

BOT MANAGER

Product Overview

Renny Shen

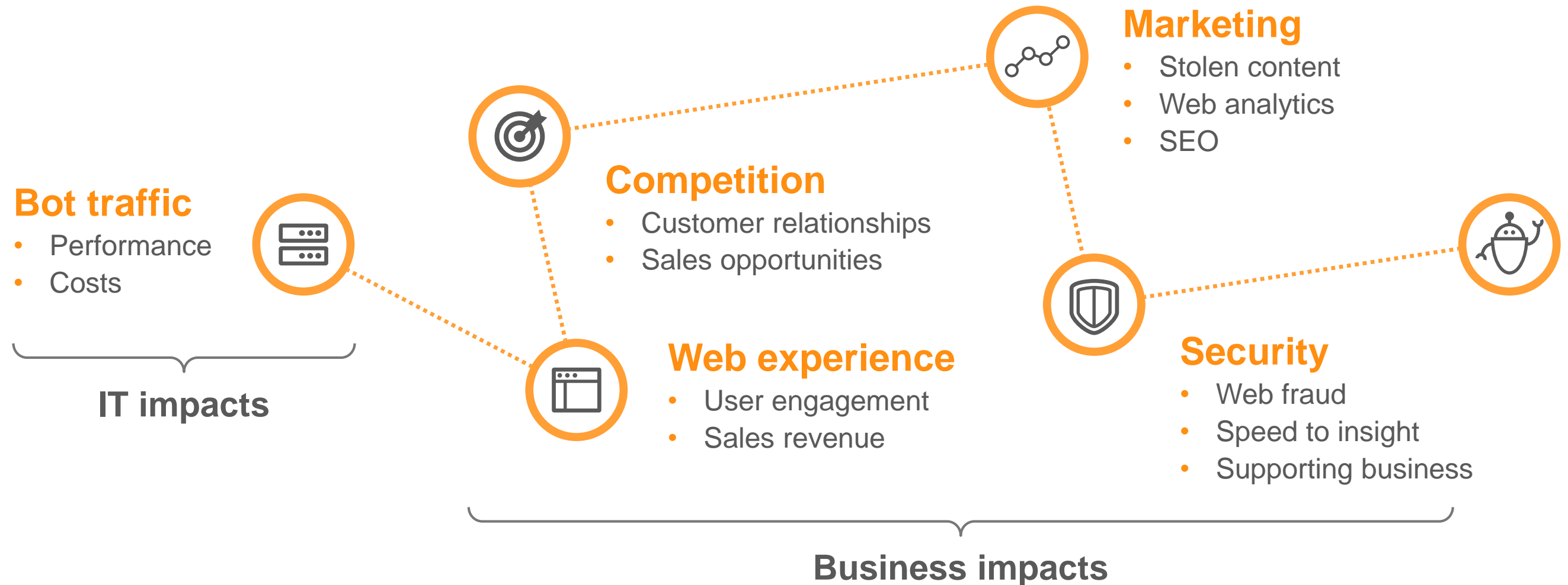
Sr. Product Marketing Manager

What do bots mean to you?

WHAT WE HEARD

What we hear from others

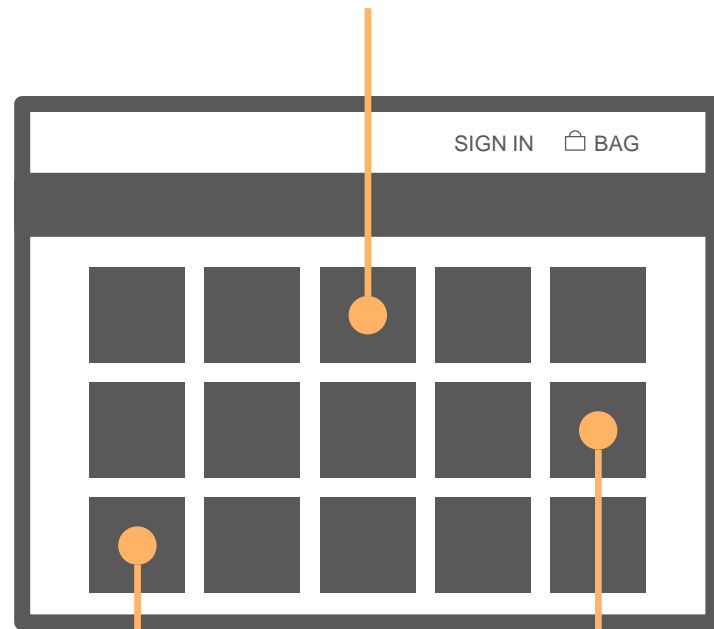
THE BOT PROBLEM



A different way to think about

THE BOT PROBLEM

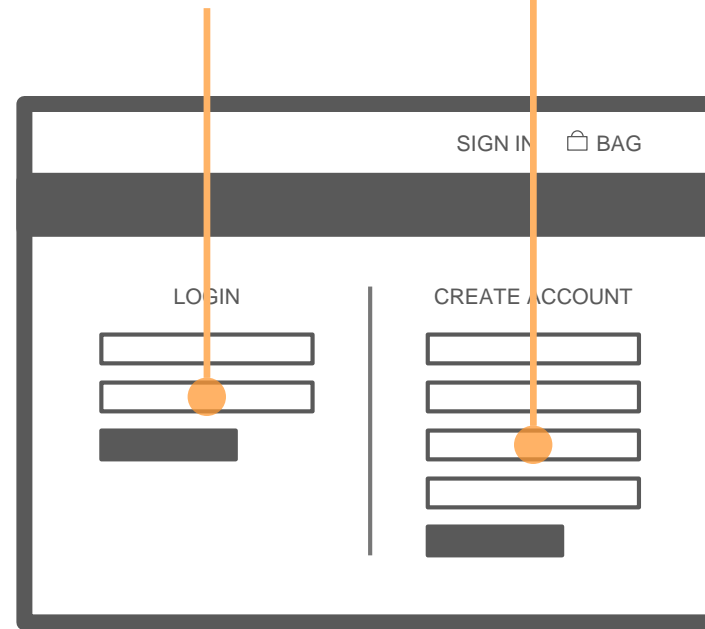
Competitors



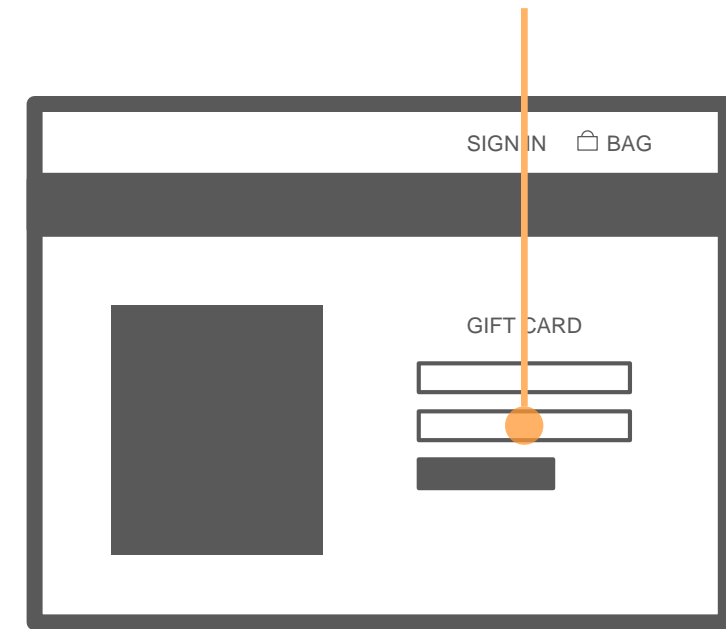
Partners

3rd parties

Fraudsters

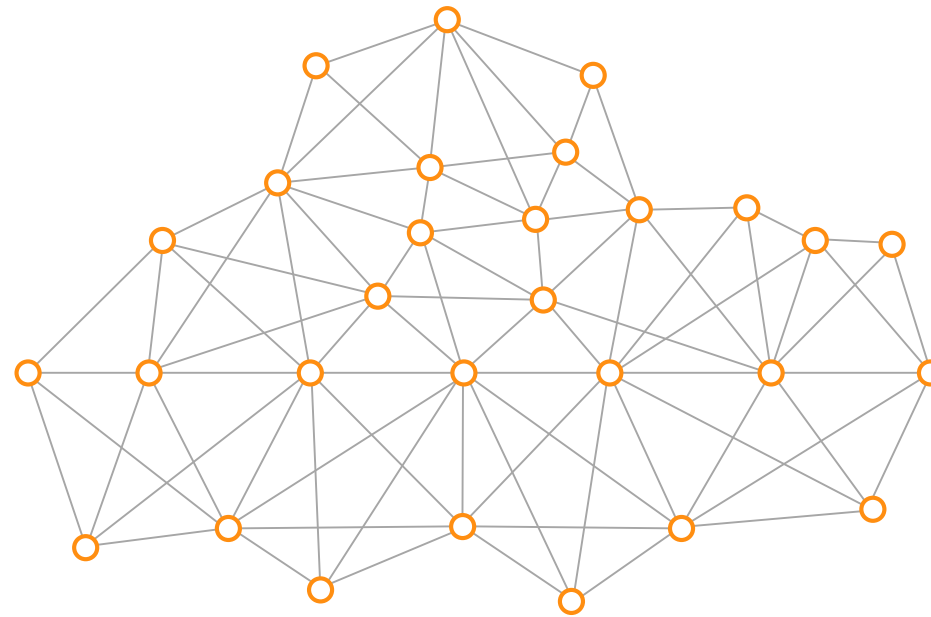


Fraudsters



Bot management requires

A FRAMEWORK



Better manage **BUSINESS and IT IMPACTS** of bots as a cloud-based service

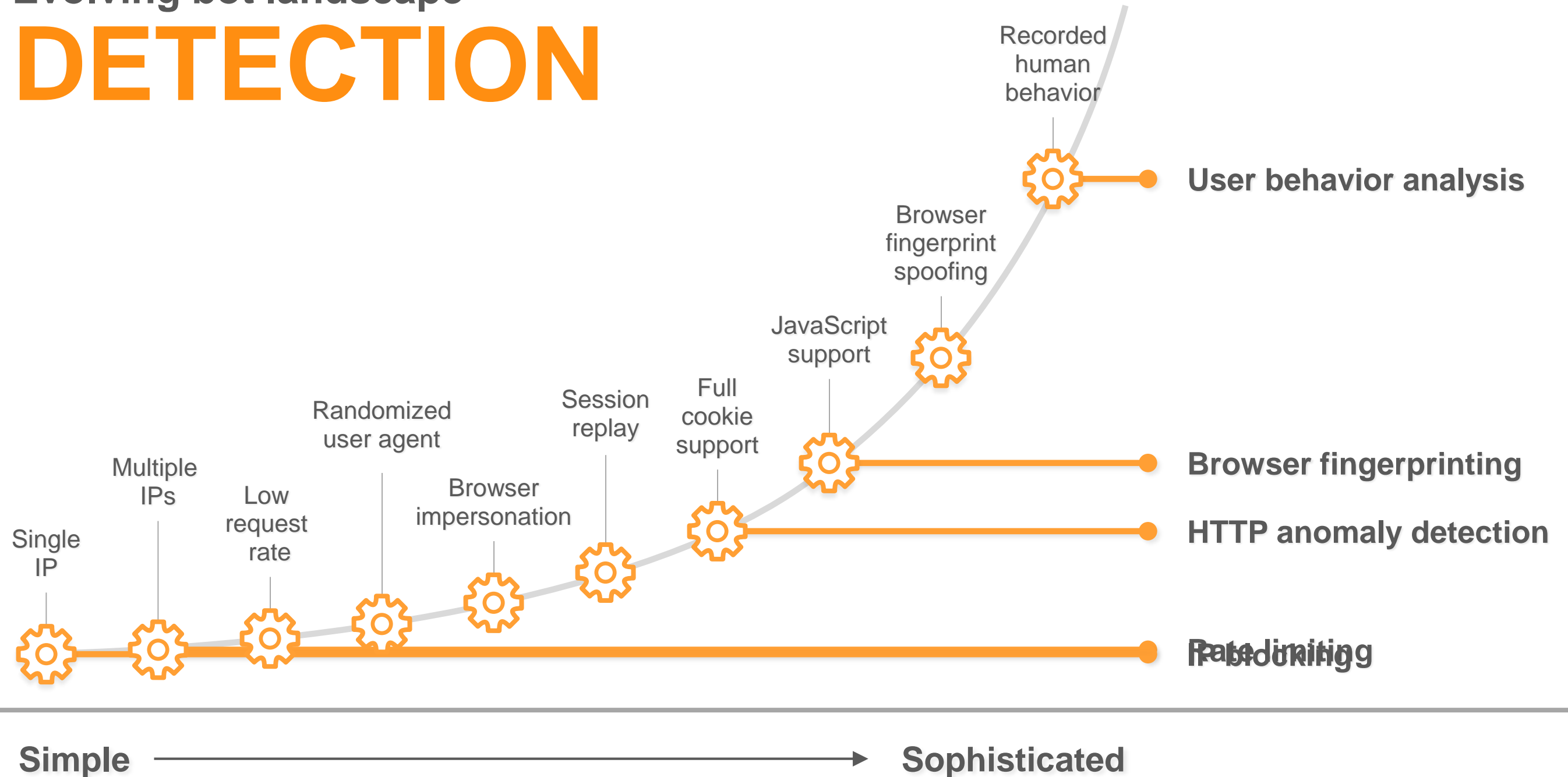
To manage bots

WHAT YOU NEED



Evolving bot landscape

DETECTION



Looking for the easiest way to run multiple accounts?

MultiLoginApp allows you to connect to websites with popular browsers using:

MULTIPLE USER NAMES	✓
DIFFERENT PROXIES	✓
AND HAVING UNIQUE FOOTPRINTS	✓

0:29 / 1:30

YouTube

 [DOWNLOAD MULTILOGINAPP FOR FREE](#)

Multiloginapp

vs.

MultiFox

Multiloginapp

vs.

FraudFox

Multiloginapp

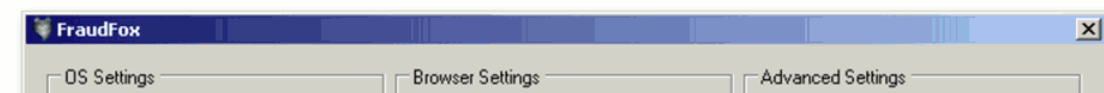
vs.

Antidetect

Multiloginapp vs. FraudFox

FraudFox is advertised on Evolution as a way to spoof browser fingerprints and commit fraud. Multiloginapp also allows you to spoof browser fingerprints, but the intended usage is to control multiple online accounts, and not to hijack the fingerprint of an individual user. If you are looking at FraudFox for its spoofing capabilities, you may want to consider Multiloginapp instead. Continue on to learn about the similarities and differences between the two.

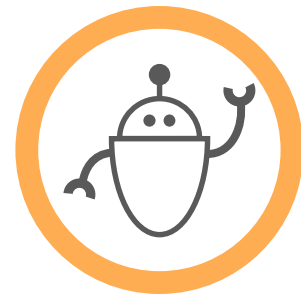
Capabilities



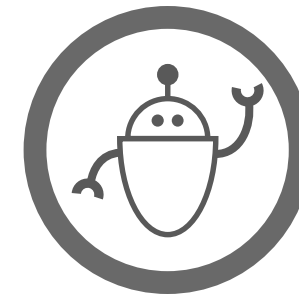
Bots defy easy

CATEGORIZATION

Most solutions approach the bot problem as a **SECURITY** problem



Good bot
(Whitelist)

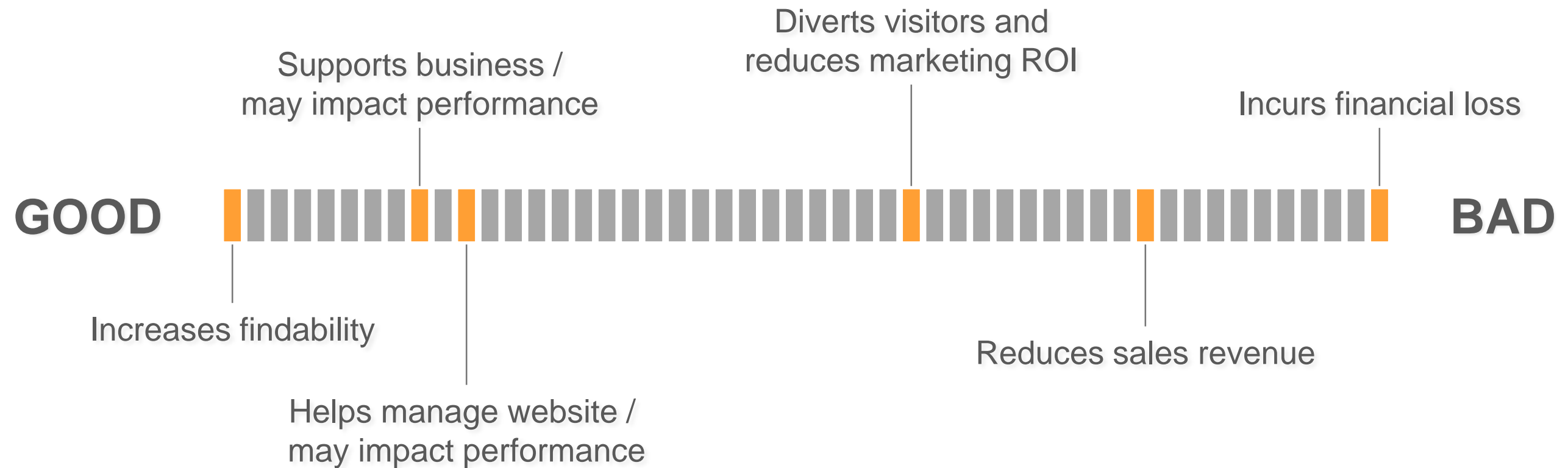


Bad bot
(Block)

Bots defy easy

CATEGORIZATION


A more flexible approach manages bots based on their **IMPACT** on you







Consumers

Round-trip One-way Multi-city

 FROM

 TO

 DEPART

 RETURN

 1 ADULT

Latest flight deals from Cambridge

Santa Clara
Premium economy round-trip from
\$500*

London
Premium economy round-trip from
\$1,000*

Singapore
Premium economy round-trip from
\$2,000*

How other organizations implemented **MANAGEMENT**



Login / credential abuse

Serve incorrect username/password to fraudsters



Online media

Prevent content aggregators f/diverting visitors



Retailer

Serve fake prices to control price scraping



Event ticketing / hype sales

Serve cached availability to 3rd-parties using bots



Financial services

Manage performance impact of aggregators



Performance

Serve alternate origin to improve performance



Airline

Serve cached content to reduce GDS costs



Partners

Slow bot traffic f/partners during business hours

U.S. News and World Report

CASE STUDY

AKAMAI CASE STUDY

U.S. News & World Report Protects its Online Intellectual Property and Reduces IT Overhead with Akamai Bot Manager

By ensuring we are the authoritative source of our data, we are funneling more of the organic search traffic into our website where we can monetize those views.
— Matt Kupferman, Senior Director of Engineering, U.S. News & World Report

The Situation
Founded in 1933, U.S. News & World Report is a multi-platform publisher of news and information, which includes www.usnews.com and annual print and e-book versions of its authoritative rankings of Best Colleges, Best Graduate Schools and Best Hospitals. In 2012, U.S. News launched a conference division focusing on important national conversations and solutions in STEM Education and Healthcare of Tomorrow. U.S. News has earned a reputation as the leading provider of service news and information that improves the quality of life of its readers by focusing on health, personal finance, education, travel, cars, news and opinion. U.S. News & World Report's signature franchises include its Consumer Advice and "Best" series of consumer guides that include rankings of colleges, graduate schools, high schools, hospitals, nursing homes, mutual funds, health plans, diets and more.

The Challenge
As a digital-centric media organization, U.S. News & World Report relies on its unique and compelling content to attract visitors to its website. It currently reaches more than 30 million decision makers every month, with 160 million page views representing a 20 percent year-over-year (YoY) increase. U.S. News monetizes this content by selling advertisements and sponsorship opportunities to businesses seeking to reach its audience of educated professionals, business leaders and policy makers.

U.S. News' intellectual property includes highly anticipated rankings in an increasing number of areas. For U.S. News, having this content freely available online makes it easier for its audience to find and helps improve its organic search rankings. However, it also makes it easier for unaffiliated third-parties to scrape and repurpose that same content on their sites using automated bots. This diverts visitors and can potentially impact advertising revenue. According to Matt Kupferman, Senior Director of Engineering, "U.S. News & World Report has actually seen independent parties taking our data, publishing it themselves and appearing higher in the search rankings."

The Goals
U.S. News & World Report needed to meet several requirements to support its business objectives:

- **Revenue protection.** U.S. News wanted to detect and prevent third parties from scraping its website and repurposing its rankings data elsewhere.
- **Reduced overhead with greater bot visibility.** Without a solution in place, U.S. News had to manually sift through and analyze logs to identify and block bots that were scraping its site.
- **Performance at scale.** With 20% YoY growth, U.S. News wanted to ensure that the origin load did not compromise performance for legitimate users.
- **Comprehensive bot management.** U.S. News wanted granular visibility into bot traffic to better understand who was coming to its site and drive its bot management strategy.

COMPANY
U.S. News & World Report
Washington, D.C.
www.usnews.com

INDUSTRY
Media

SOLUTIONS
• Akamai Bot Manager

KEY IMPACTS
• Protects digital advertising revenue by preventing web scraping
• Enables acquisition of more sensitive data to enhance the value of their health care rankings
• Ensures visibility and simple management of bots
• Reduces management overhead by 25% with integrated, turnkey solution
• Scales to support substantial YoY growth by offloading origin infrastructure by at least 20%



- **Challenge**

- 3rd-parties scraping and repurposing rankings content from www.usnews.com, diverting potential visitors to 3rd-party sites and impacting ad revenue

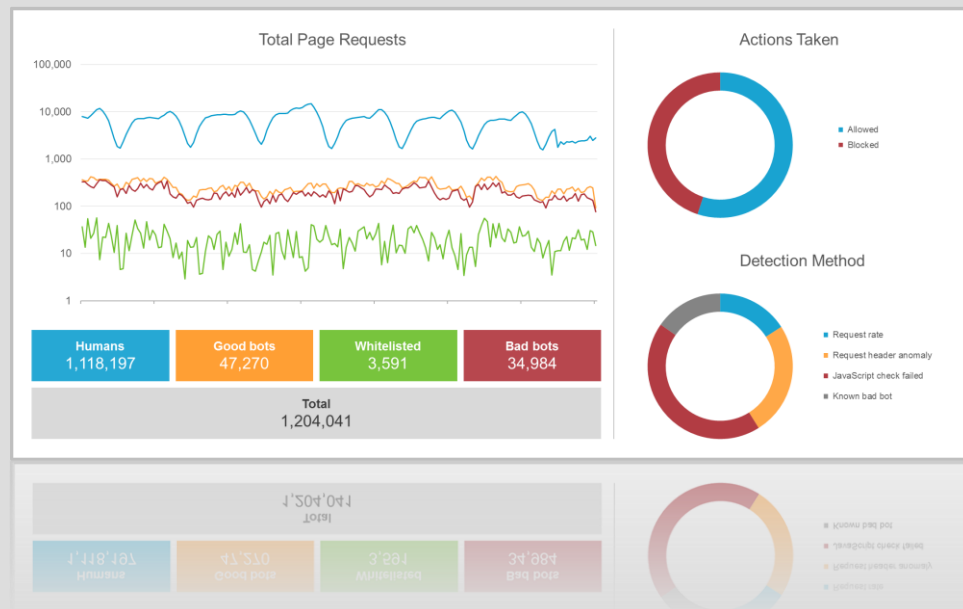
- **Benefits**

- Prevent scraping to protect digital advertising revenue
- Gain visibility into bot traffic and reduce overhead
- Manage bots without sacrificing caching or requiring infrastructure changes

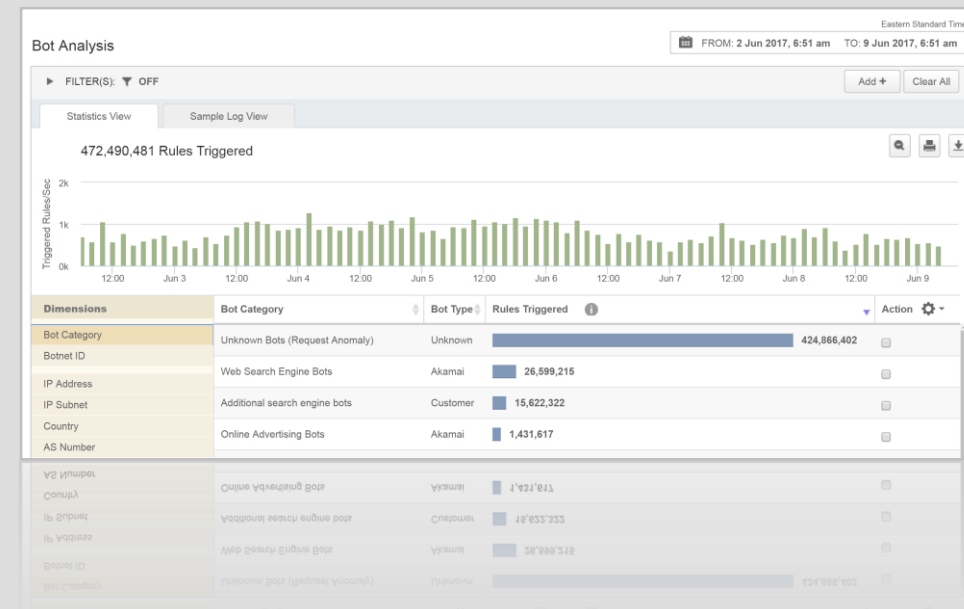
How to think about **VISIBILITY**

Visibility needs to support your **STRATEGY**

Example 1:



Example 2:



How to think about

VISIBILITY

Black box

- Easy to configure
- Reports actions taken but no ability to verify

High-level statistics

- Good for identifying infrastructure and network requirements
- Responding to security events or implementing strategy requires greater granularity



Statistics View

Sample Log View



500 Events

 This is not all the requests but a sampling of the requests



Time	Botnet ID	IP Address	Hostname	URL Path	# of Req Header
------	-----------	------------	----------	----------	-----------------

2017-06-05, 05:00:28 PM	Bot_1420AA6A848595F7C61E27B2FAE7FDF0	104.239.230.42			6
-------------------------	--------------------------------------	----------------	--	--	---

  Client Information

Botnet ID:	Bot_1420AA6A848595F7C61E27B2FAE7FDF0
Client IP:	104.239.230.42
Country:	US
Region:	VA
City:	HERNDON
ASNUM:	27357
Company Name:	Cloud_Servers_Cell_0001-0003_IAD3
Domain Name:	lakeridgewinery.com

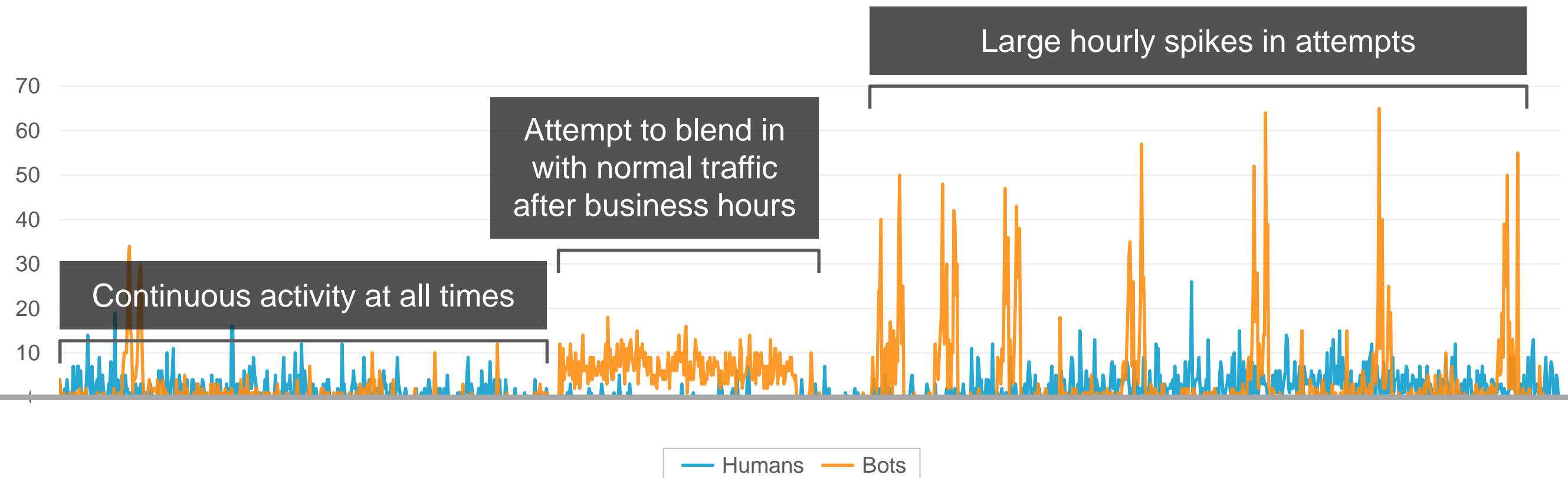
 Request Information

Protocol:	HTTP/1.1
HTTP Method:	GET
HTTP Version:	1.1
Referer:	http://www.gutenberg.org/cache/epub/24602/24602-h/images/cover.html
Host:	www.gutenberg.org
Path:	/images/cover.html
Query:	24602-h/images/cover.html

Online retailer

CASE STUDY

Challenge: fraud-related losses from bots checking gift card balances



Achieving desired outcomes

AKAMAI DIFFERENCE



The latest technologies that can **detect the most sophisticated bots** today even as they evolve to avoid detection



Real-time intelligence from visibility into bot traffic interacting with many of the largest web presences around the world



Ability to manage wide array of both good and bad bots and **customize response based on your business and IT goals**



Ability to **manage bot traffic on the Akamai CDN** before it reaches your website, offloading your origin infrastructure



Granular visibility / reporting allows you to analyze your bot traffic and implement your bot strategy without being a black box



Security experts who can help implement and tune your bot management strategy and respond to security events



THANK YOU

Introducing **READINESS AND RESPONSE SERVICE**

Designed for organizations that want guidance on their bot strategy, to close security operation gaps, and have peace of mind they're covered to efficiently manage incidents and focus on their business.

Named Akamai Solution Expert

Seasoned practitioners with deep visibility and threat landscape knowledge



Advisory Services

Strategic recommendations based on in-depth reviews of your bot traffic and configurations



Implementation Services

Resources to implement configuration changes regularly



Security Event Management

Prioritized SOC support and mitigation for security events



SERVICE ENTITLEMENTS

Advisory Services

Security Service Review

3x/year included

Implementation Services

Non-emergency configuration assistance (9-5 M-F)

24 hours/quarter

Named Akamai Solution Expert

Named expert with knowledge of the threat landscape and your security and business challenges

Included

Security Event Management

Emergency response line (24x365)

Included for observed bot related security events

Emergency configuration assistance (24x365)

Included for observed bot related security events

Security event recap

Included, sent via e-mail after observed bot related security events

CATEGORY

- Women >
- Men >
- Kids >

- Clothing
- Shoes
- Sport & Swimwear
- Accessories

Clothing > 2,000 products

"shoes" X Blue X Suede X

Popular

DEPARTMENT

- Women
- Boys
- Men
- Girls
- Kids
- Baby

Plus Size

BRAND

- Tommy Hilfiger
- Nike
- Clarks
- adidas
- Converse
- Asics
- Geox
- Diesel
- Jack & Jones
- Fila
- More

PRICE

£ 0 £ 2650

SIZE

- 4.5
- 5
- 5.5
- 6
- 6.5
- 7
- 7.5
- 8
- 8.5
- 9
- More

SALE

- > 20% discount



£85.00 Tommy Hilfiger Suede Espadrille S...



£400.00 santoni Suede Pe...



£101.00 New Balance 996 SUEDE & MES...



Sale Alert Share Save

Bottega Veneta Intrecciato Suede Slippers

Housed in a restored 19th century villa, Bottega Veneta 's Montebello Vicentino atelier is comprised of over 100 expert artisans. These slippers are hand-woven from butter-soft petrol suede in the label's signature intrecciato design. They're lined with leather for the utmost comfort. Shown here with Valentino shirt, Jil Sander T-shirt, Valentino trousers. This item is large to size; see Size &...

MR PORTER £520.00

Go to Mr. Porter

Available sizes

- eu40
- eu41
- eu41.5
- eu42
- eu42.5
- eu43
- eu43.5
- eu44
- eu45

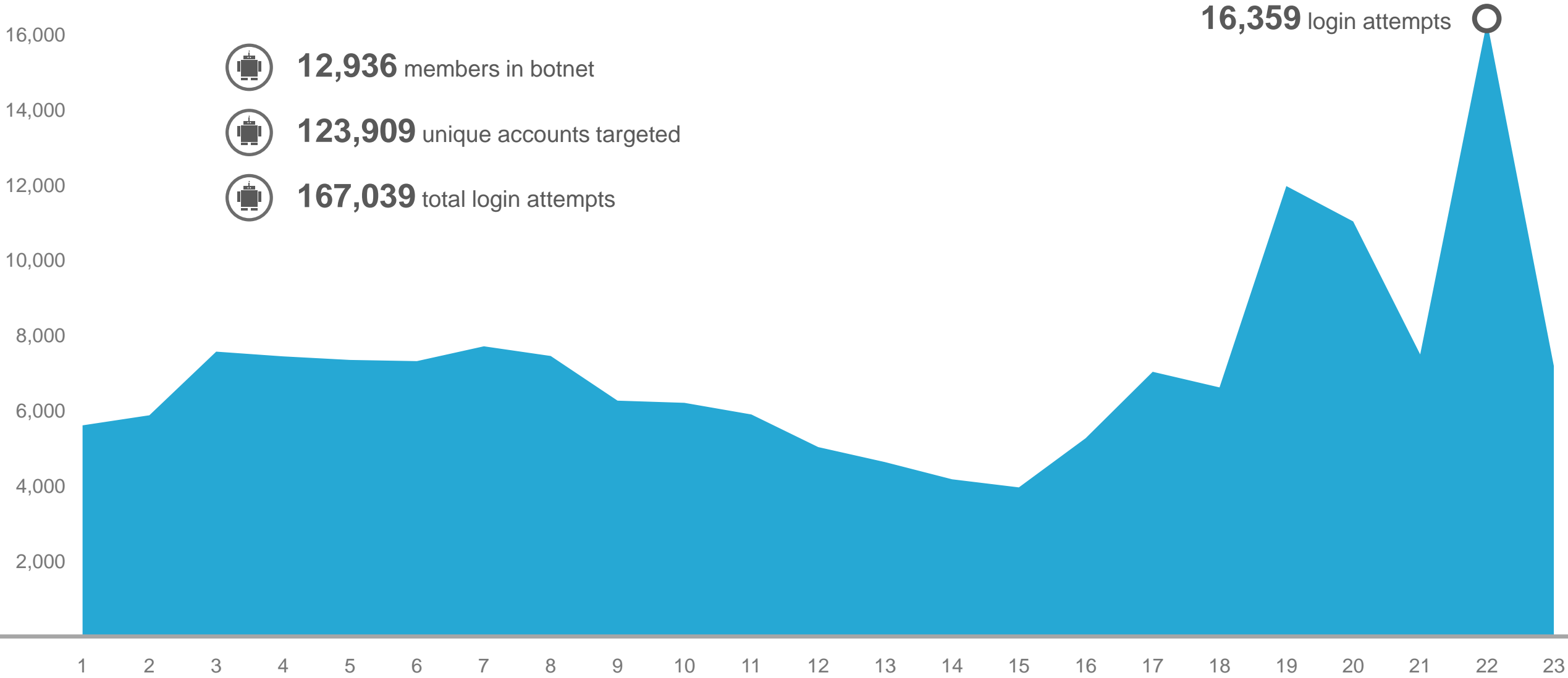
Colours	Blue
Material	Leather • Rubber • Suede
Payment methods	Credit Card • PayPal
Delivery time	Within 2 working days
Delivery charges	£5.00. same day delivery available for some parts of the UK




Fashiola.co.uk > Men > Shoes > Slippers



- Moto Suede, Nylo...
- Intrecciato Suede ...
- Denim, Suede And...
- + Missoni All Star ...
- Suede Loafers
- James Leather Pen...
- Onitsuka Tiger MEXICO 66 LEATH...

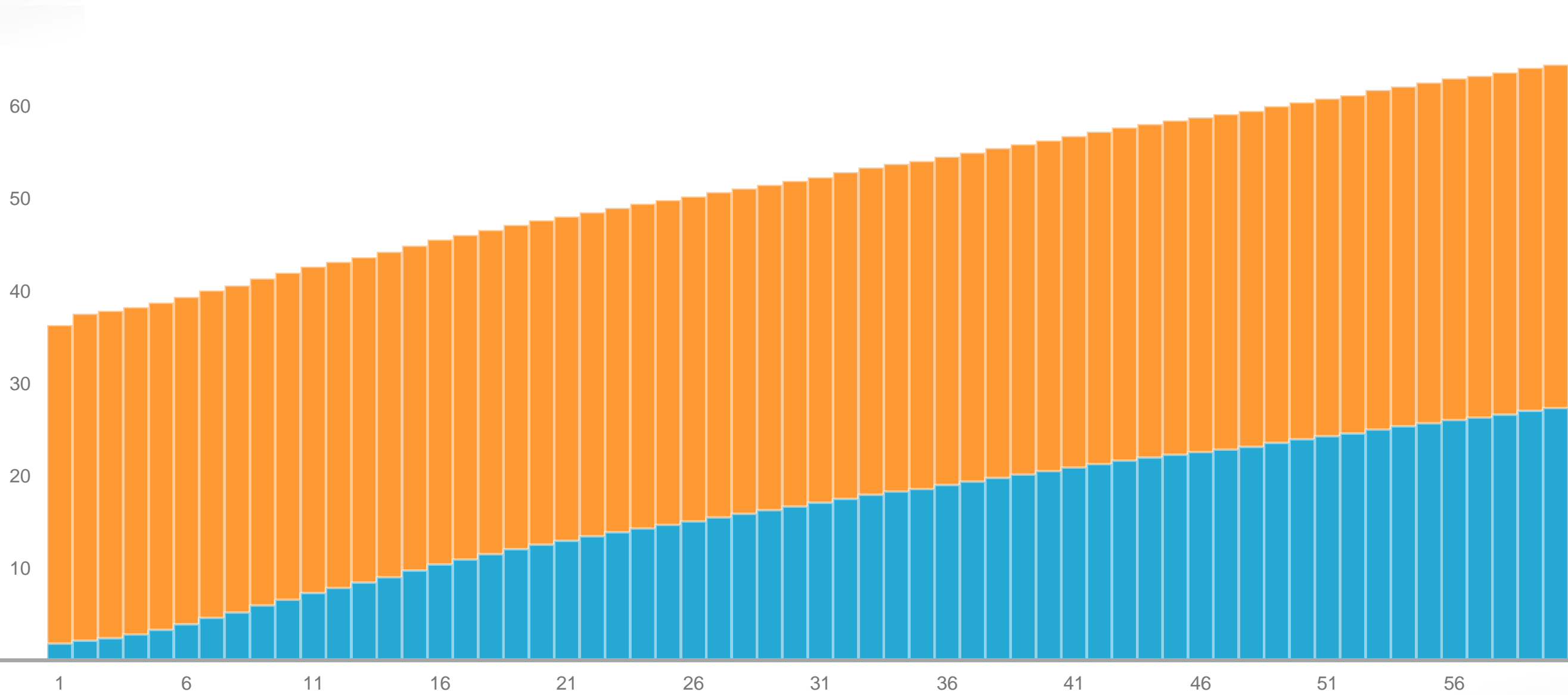
ATTACK CAMPAIGN



-  **12,936** members in botnet
-  **123,909** unique accounts targeted
-  **167,039** total login attempts

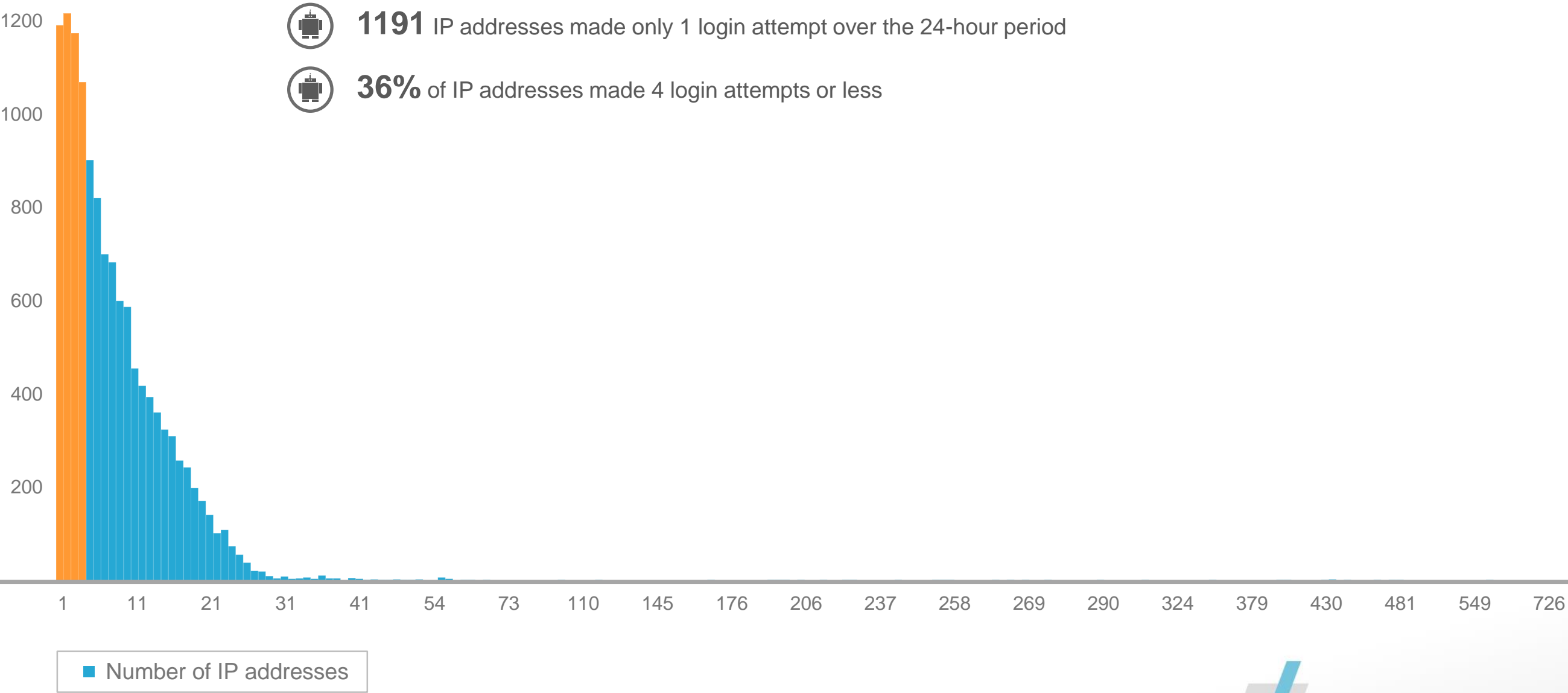
■ Number of login attempts

LOGINS ATTEMPTS, LOW & SLOW

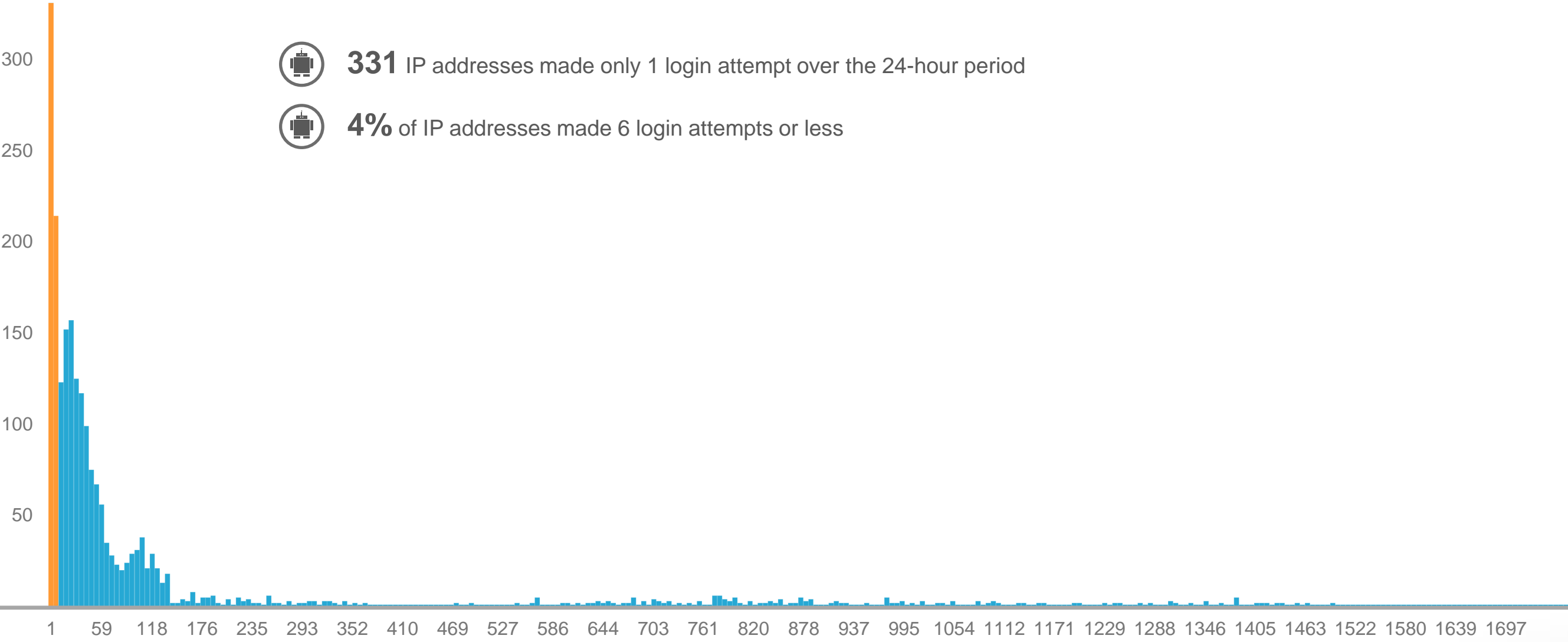




■ % detected within current time window ■ % detected within current and previous time windows

DETECTING BOTS – SINGLE SITE

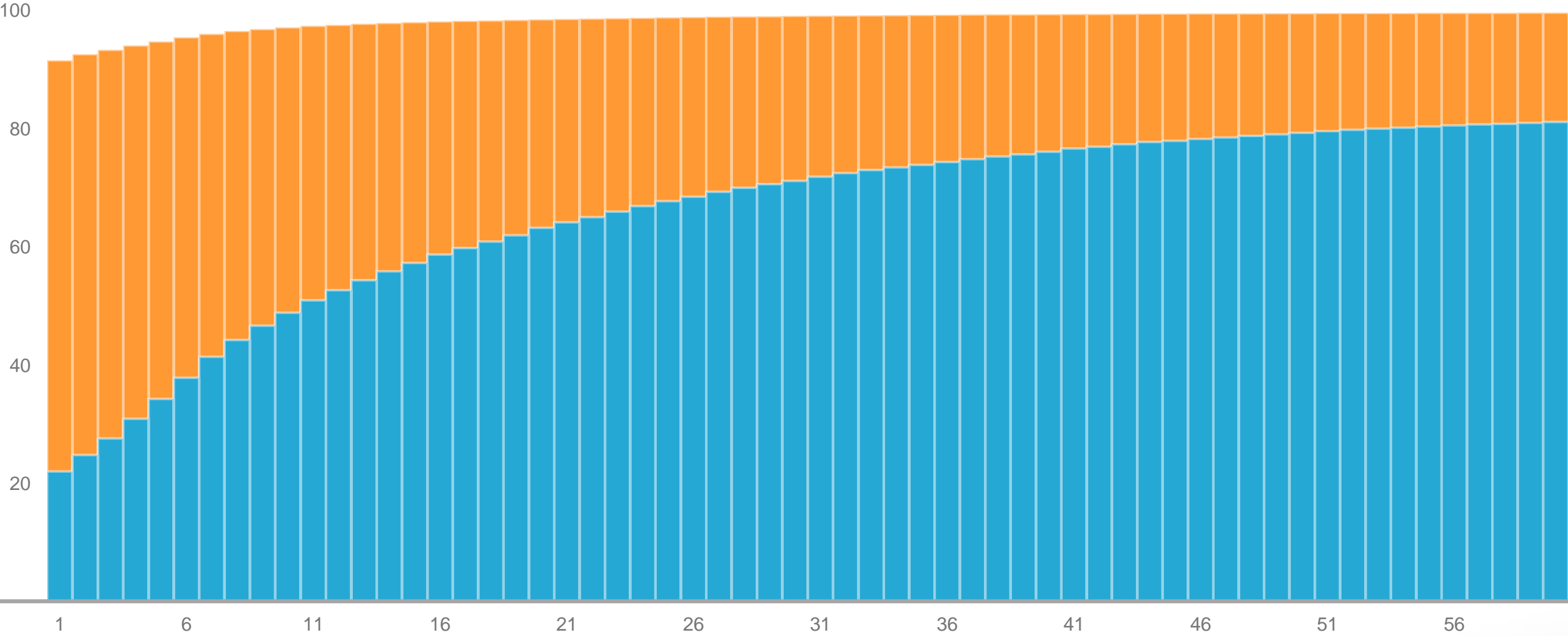


DETECTING BOTS – MANY SITES



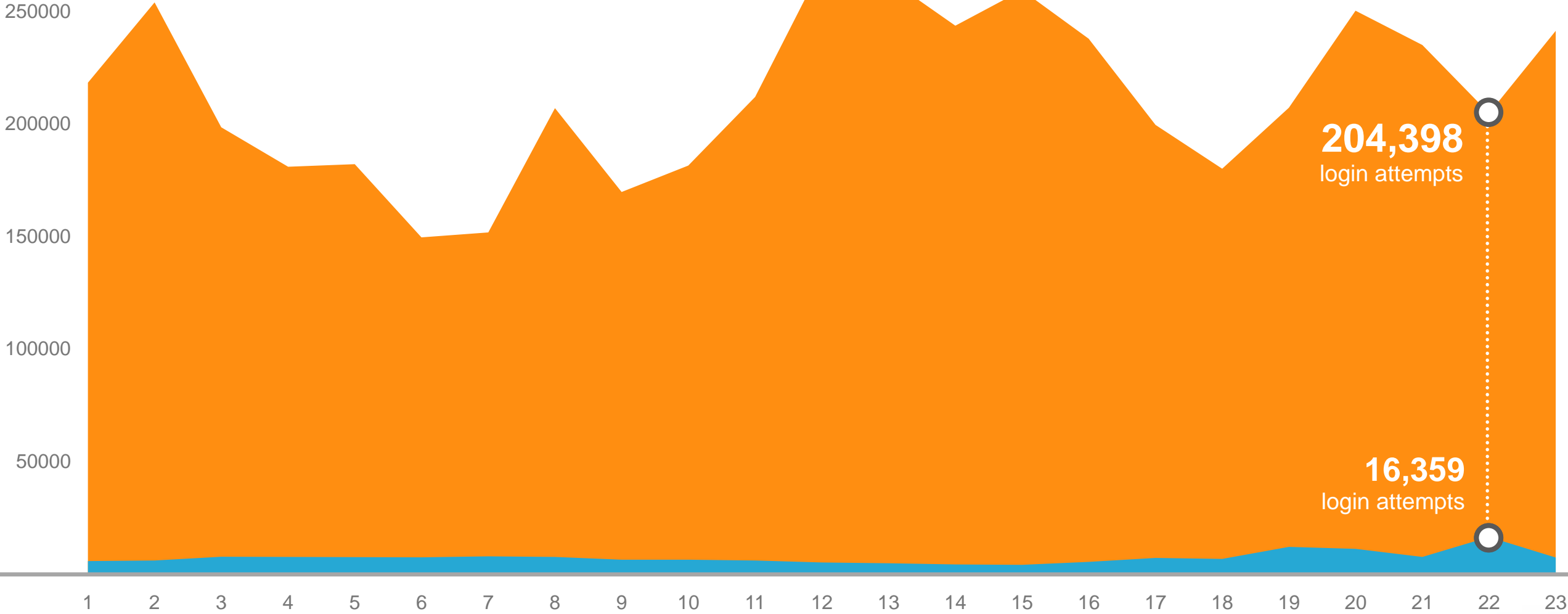
-  **331** IP addresses made only 1 login attempt over the 24-hour period
-  **4%** of IP addresses made 6 login attempts or less

LOGINS ATTEMPTS, LOW & SLOW



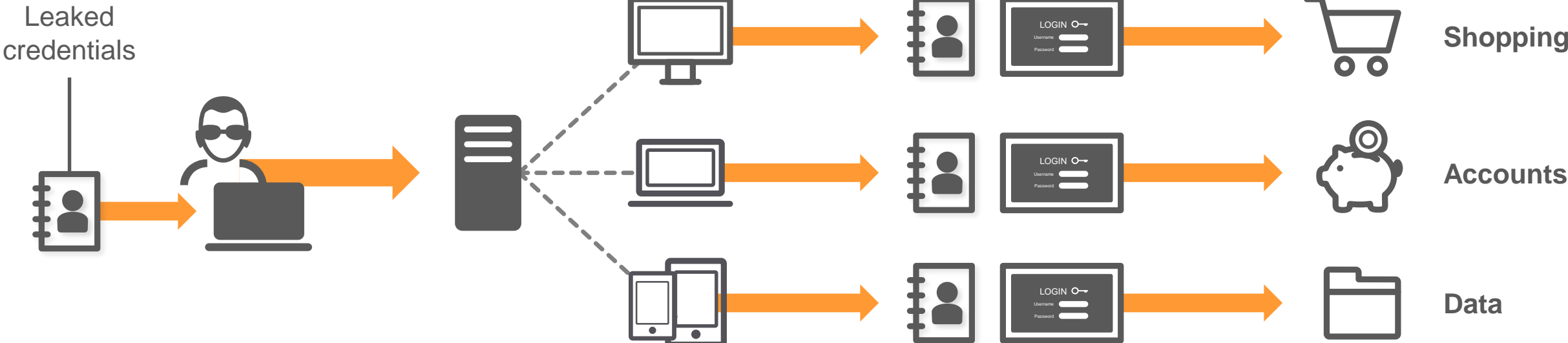
■ % detected within current time window ■ % detected within current and previous time windows

ATTACK CAMPAIGN



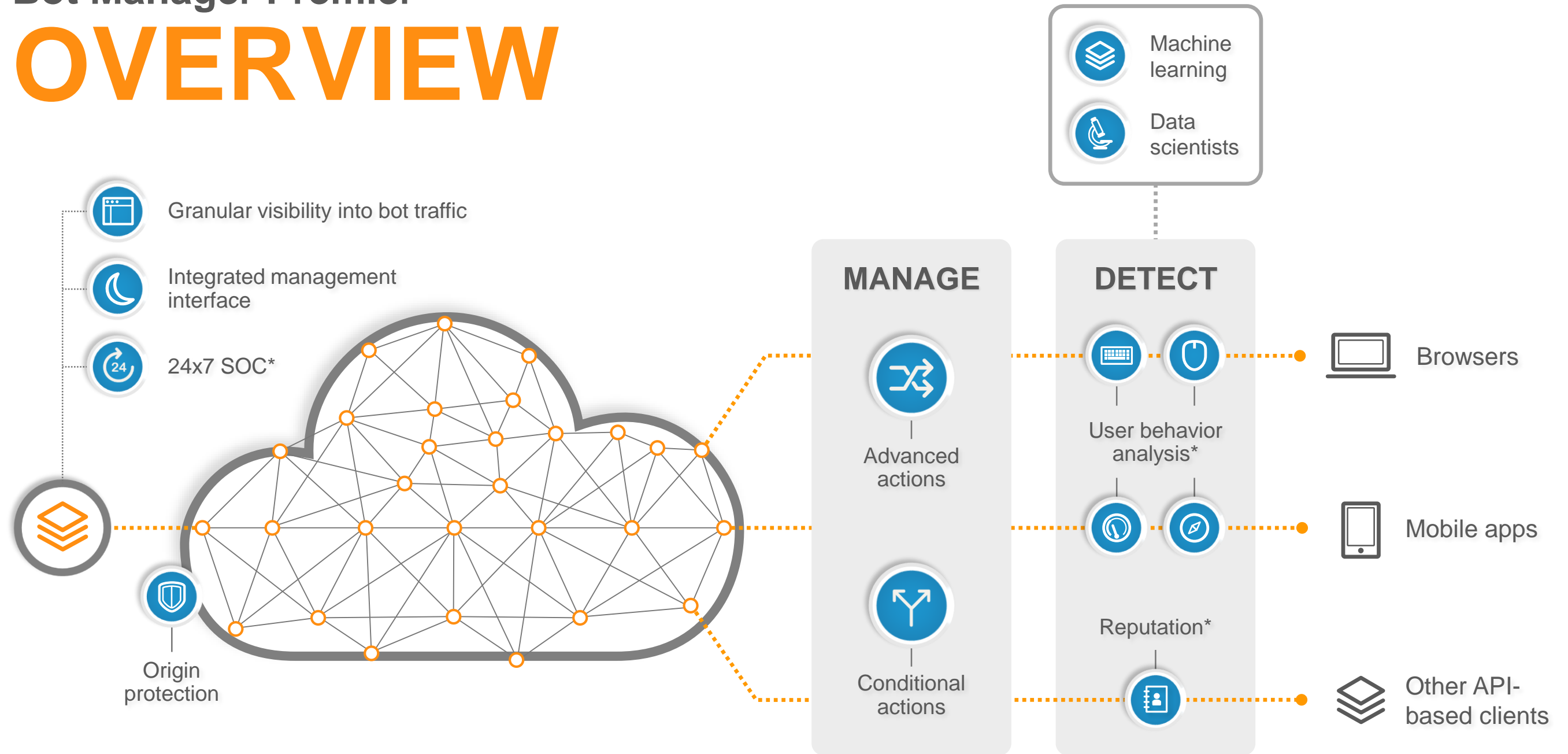
■ Visibility across many customers ■ Visibility from a single customer

CREDENTIAL ABUSE



Bot Manager Premier

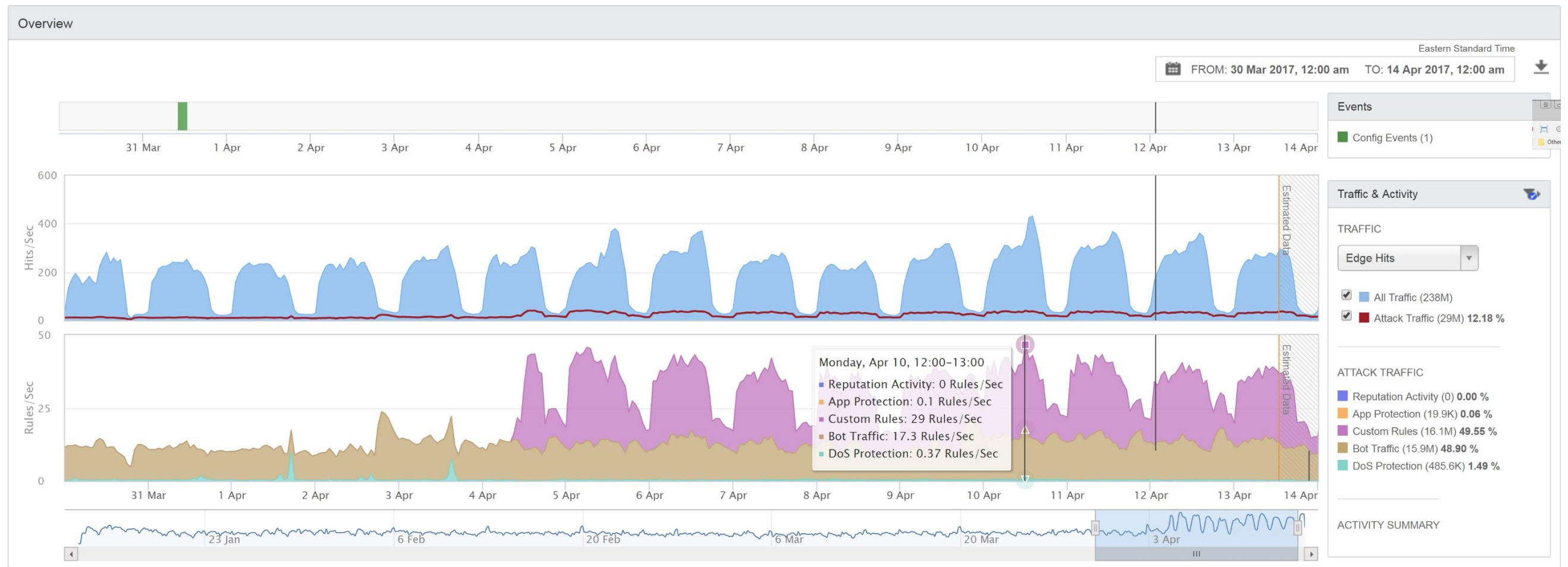
OVERVIEW



*Optional

Premier vs. Standard

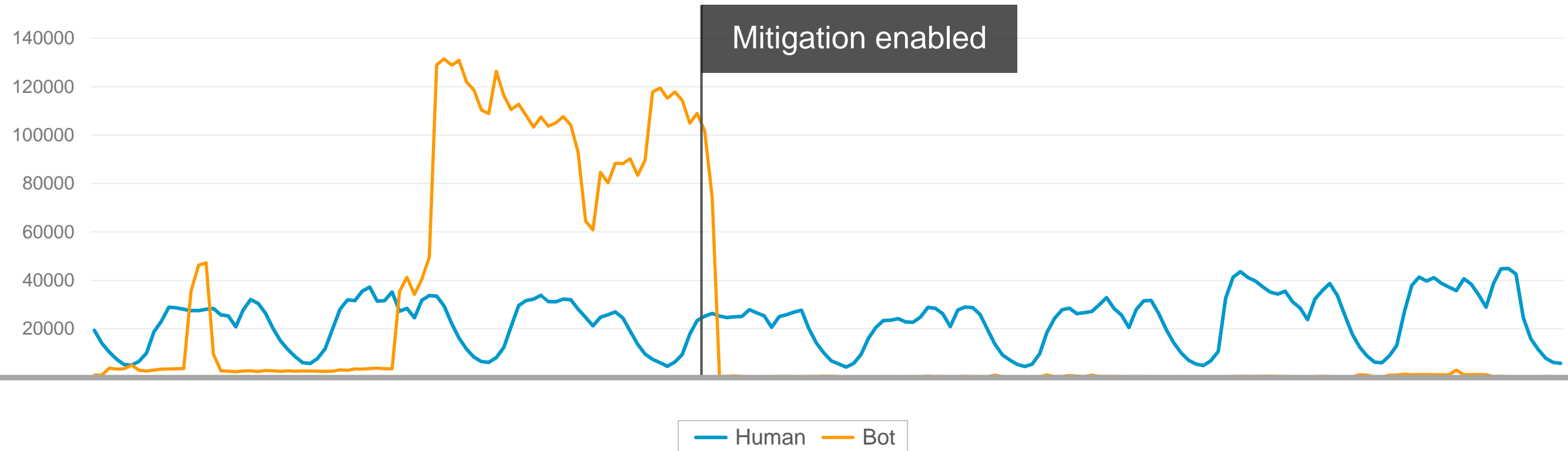
IMPROVED DETECTION



Online retailer

CASE STUDY

Challenge: credential abuse attack peaking at 130k requests per hour



Protecting against credential abuse

AKAMAI DIFFERENCE



The latest technologies that can **detect the most sophisticated bots** today even as they evolve to avoid detection



Real-time intelligence from visibility into bot traffic interacting with many of the largest web presences around the world



Ability to manage wide array of both good and bad bots and **customize response based on your business and IT goals**



Ability to **manage bot traffic at the Akamai edge** to offload your website infrastructure and application development team



Machine learning tailored to credential abuse to better **identify human behavior from bot** and **minimize false positives** (under 0.3%)



Granular visibility / reporting allows you to analyze your bot traffic and implement your bot strategy without being a black box