that are acceptable.	`Accept-Charset: utf-8`
Accept-Encoding	List of acceptable encodings. See HTTP compression.	`Accept-Encoding: gzip, deflate`
Accept-Language	List of acceptable human languages for response. See Content negotiation.	`Accept-Language: en-US`
Accept-Datetime	Acceptable version in time.	`Accept-Datetime: Thu, 31 May 2007 20:35:00 GMT`
Authorization	Authentication credentials for HTTP authentication.	`Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==`
Cache-Control	Used to specify directives that *must* be obeyed by all caching mechanisms along the request-response chain.	`Cache-Control: no-cache`
Connection	Control options for the current connection and list of hop-by-hop request fields.[7] Must not be used with HTTP/2.[8]	`Connection: keep-alive` `Connection: Upgrade`



LIE?

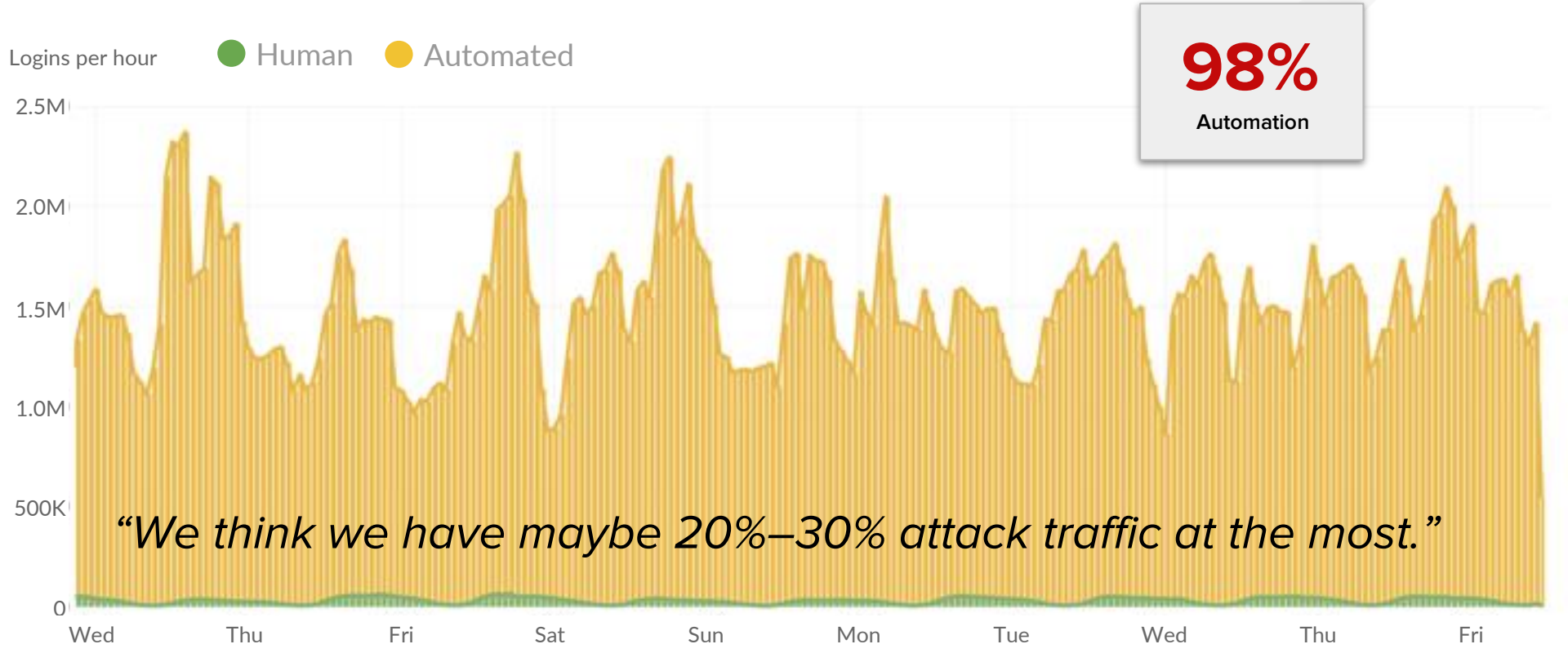
Login traffic at F100 F5 customer

Prior to the application of client-side signals



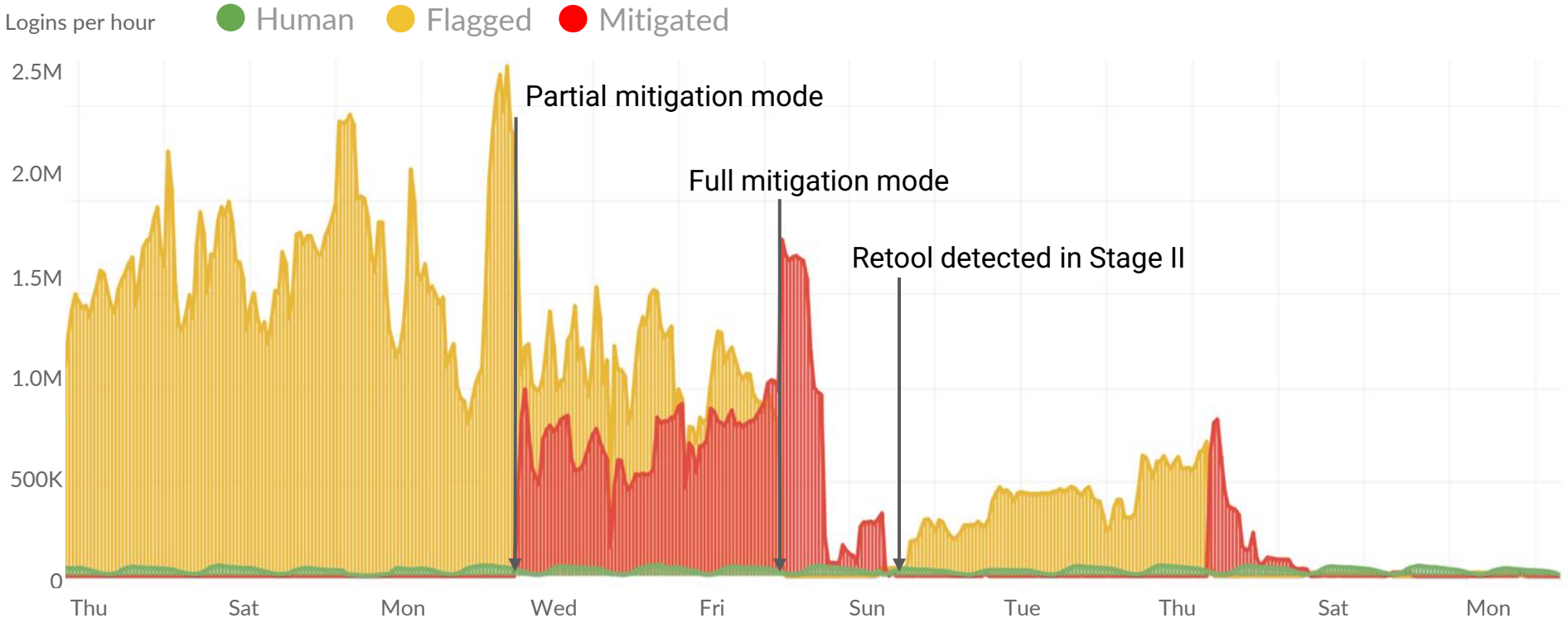
Virtually all login traffic was attempted ATO

Unauthorized traffic originated from millions of IP addresses

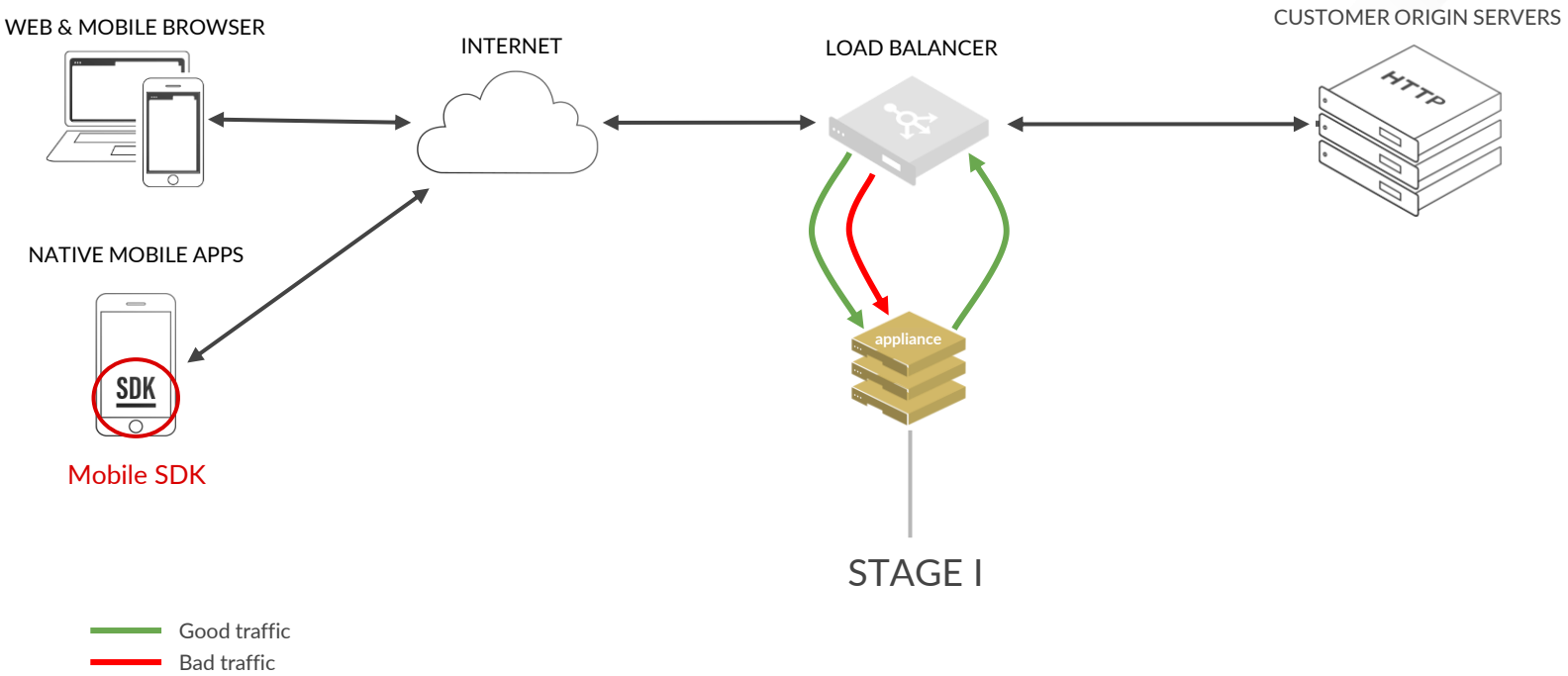


Attempted ATO mitigated using client-side signals

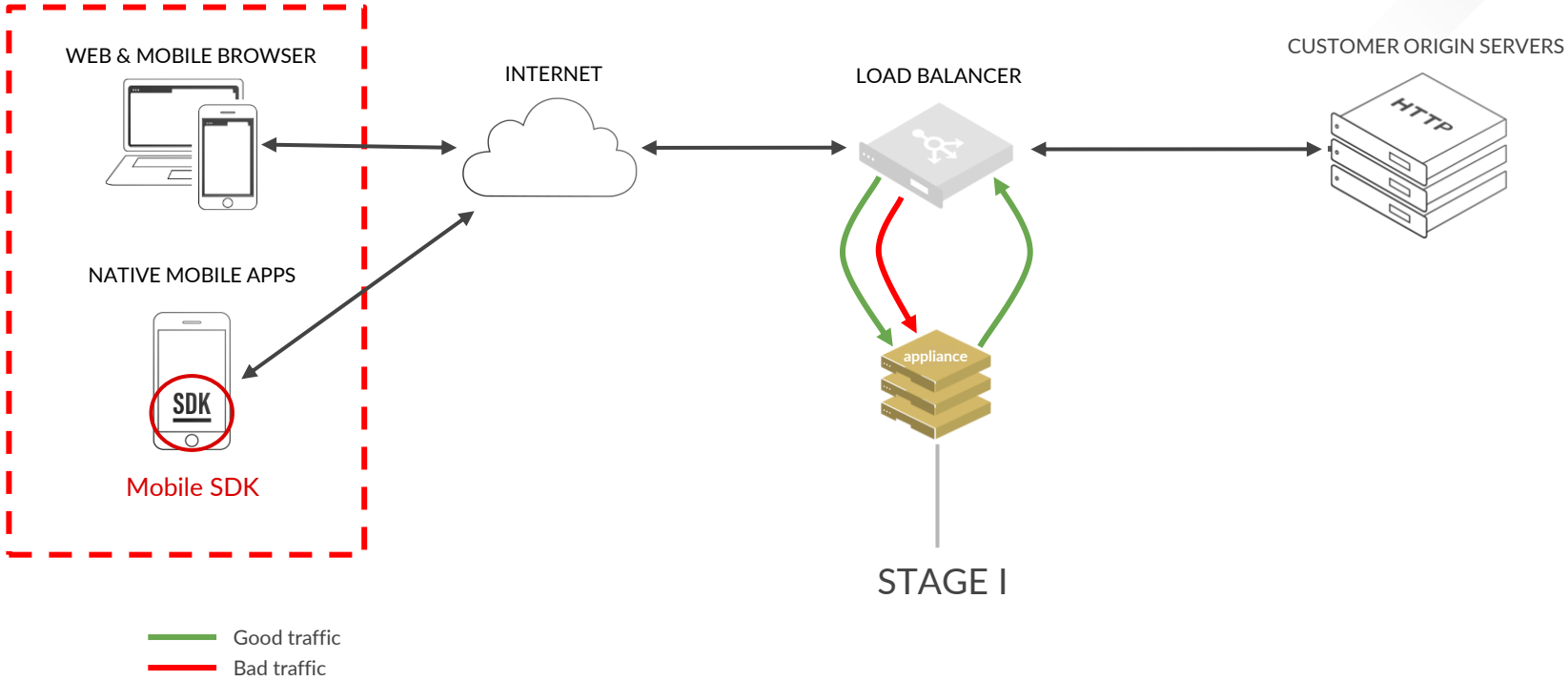
Individual(s) behind the attempted ATO gave up after one retool



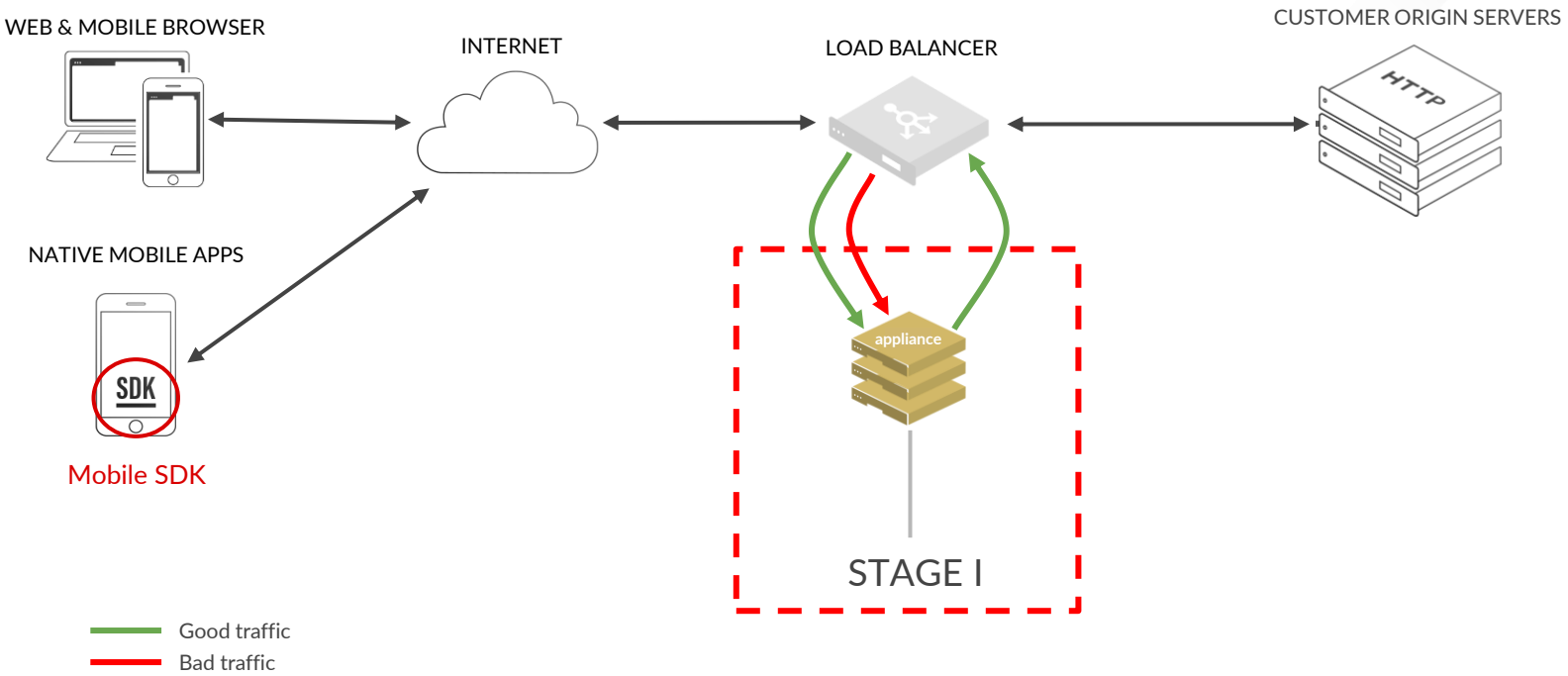
Multi-stage detection is paramount



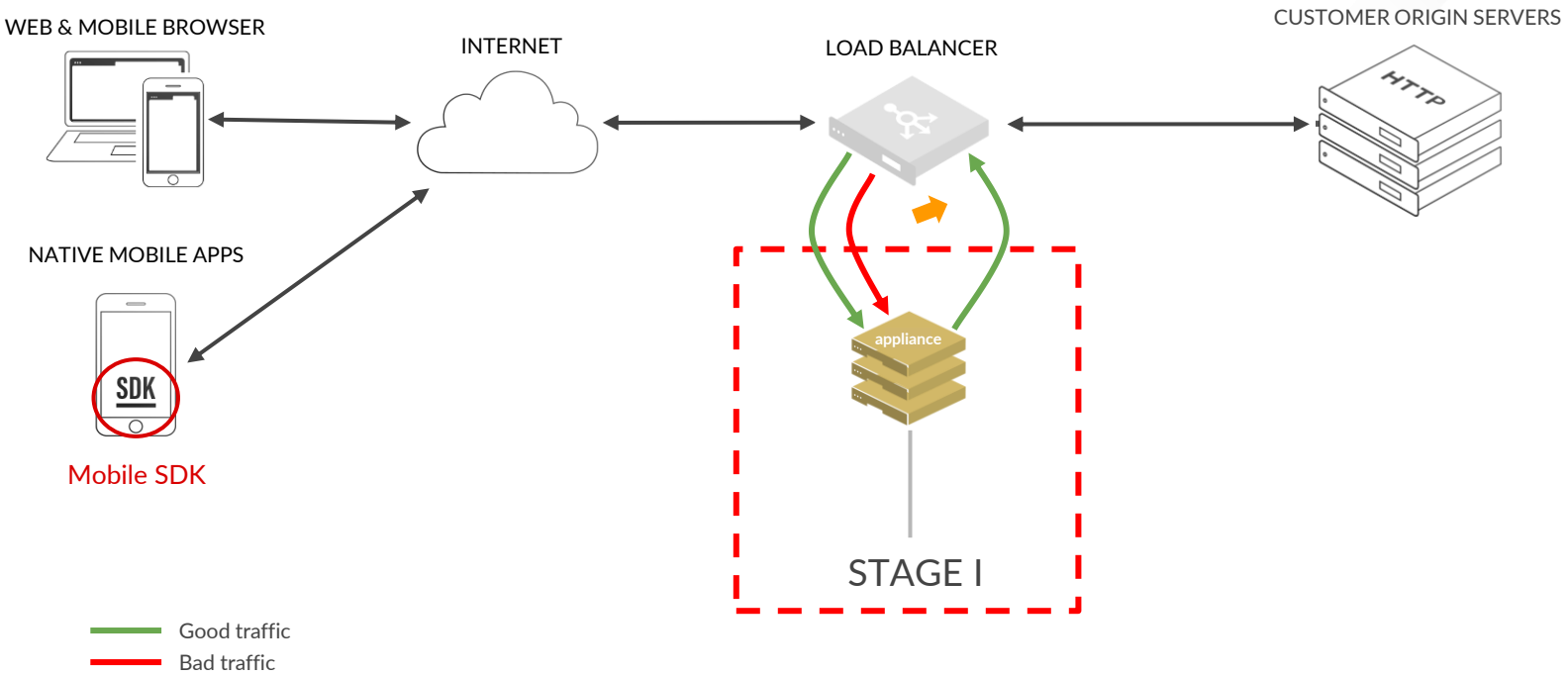
Multi-stage detection is paramount



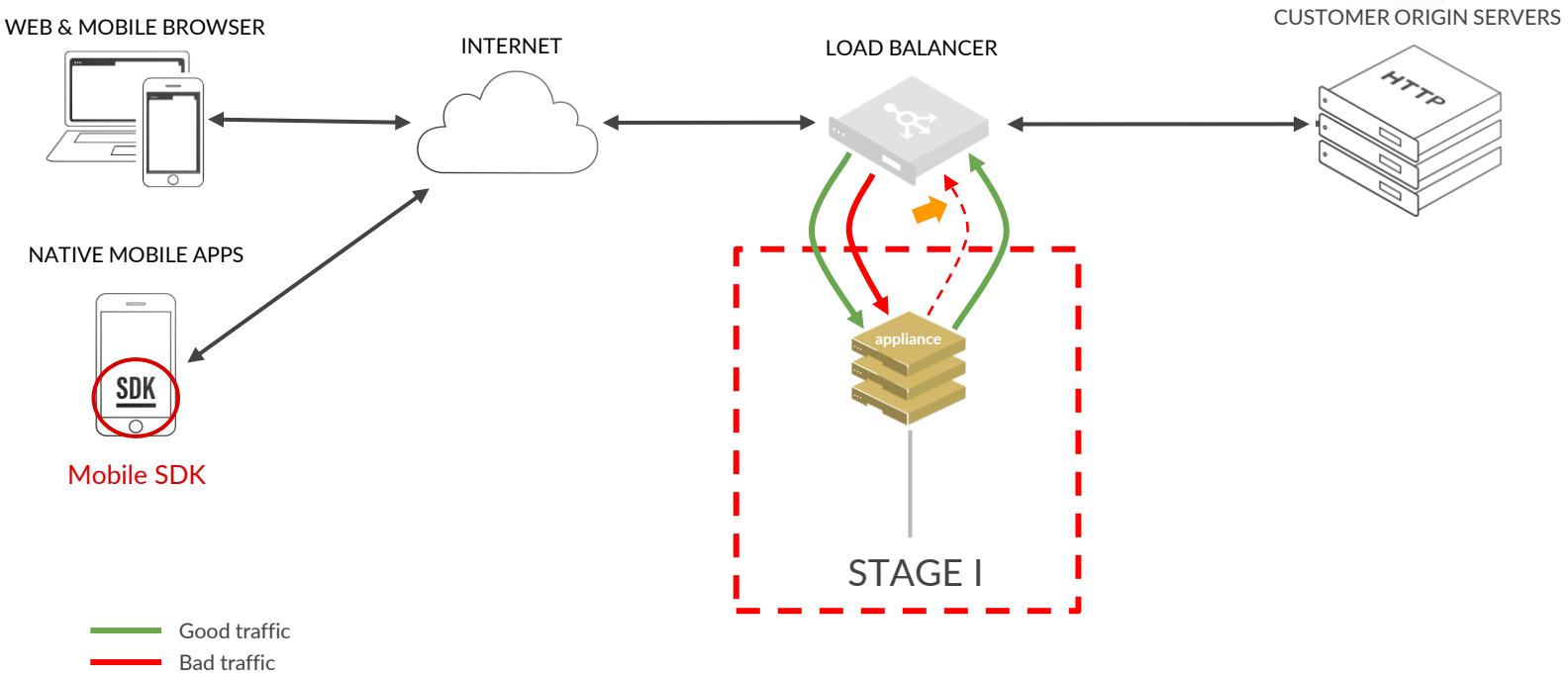
Multi-stage detection is paramount



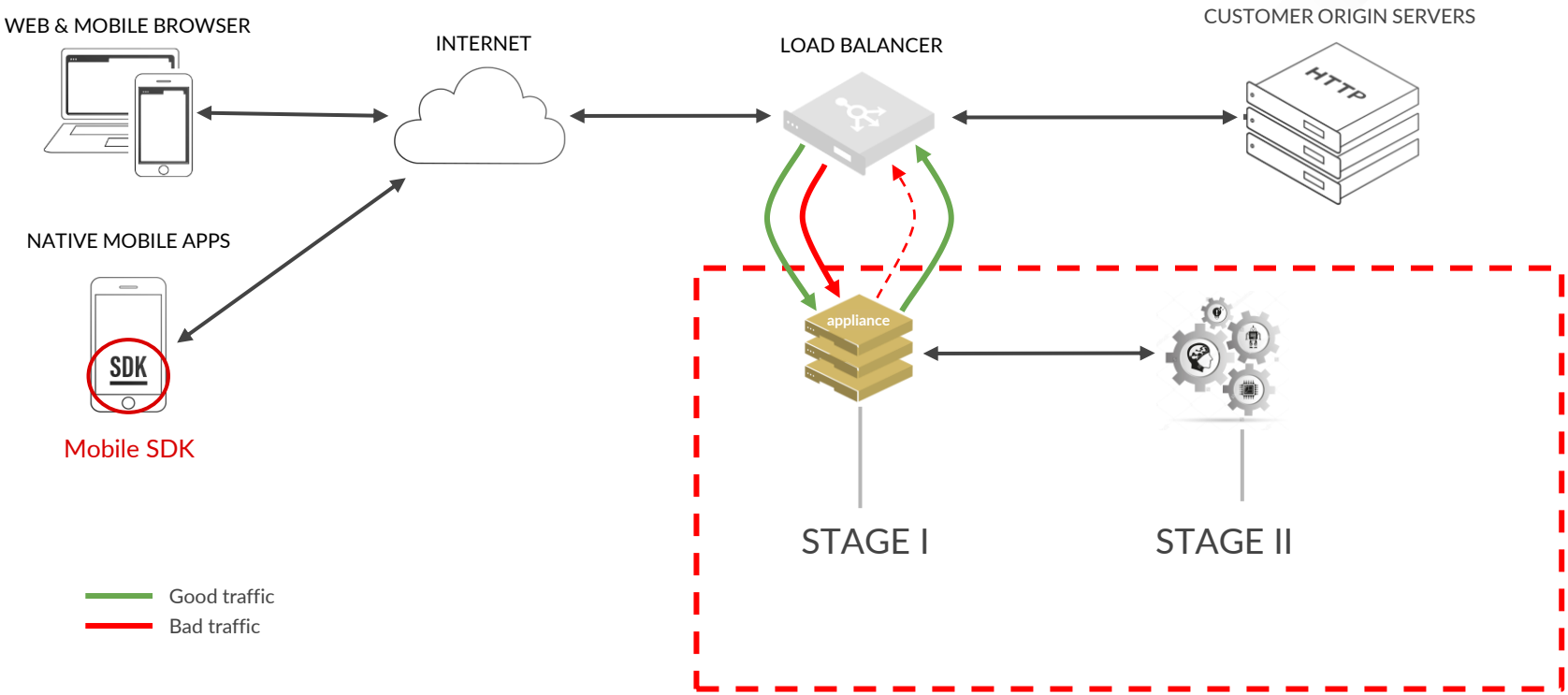
Multi-stage detection is paramount



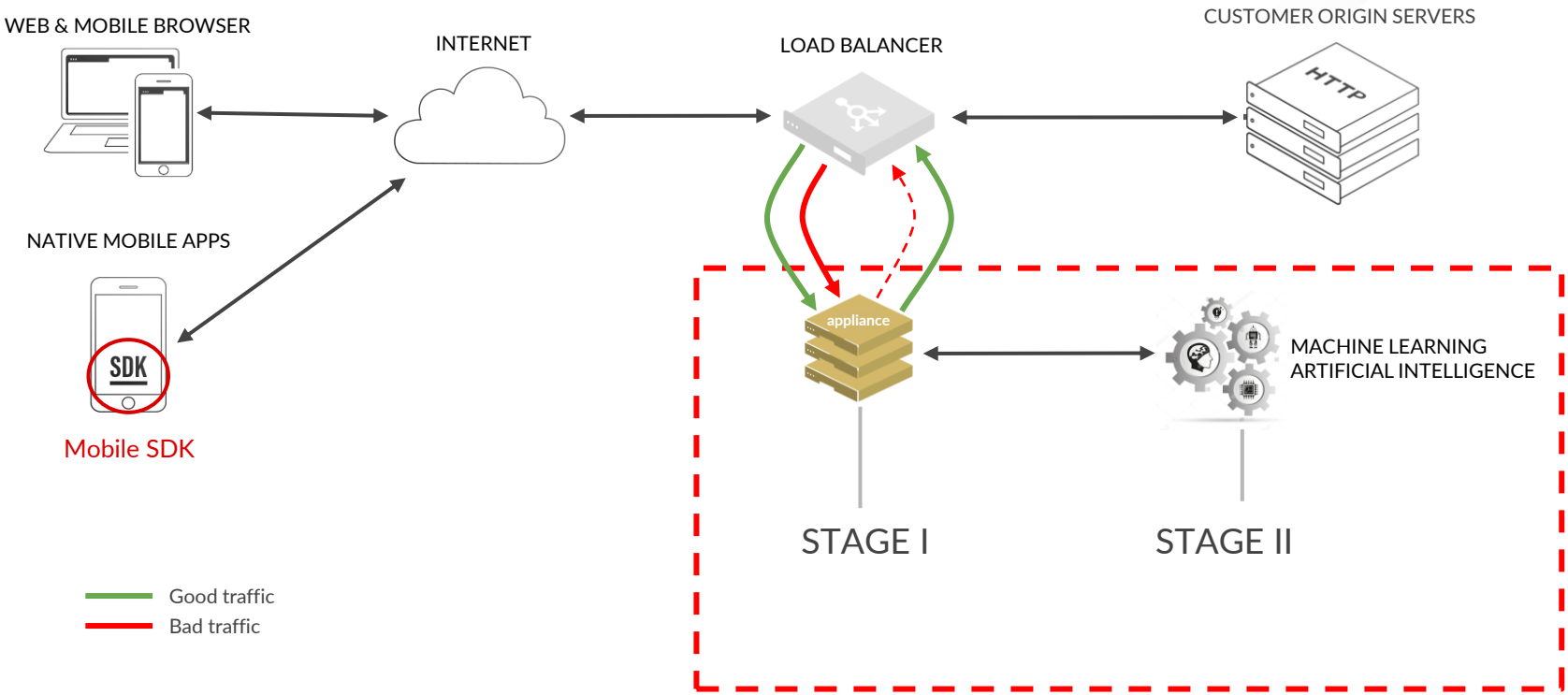
Multi-stage detection is paramount



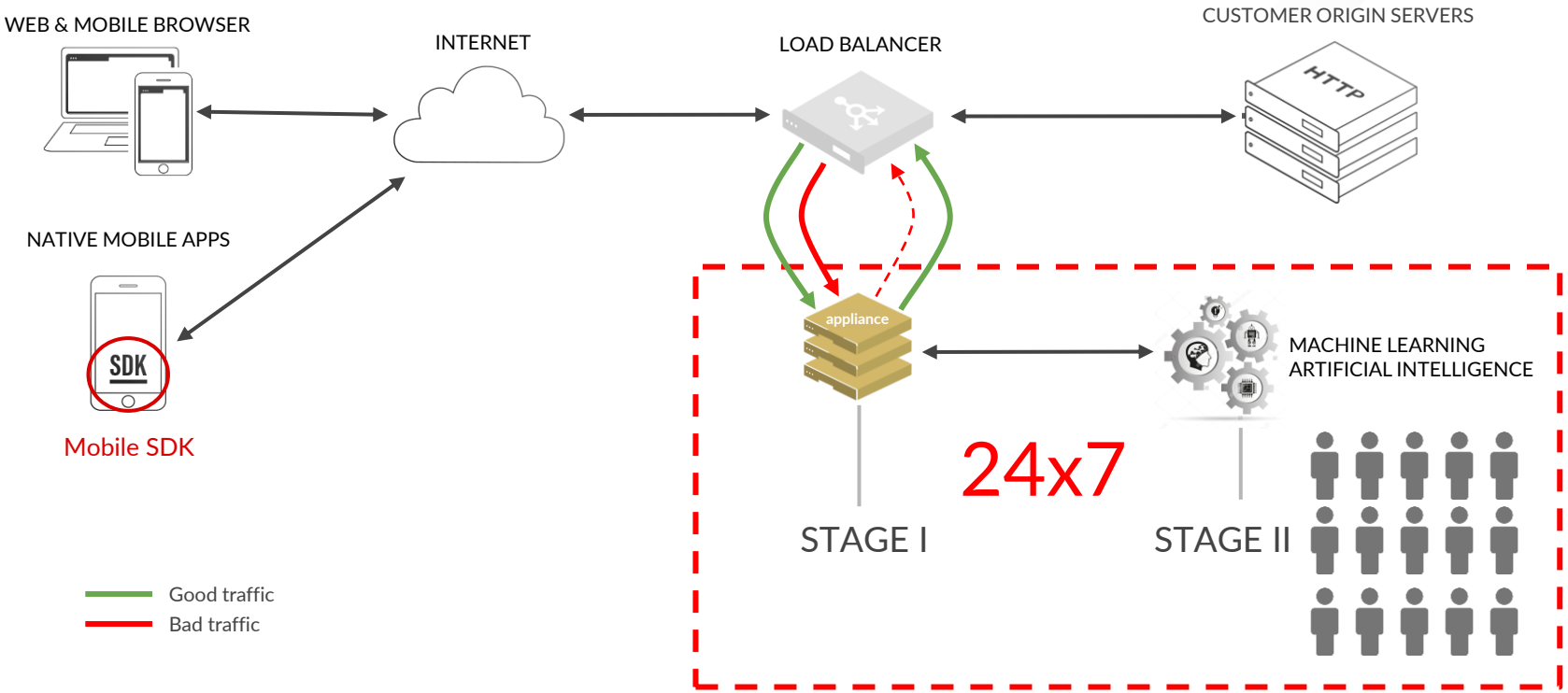
Multi-stage detection is paramount



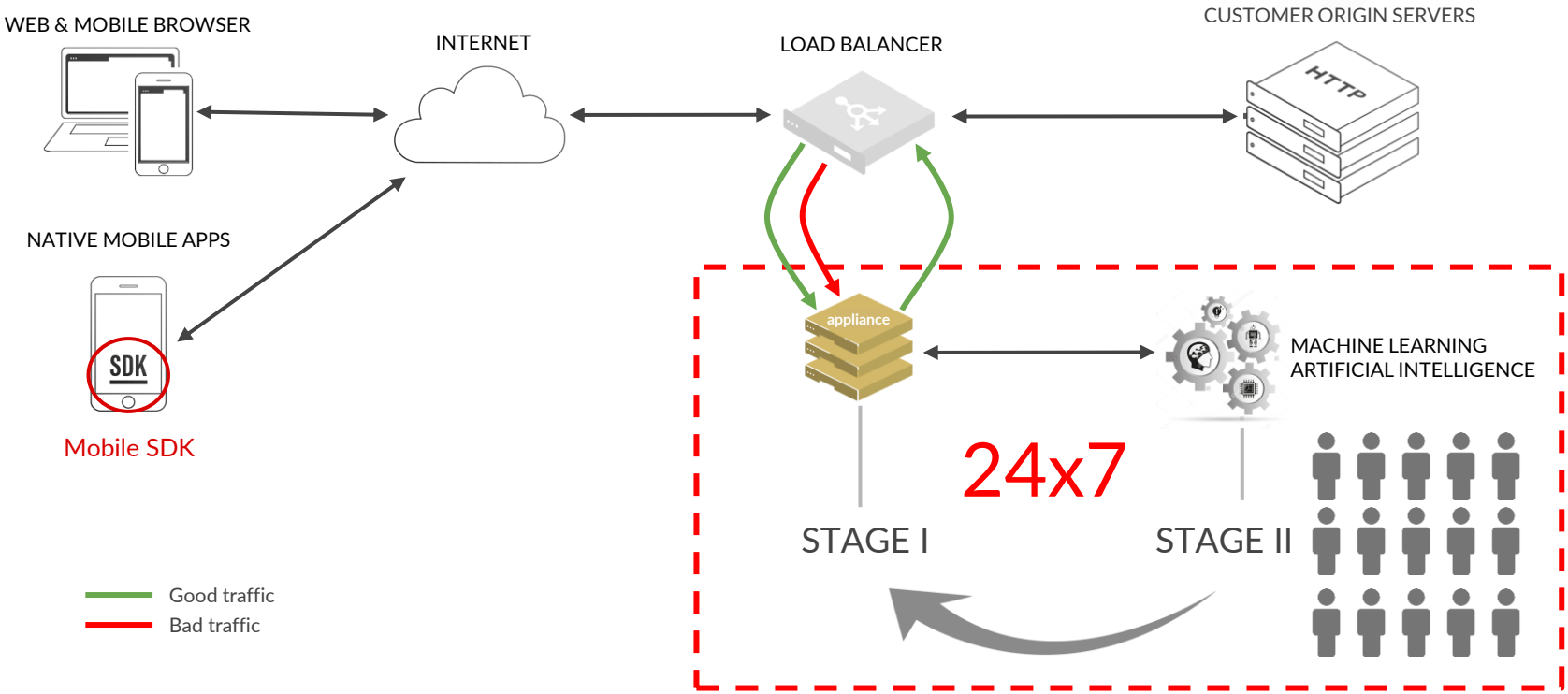
Multi-stage detection is paramount



Multi-stage detection is paramount

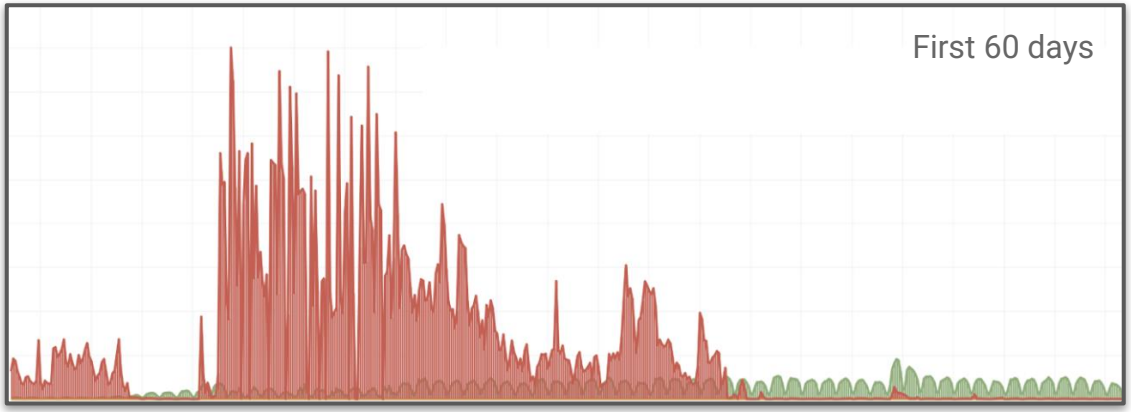


Multi-stage detection is paramount



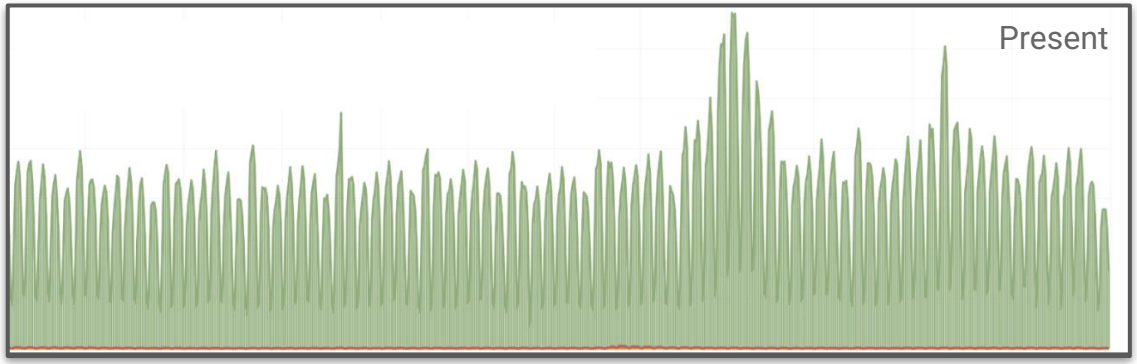
Multi-stage defense enables long-term efficacy

Actual customer journey to less than 1% unwanted traffic



78%

Unwanted

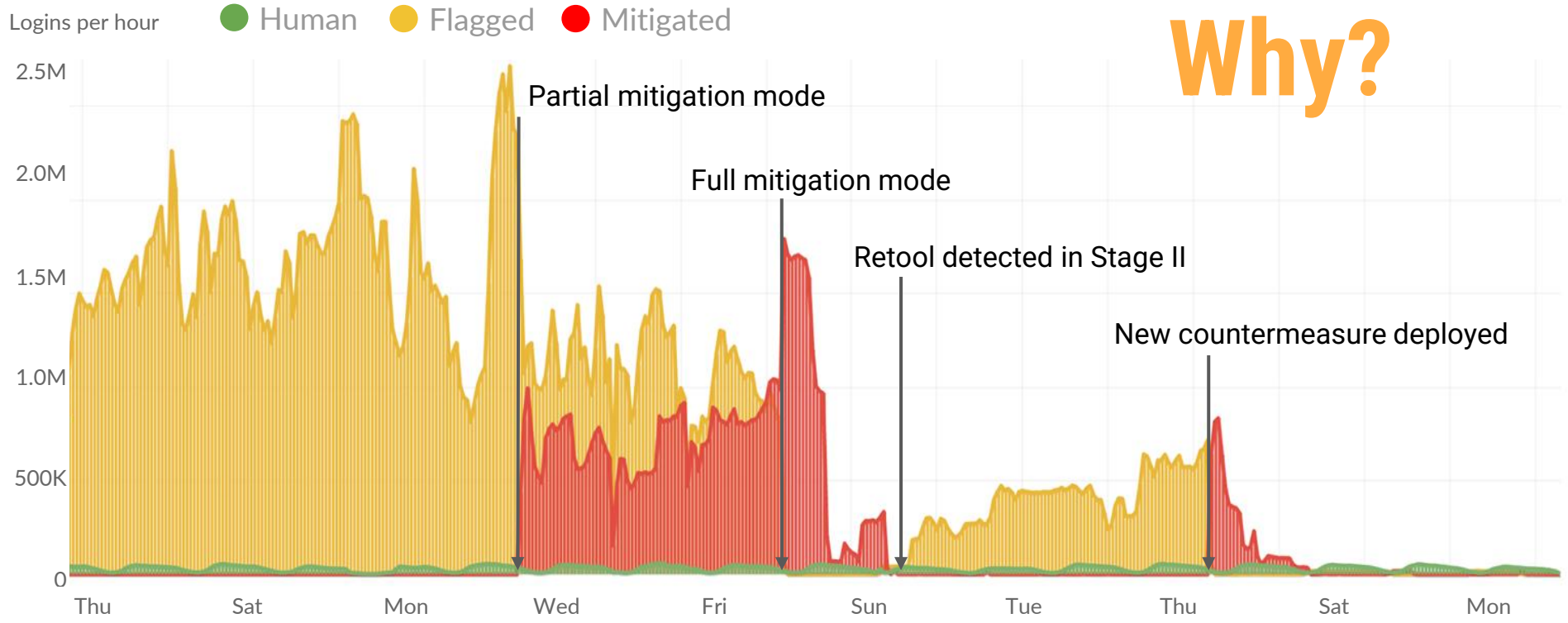


<1%

Unwanted

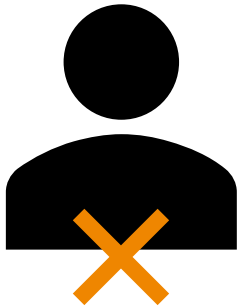
Attempted ATO mitigated using client-side signals

Individual(s) behind the attempted ATO gave up after one retool



Automation against login can verify credentials

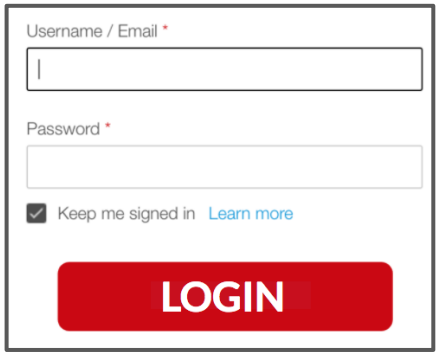
Credential stuffing leads to ATO, fraud, significant financial loss, and brand damage



Fraudster



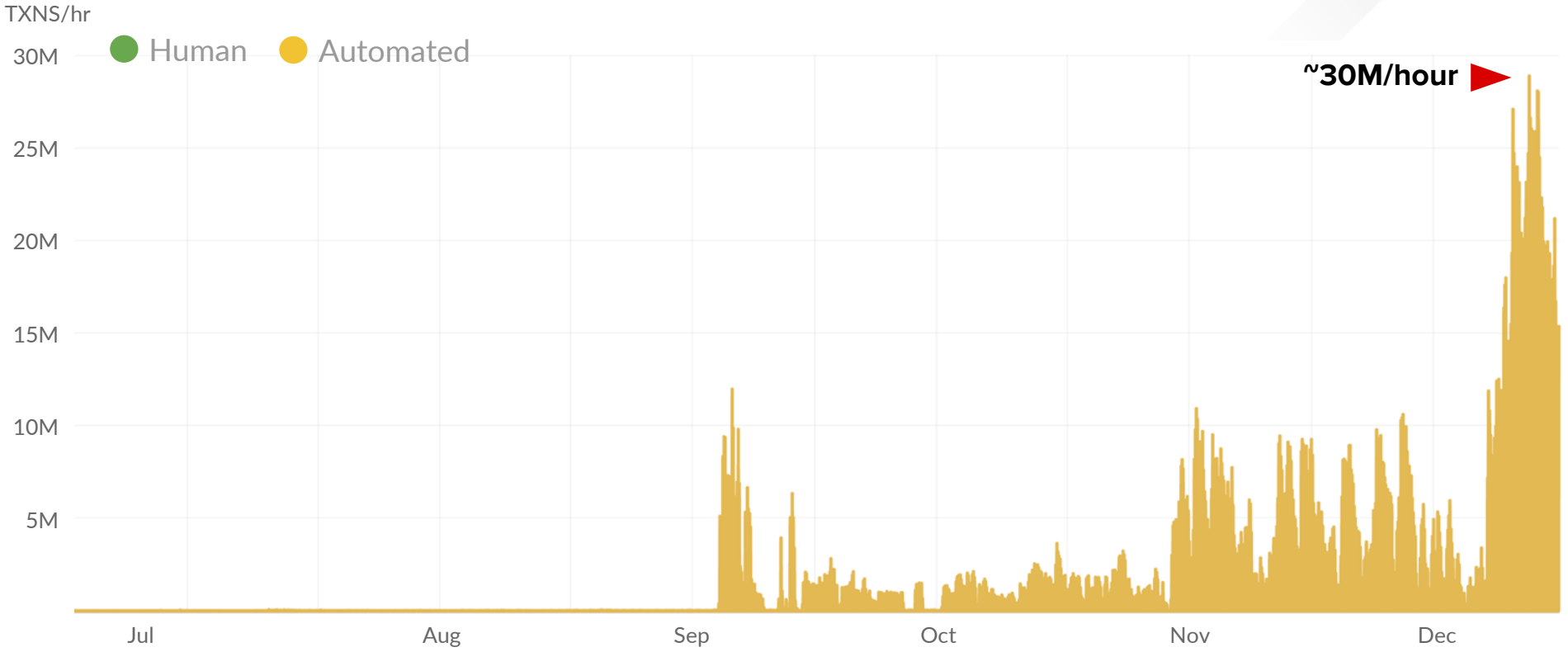
Millions of stolen credentials



0.1% to 3% ATO success rate

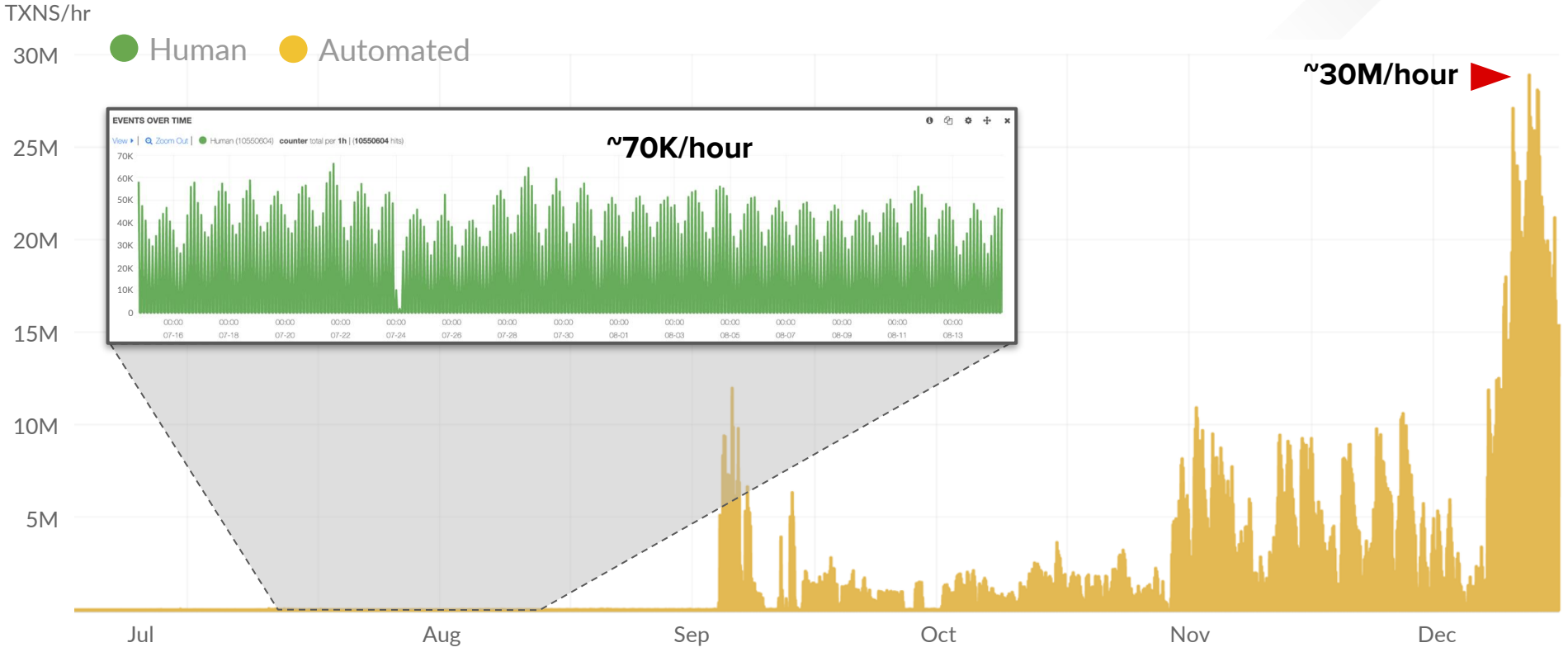
More than 99% of all Create Account traffic was unwanted bots

3.4 billion transactions associated with the creation of fake accounts

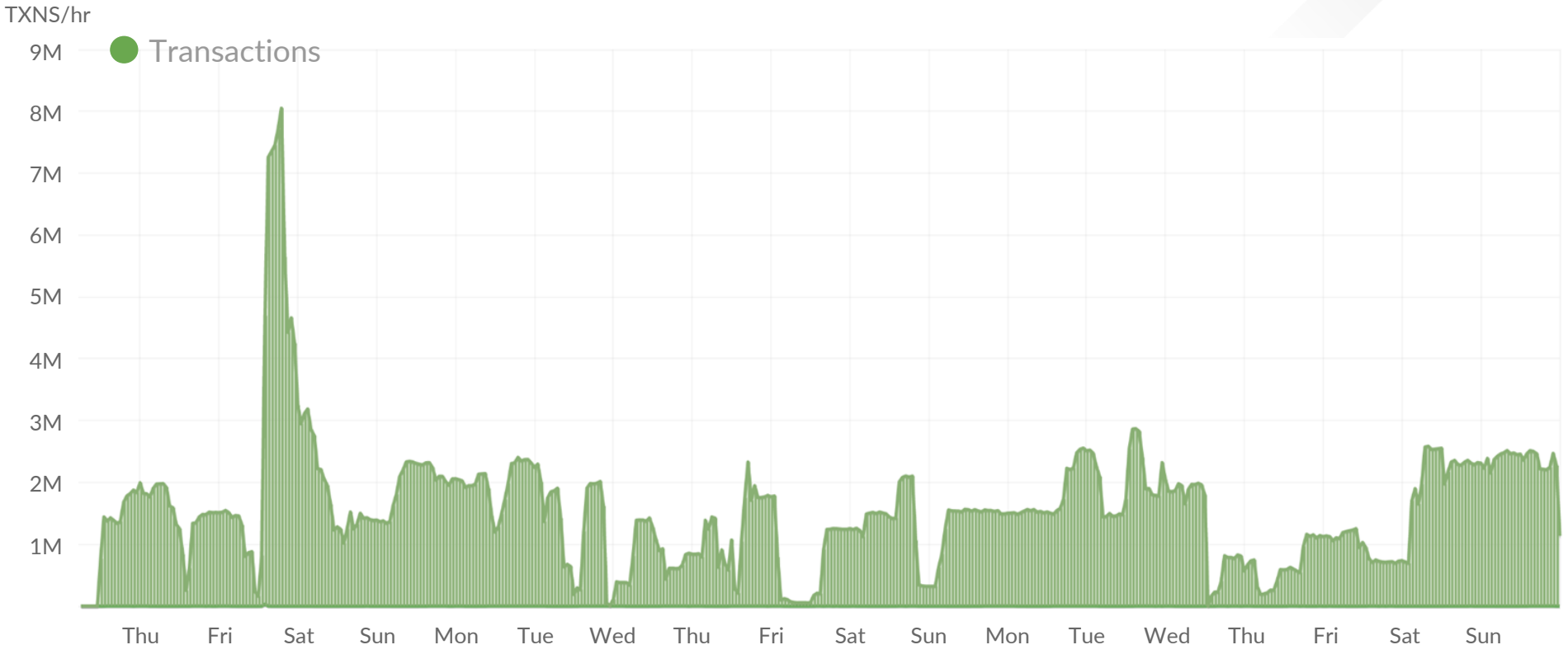


More than 99% of all Create Account traffic was unwanted bots

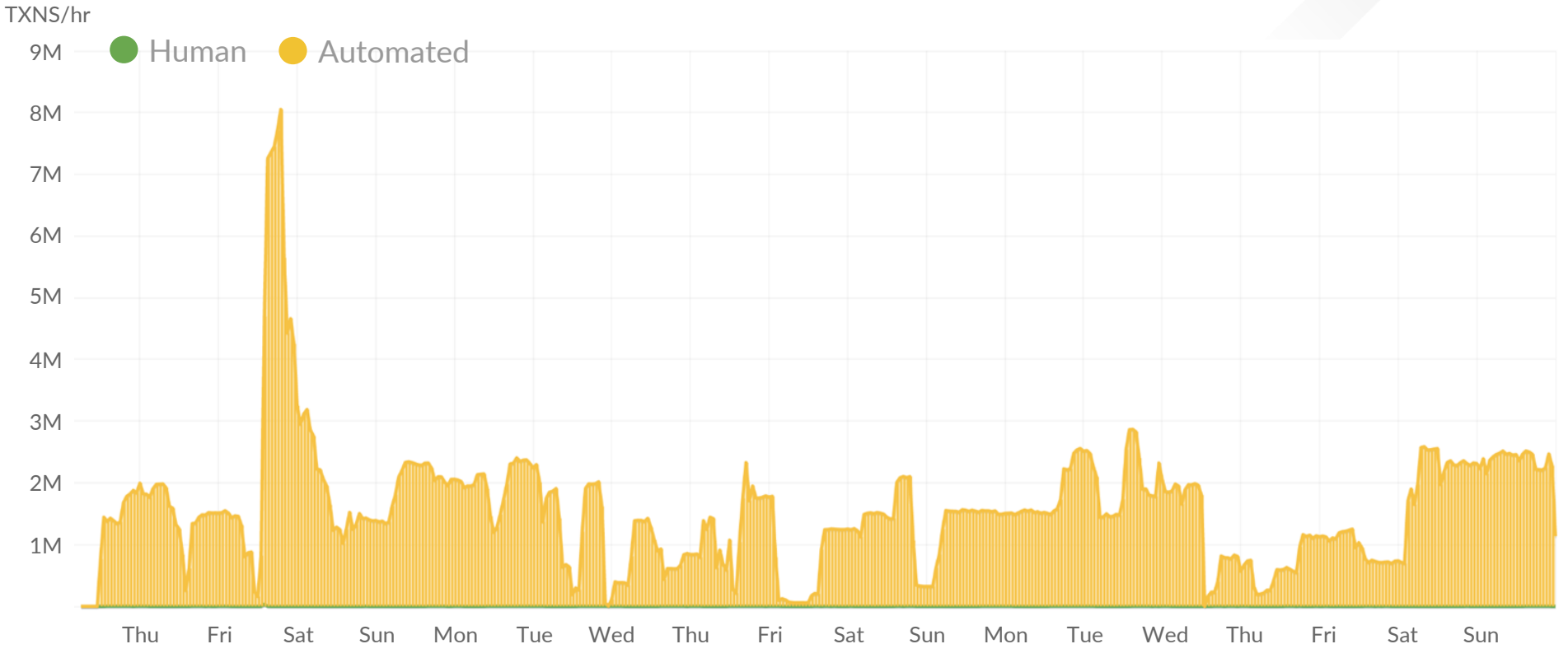
3.4 billion transactions associated with the creation of fake accounts



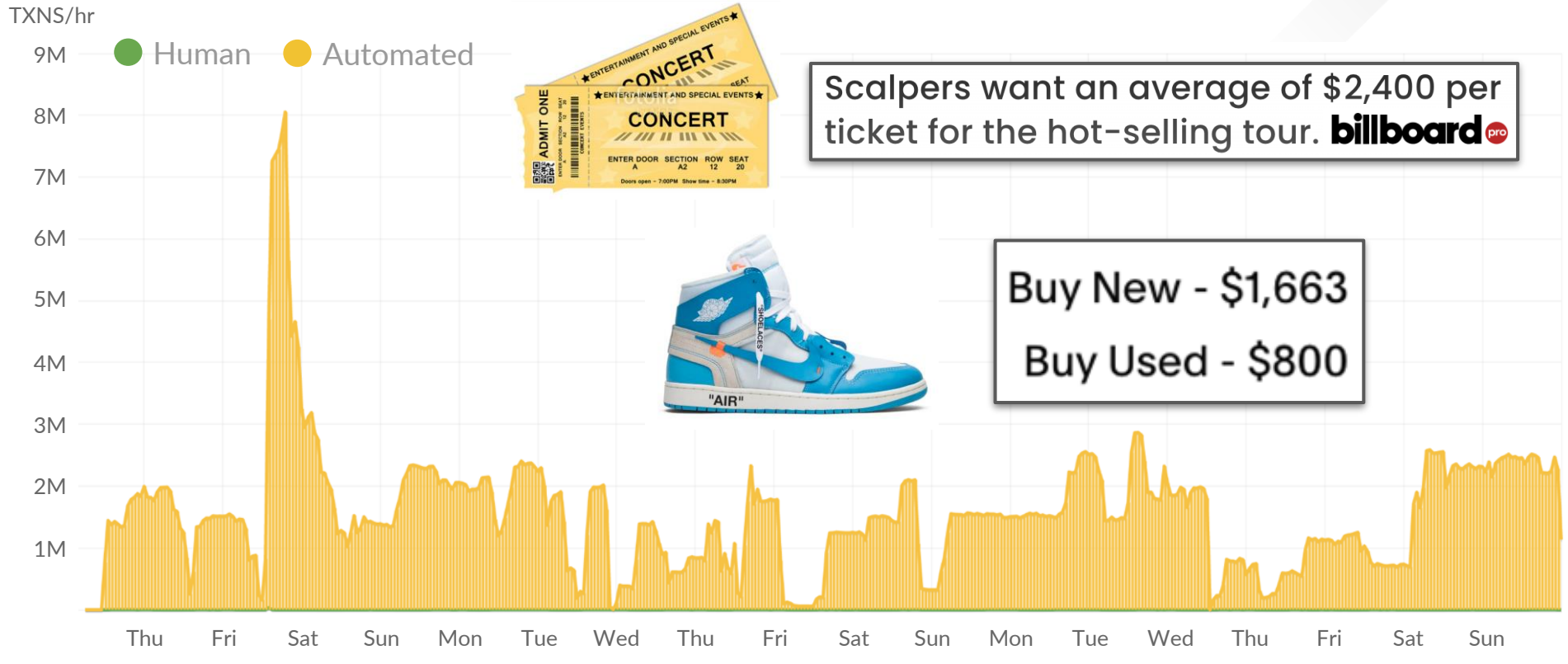
Add-to-Cart traffic at F5 ecommerce customer



More than 99% of all Add-to-Cart traffic was unwanted bots



More than 99% of all Add-to-Cart traffic was unwanted bots

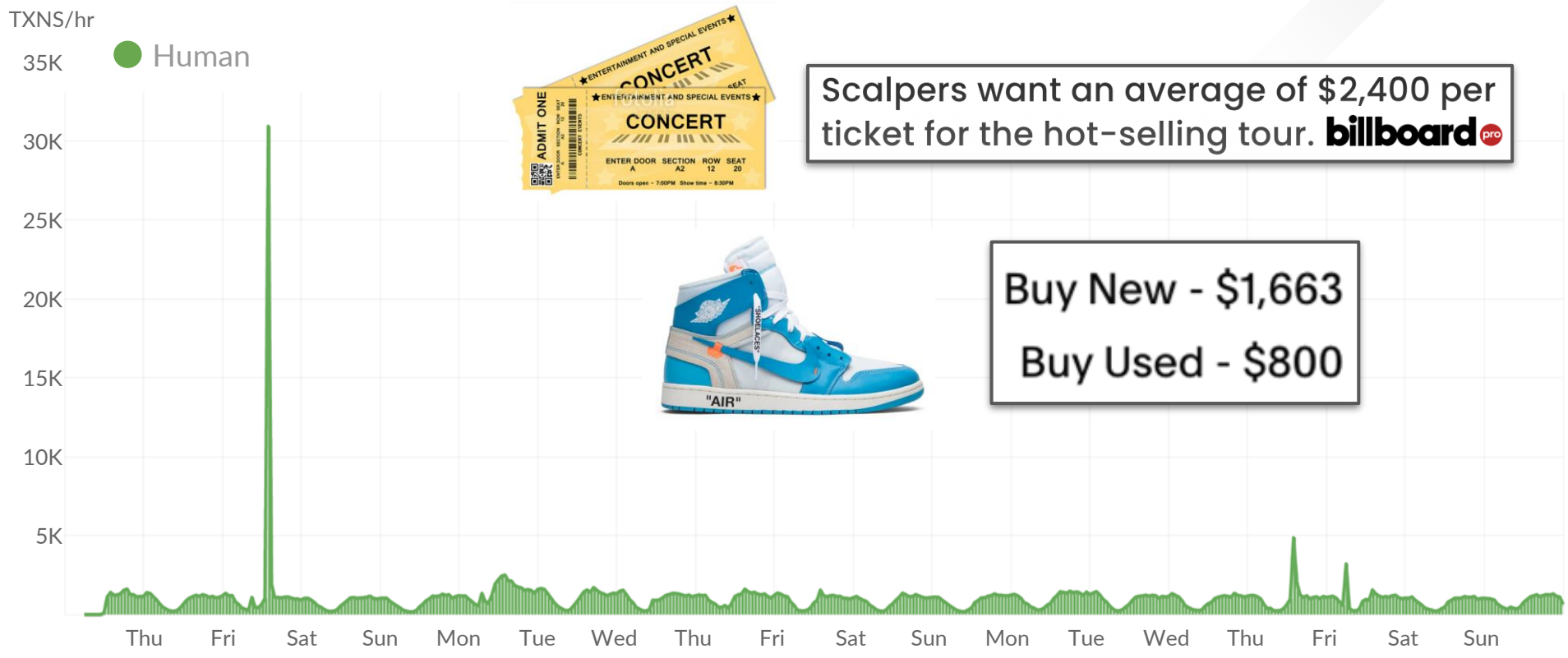


Scalpers want an average of $2,400 per ticket for the hot-selling tour. billboard pro

Buy New - $1,663

Buy Used - $800

Mitigating bot traffic reveals legitimate human traffic

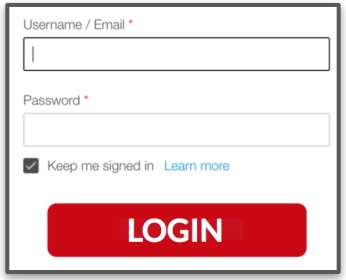


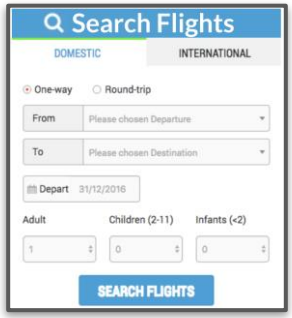
Scalpers want an average of $2,400 per ticket for the hot-selling tour. billboard pro

Buy New - $1,663

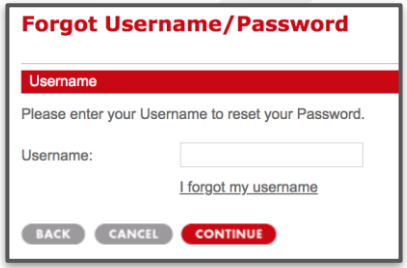
Buy Used - $800

All publicly accessible web & mobile applications targeted

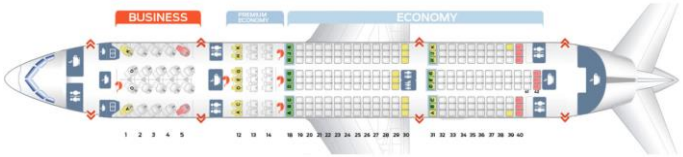


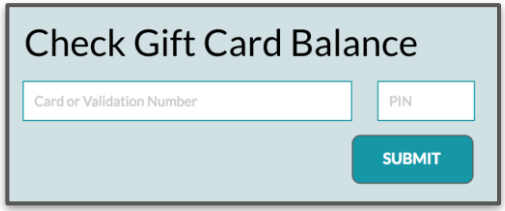


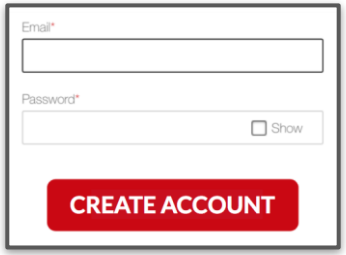


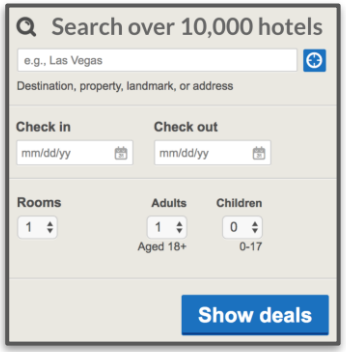














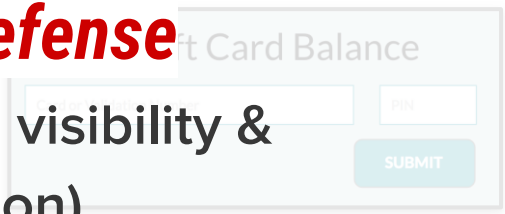


All publicly accessible web & mobile applications targeted

F5 Distributed Cloud ***Bot Defense***

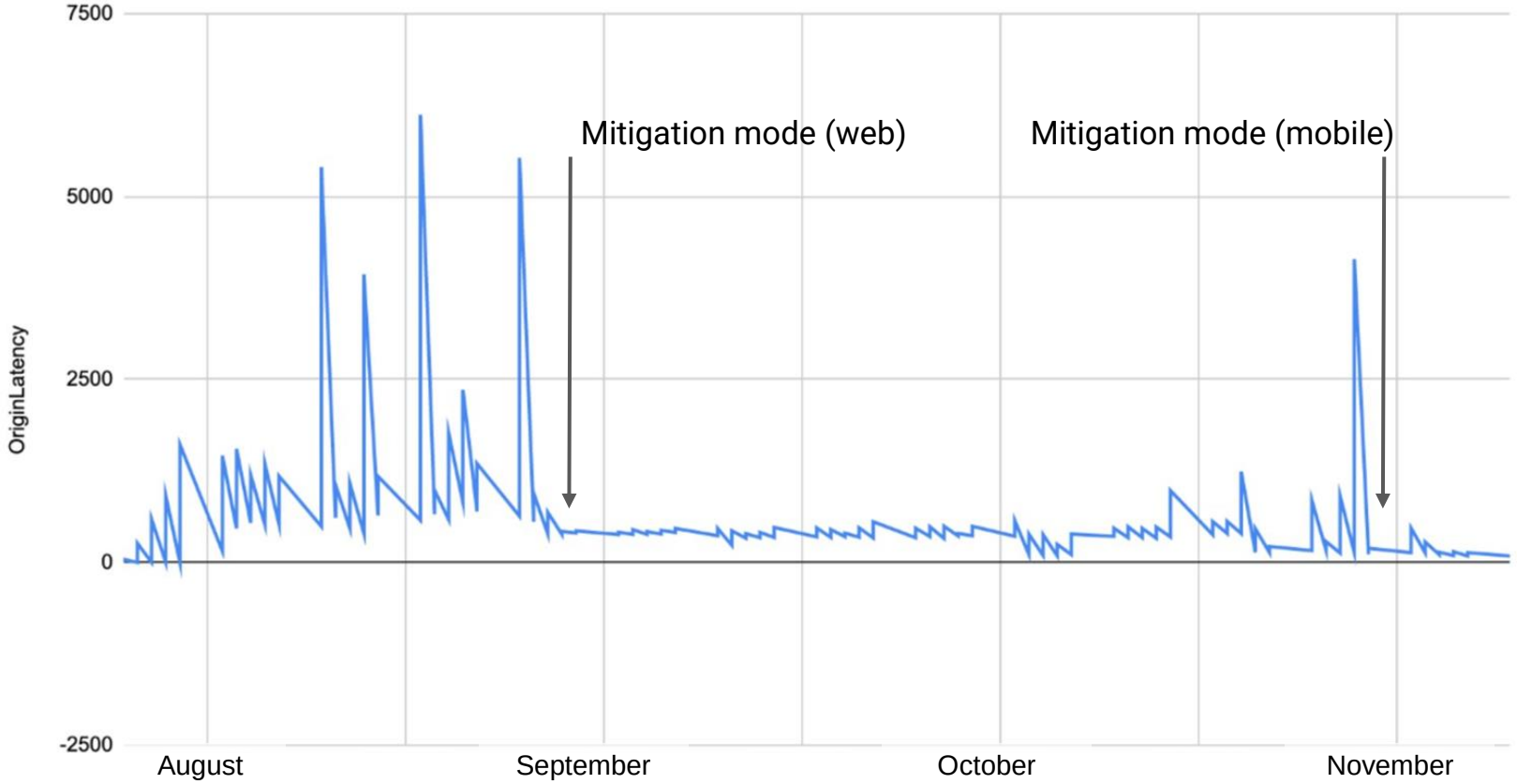
Stops malicious bots (and provides visibility & control over other automation)



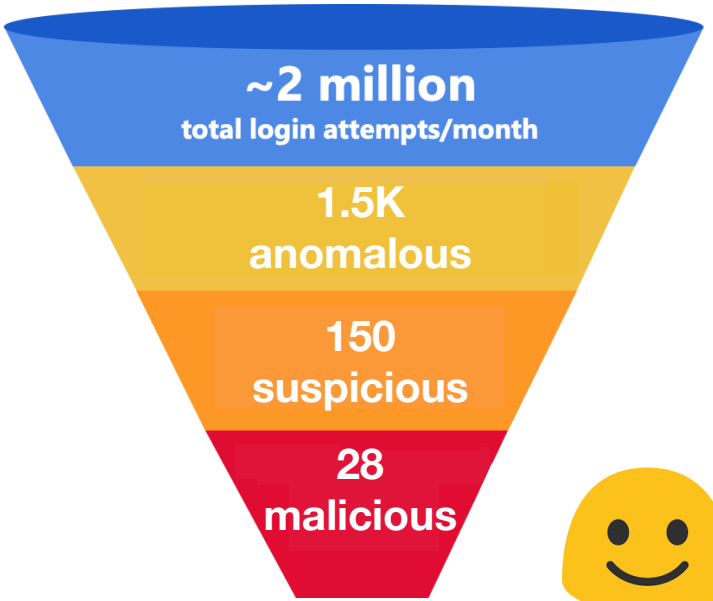


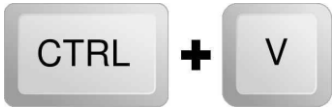
After noise from bots is removed…

Mitigation resulted in a significant decrease in latency



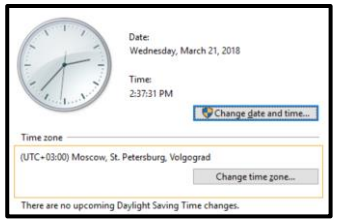
Noise removed, signals can find suspicious *manual* transactions





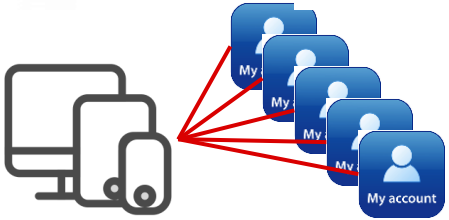








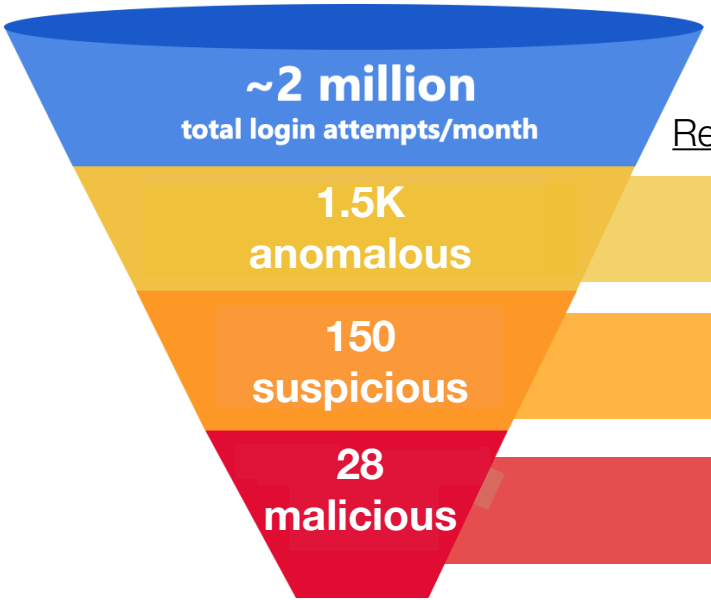






Network intelligence

Noise removed, signals can find suspicious *manual* transactions



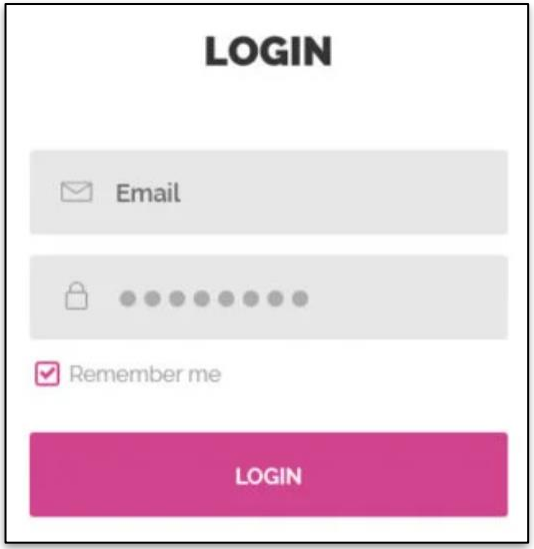
	Recommendation based on signals	Proposed enterprise action
1.5K anomalous	Challenge	Issue MFA challenge
150 suspicious	Review	Fraud team review
28 malicious	Drop	Revoke transaction

F5 Distributed Cloud ***Account Protection***

Identifies human-click farms engaged in unauthorized activity

What else can you do with client-side signals?

Noise removed, signals can find significant *friction*

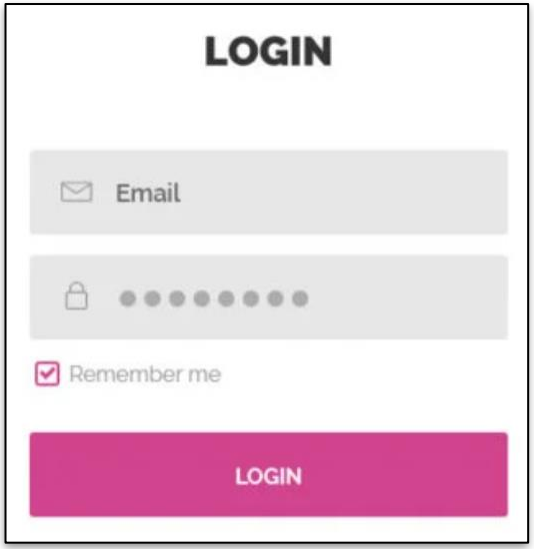


78% → **77.4k**
Login directly on first attempt

14% → **13.9K**
Login after multiple attempts

6% → **5.9K**
Unable to login

Noise removed, signals can find significant *friction*



78% → **77.4k**
Login directly on first attempt

14% → **13.9K**
Login after multiple attempts

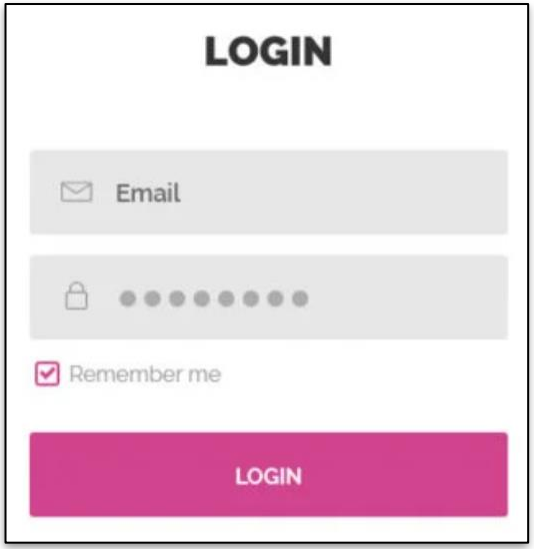
6% → **5.9K**
Unable to login

~5%–15% of those in login distress would dial in

2,000+ calls/day



Noise removed, signals can find significant *friction*



78% → **77.4k**
Login directly on first attempt

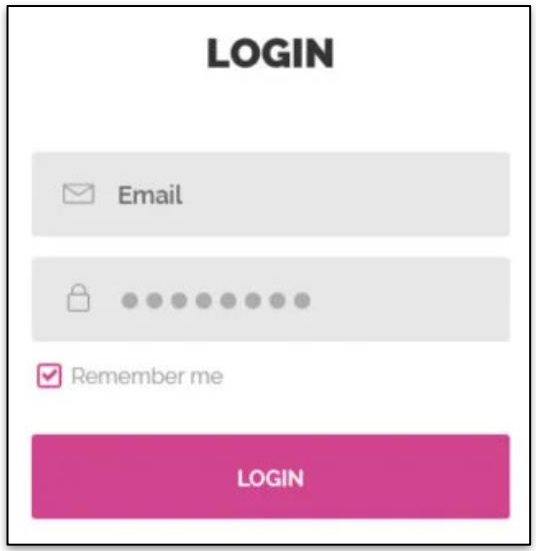
14% → **13.9K**
Login after multiple attempts

6.8k known good users

6% → **5.9K**
Unable to login

1.1k known good users

Noise removed, signals can find significant *friction*



86% 85.3K
Login directly on first attempt

7% 7.1K
Login after multiple attempts

5% 4.8K
Unable to login

Session extension

6.8k known good users

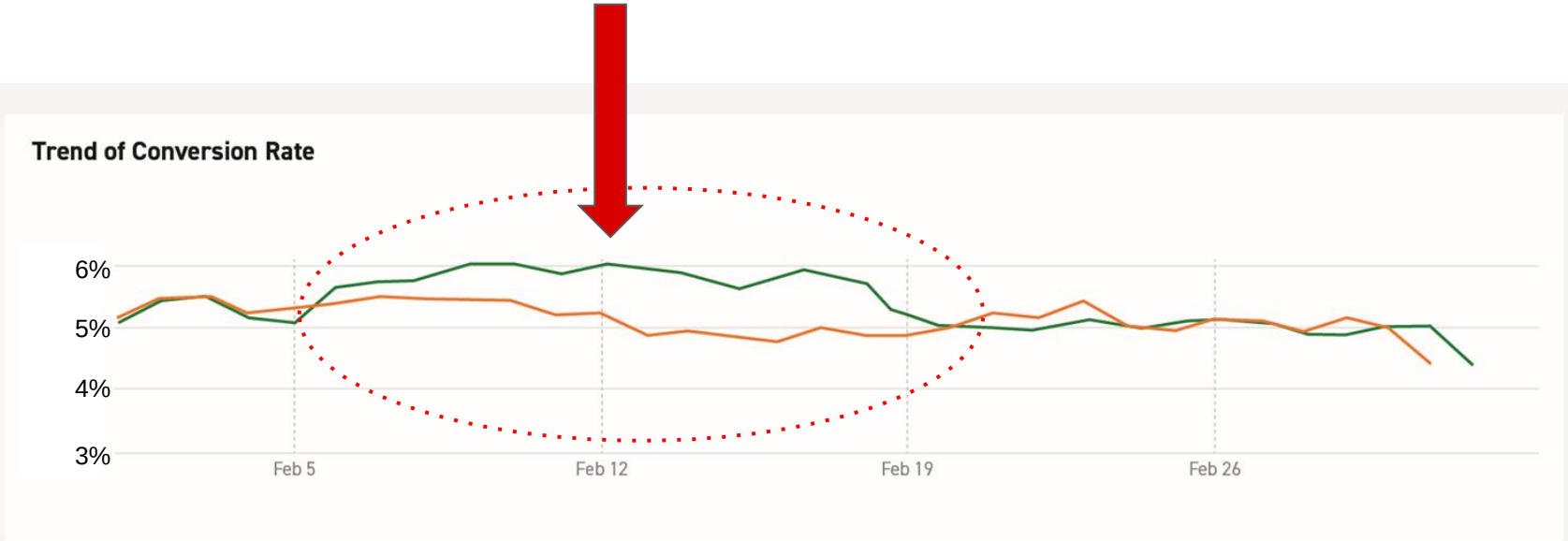
1.1k known good users

F5 Distributed Cloud ***Authentication Intelligence***

Reduces friction using silent and continuous authentication

Value of extending sessions for recognized users

Two-week A/B test showed 17% conversion lift due to 7-day session (vs. default of 30 minutes)



To detect and prevent unauthorized traffic, you must . . .

- Identify web and mobile applications likely to be targeted
- Design applications to remove incentive
- Collect client-side signals
- **Harden** your JS & SDK
- Mitigate in a way bad actors will not immediately notice
- Conduct ongoing retrospective analysis (Stage II)
- Leverage ISACs and other networks
- Break down corporate stovepipes

Stop bad bots
F5 Bot Defense

Stop bad humans
F5 Account Protection

Reduce friction
F5 Authentication Intelligence

d.woods@f5.com

Thank you!

Dan Woods

d.woods@f5.com



Please complete the session survey in the **mobile app**

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.