RISKIQ™

Modern Threat Vectors and their impact to your Web footprint

Till Jäger, RiskIQ

KNOWING IS THE BEST DEFENSE™

BUSINESS HAS EVOLVED

DIGITAL COMMERCE

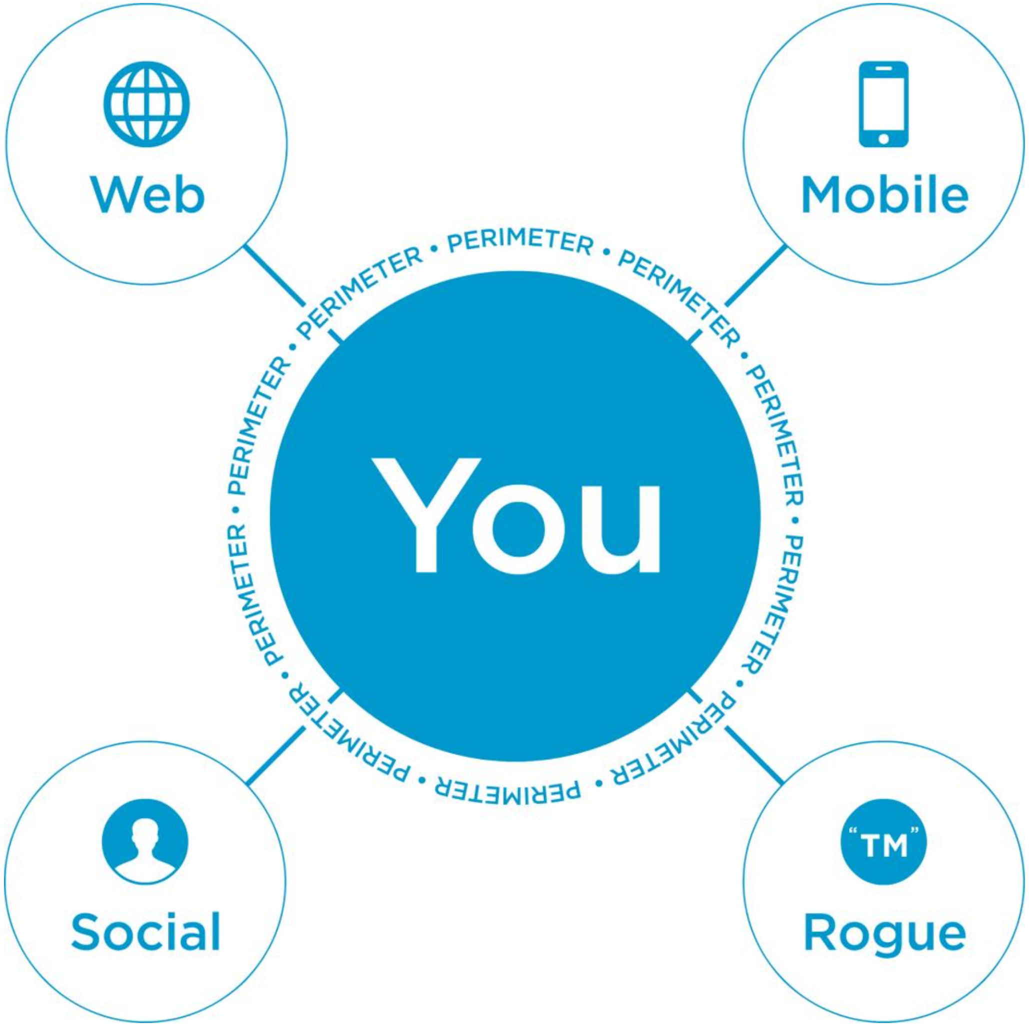
DIGITAL INTERACTIONS

MORE BUSINESS RISK AND CRIPPLING SECURITY BREACHES

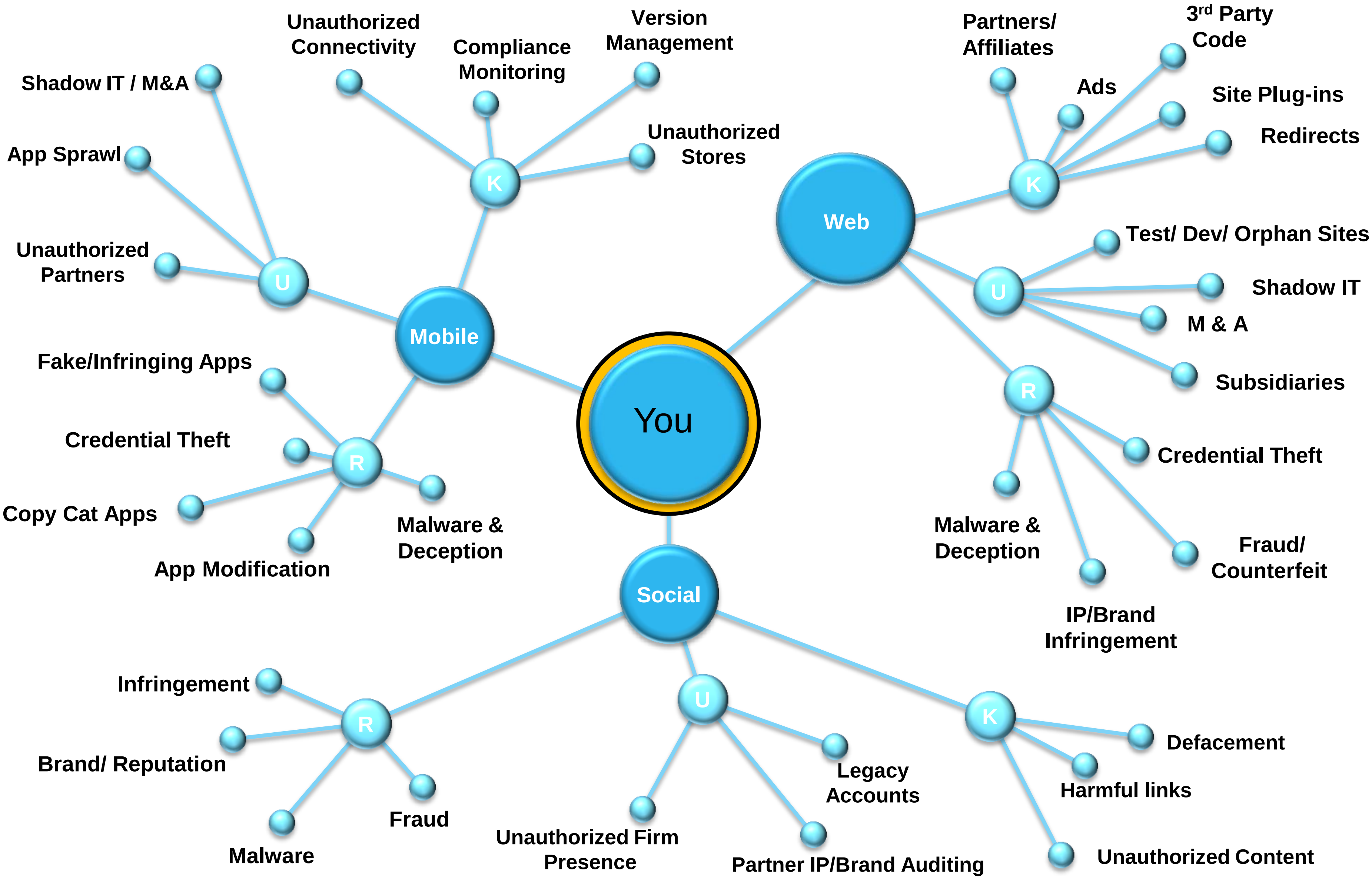
DIGITAL PROCESSES

DIGITAL ASSETS

The result – a rapid expansion of digital channels


Web
Mobile
PERIMETER • PERIMETER • PERIMETER • PERIMETER • PERIMETER • PERIMETER • PERIMETER • PERIMETER • PERIMETER • PERIMETER • PERIMETER • PERIMETER •
You
Social
"TM"
Rogue

Enterprise Digital Footprint Discovery



The enterprise digital footprint challenge

A growing attack surface, which is increasingly hard to manage and therefore defend

Digital footprint questions

What do I have?

- Number of sites
- Number of mobile apps

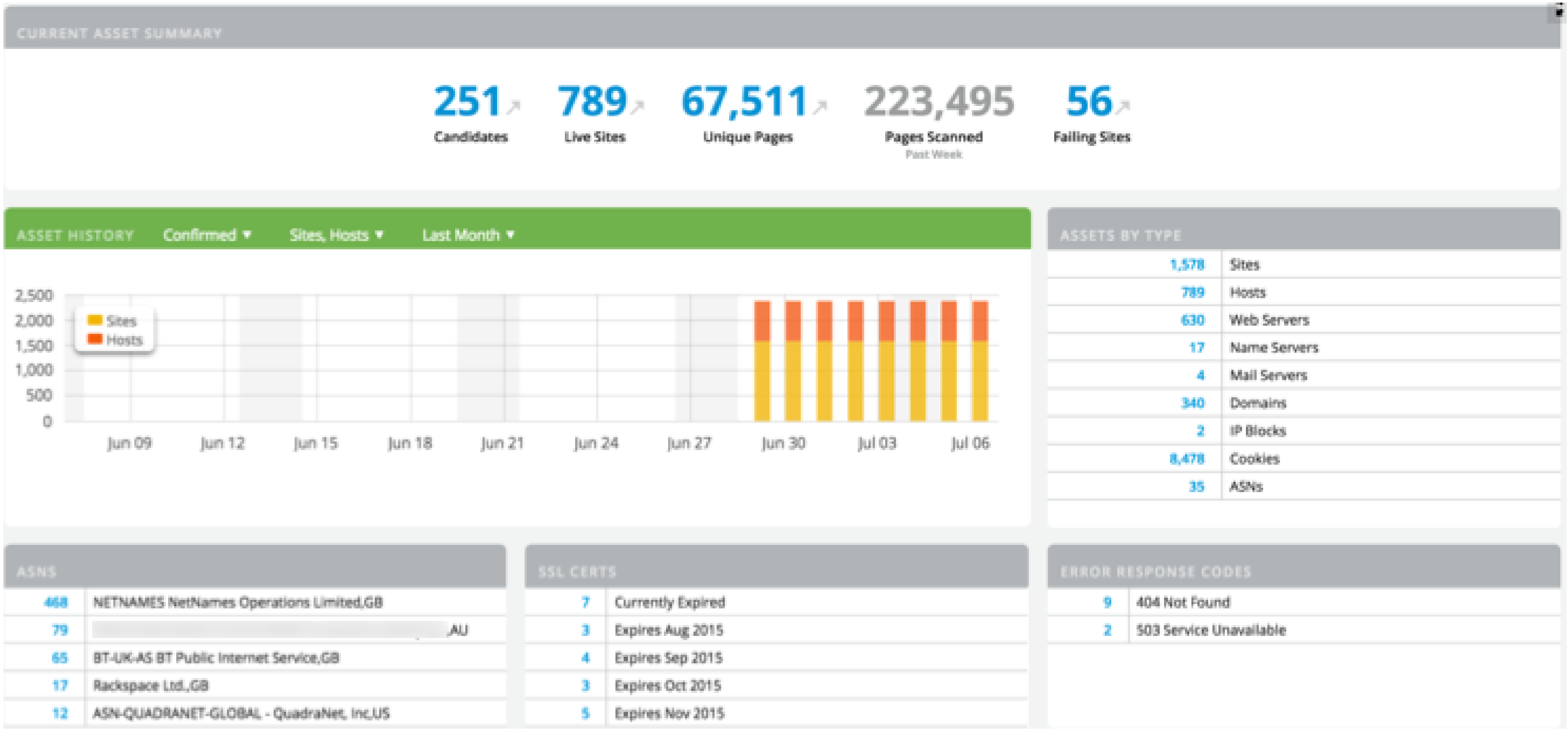
Am I safe?

- Broken links
- Bad certs
- Logins
- Unpatched/Unsupported Servers
- Externally hosted code

Am I compliant?

- Industry regulations
- Internal policies

What do I have?



CURRENT ASSET SUMMARY

251	789	67,511	223,495	56
Candidates	Live Sites	Unique Pages	Pages Scanned Past Week	Failing Sites

ASSET HISTORY Confirmed ▾ Sites, Hosts ▾ Last Month ▾

ASSETS BY TYPE

1,578	Sites
789	Hosts
630	Web Servers
17	Name Servers
4	Mail Servers
340	Domains
2	IP Blocks
8,478	Cookies
35	ASNs

ASNS

468	NETNAMES NetNames Operations Limited,GB
79	[redacted],AU
65	BT-UK-AS BT Public Internet Service,GB
17	Rackspace Ltd.,GB
12	ASN-QUADRANET-GLOBAL - QuadraNet, Inc,US

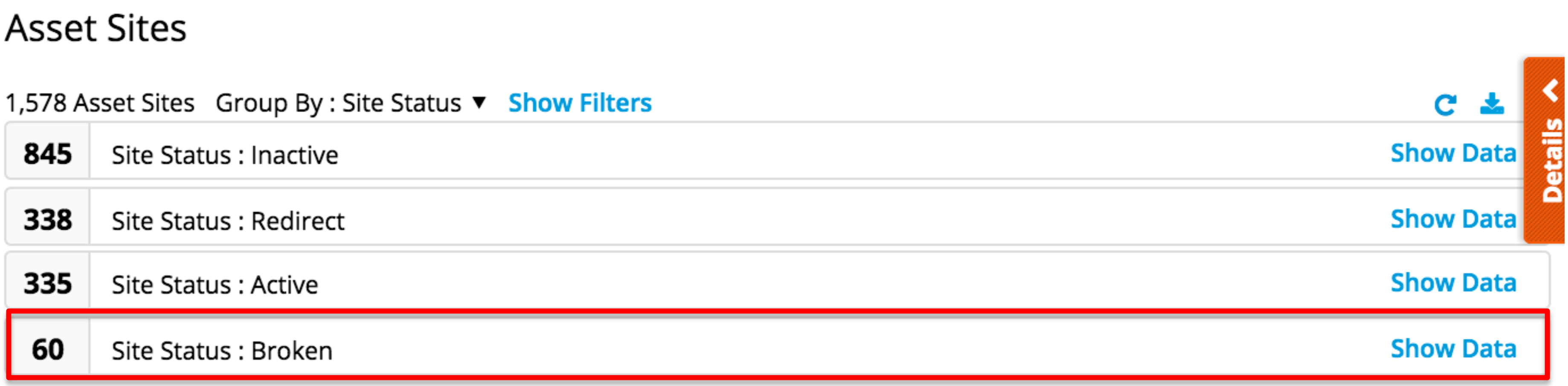
SSL CERTS

7	Currently Expired
3	Expires Aug 2015
4	Expires Sep 2015
3	Expires Oct 2015
5	Expires Nov 2015

ERROR RESPONSE CODES

9	404 Not Found
2	503 Service Unavailable

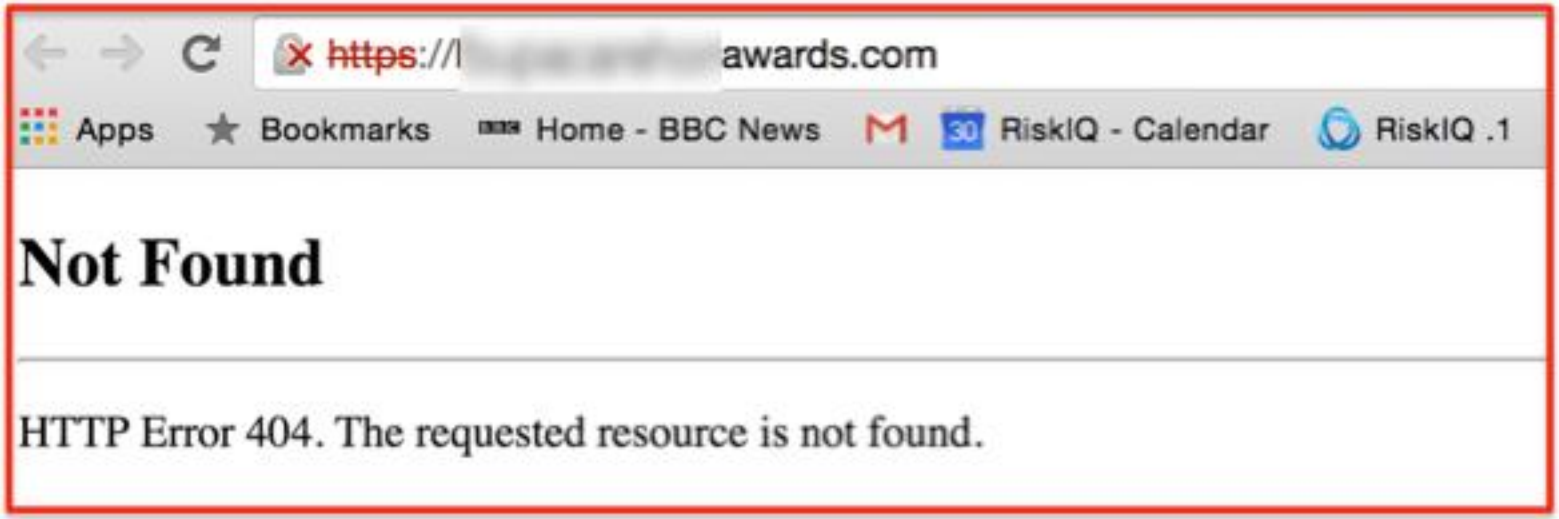
Looking for soft targets



Asset Sites

1,578 Asset Sites Group By : Site Status ▼ Show Filters

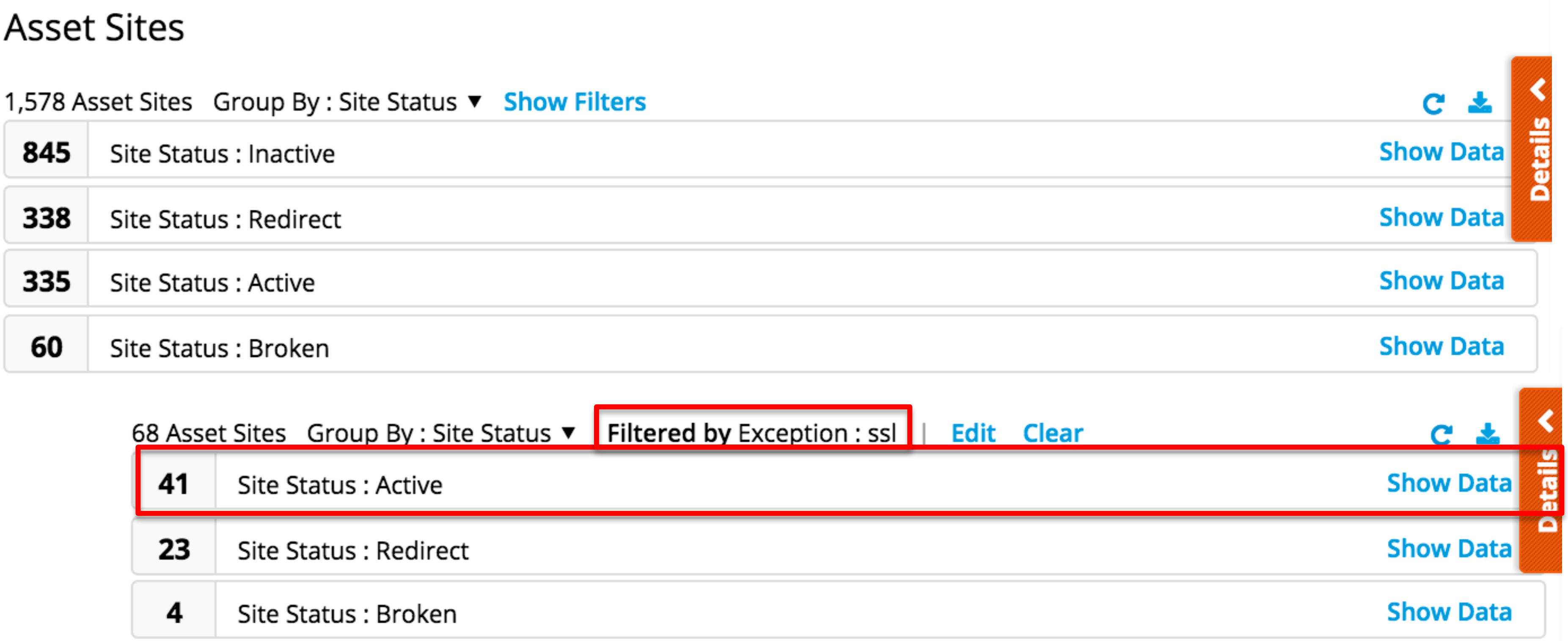
845	Site Status : Inactive	Show Data
338	Site Status : Redirect	Show Data
335	Site Status : Active	Show Data
60	Site Status : Broken	Show Data



Not Found

HTTP Error 404. The requested resource is not found.

Ensuring trust



Asset Sites

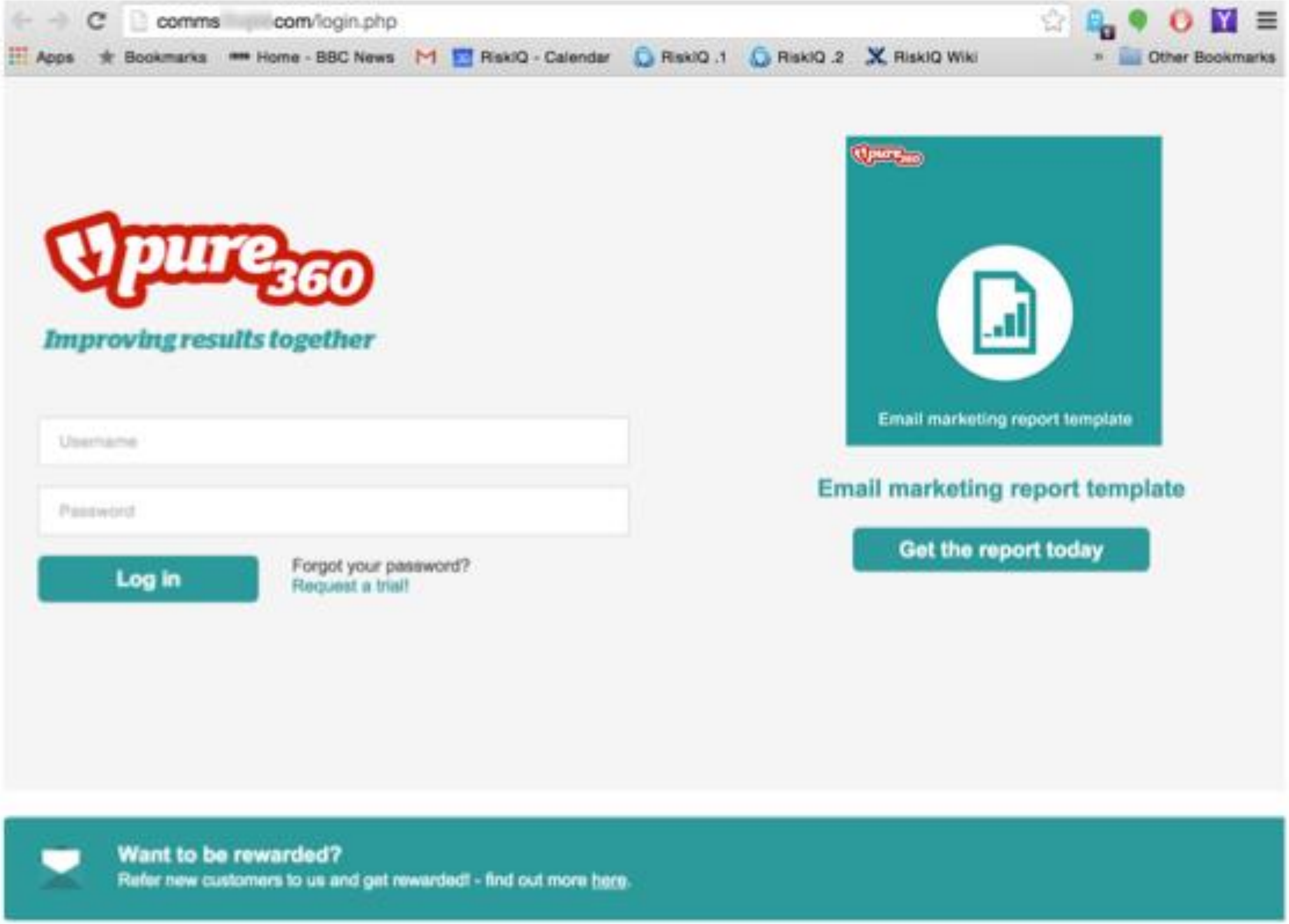
1,578 Asset Sites   Group By : Site Status ▼   Show Filters

845	Site Status : Inactive	Show Data
338	Site Status : Redirect	Show Data
335	Site Status : Active	Show Data
60	Site Status : Broken	Show Data

68 Asset Sites   Group By : Site Status ▼   Filtered by Exception : ssl | Edit   Clear

41	Site Status : Active	Show Data
23	Site Status : Redirect	Show Data
4	Site Status : Broken	Show Data

Protecting credentials

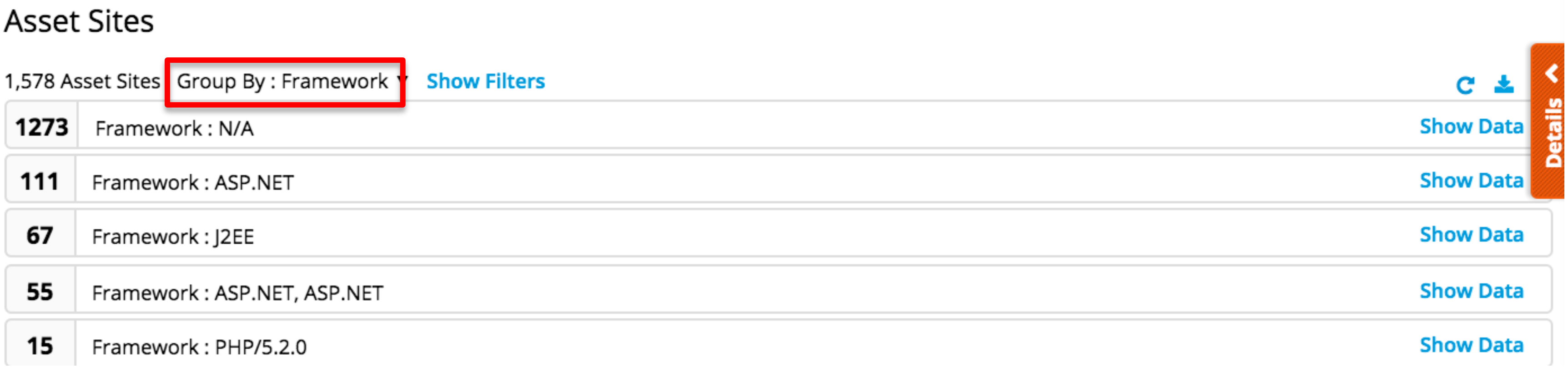


Email marketing report template

Want to be rewarded?

Refer new customers to us and get rewarded! - find out more here.

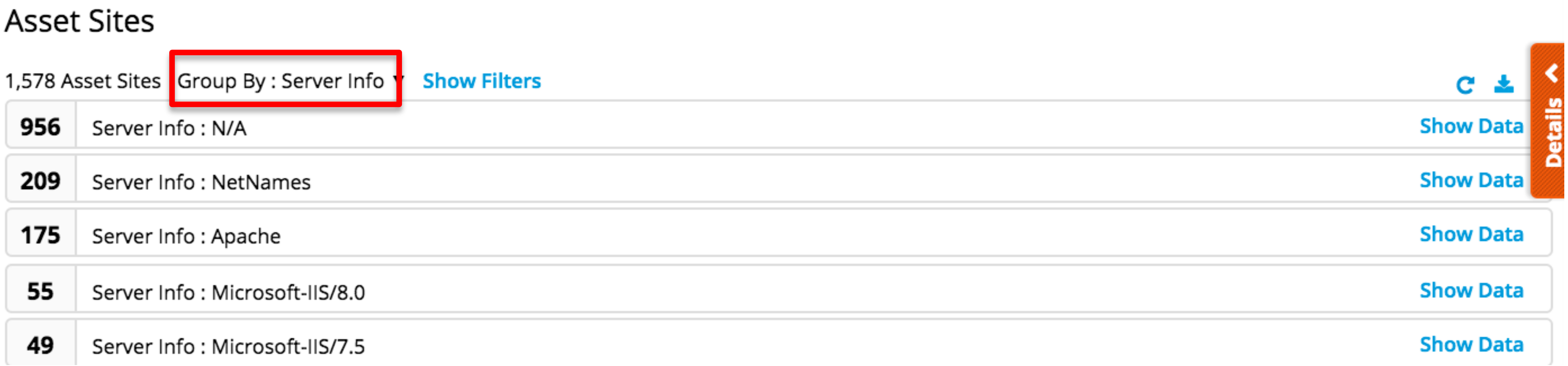
Out of date technology



Asset Sites

1,578 Asset Sites | Group By : Framework ▾ | Show Filters

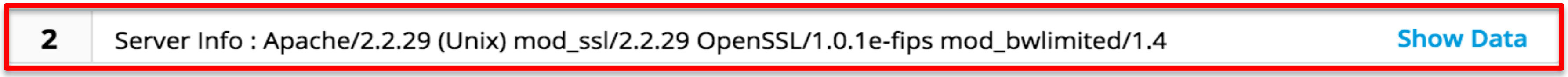
1273	Framework : N/A	Show Data
111	Framework : ASP.NET	Show Data
67	Framework : J2EE	Show Data
55	Framework : ASP.NET, ASP.NET	Show Data
15	Framework : PHP/5.2.0	Show Data



Asset Sites

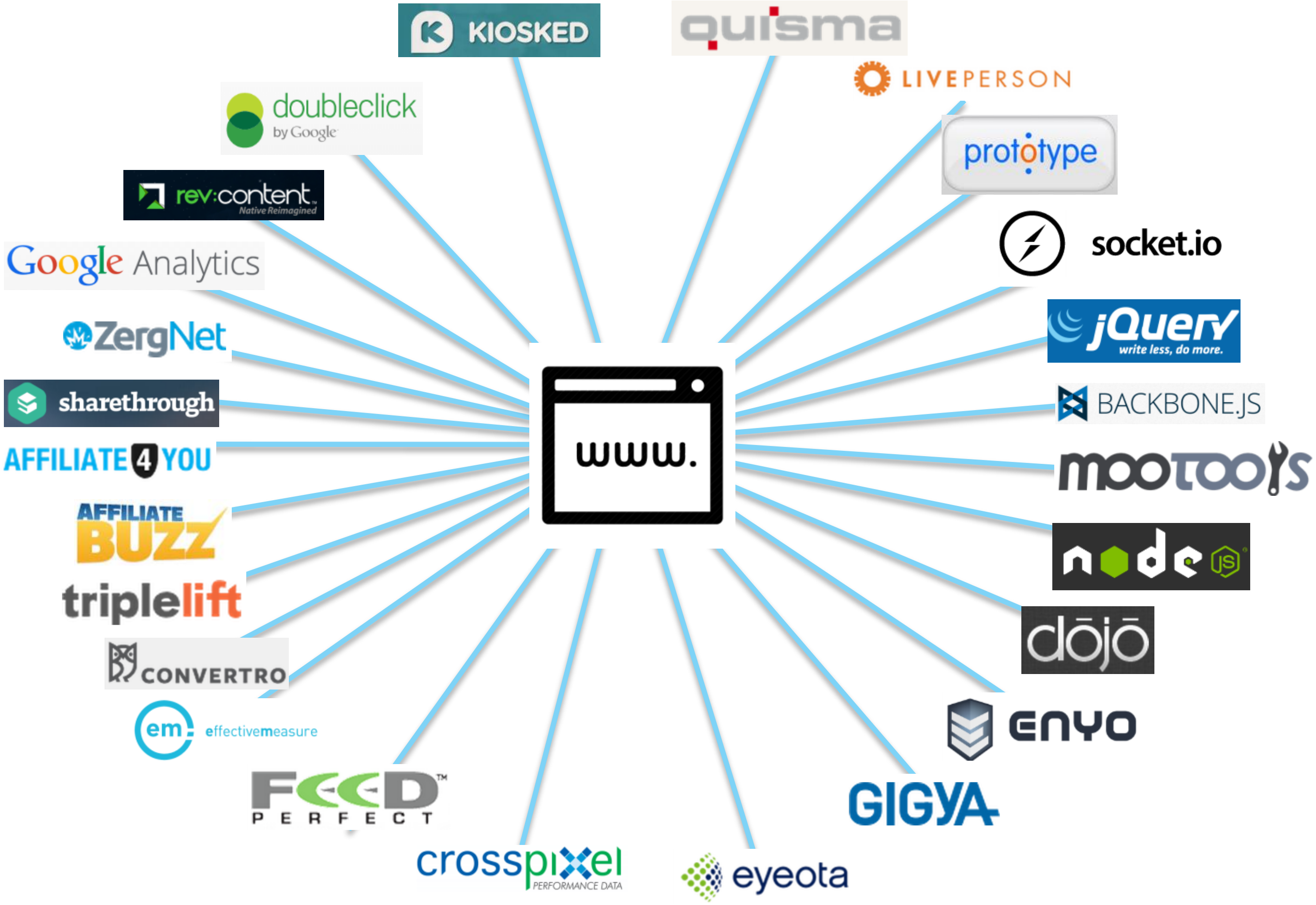
1,578 Asset Sites | Group By : Server Info ▾ | Show Filters

956	Server Info : N/A	Show Data
209	Server Info : NetNames	Show Data
175	Server Info : Apache	Show Data
55	Server Info : Microsoft-IIS/8.0	Show Data
49	Server Info : Microsoft-IIS/7.5	Show Data

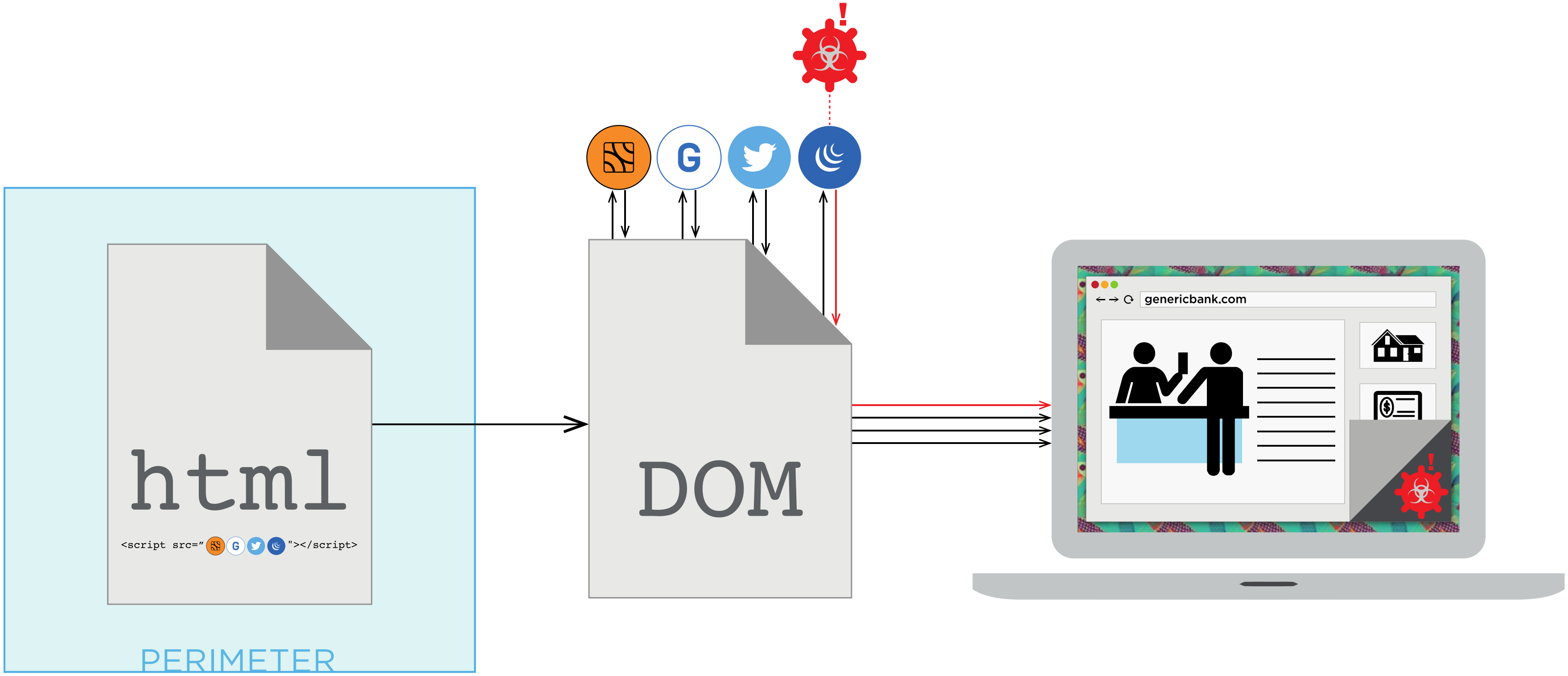


2	Server Info : Apache/2.2.29 (Unix) mod_ssl/2.2.29 OpenSSL/1.0.1e-fips mod_bwlimited/1.4	Show Data

3rd Party Code - The Web Eco System



The Third-Party Security Challenge

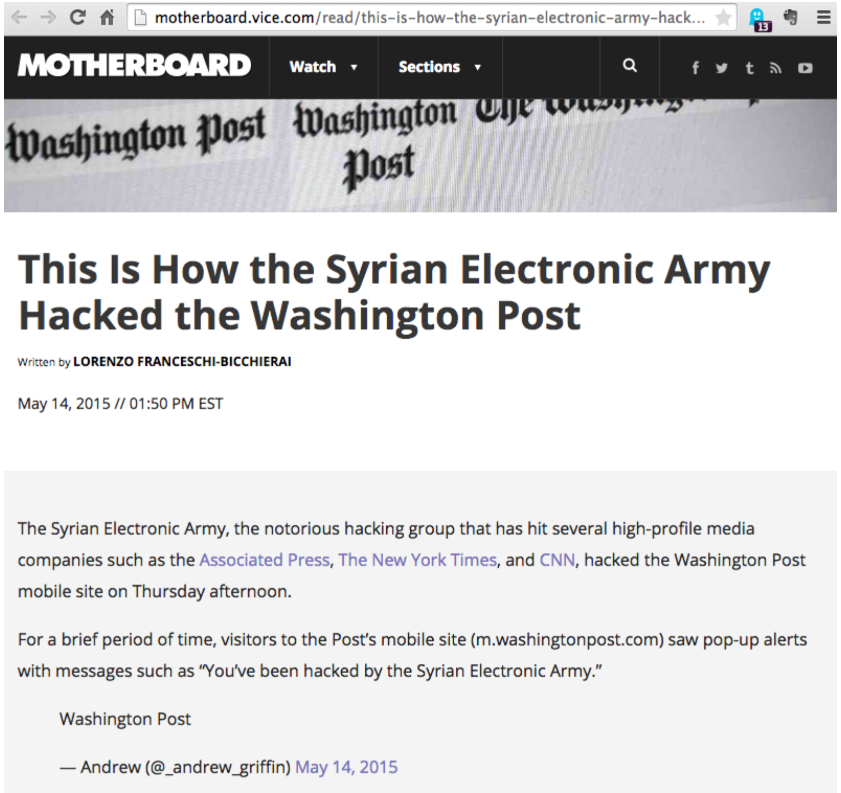


Who’s in control?

jQuery.com Compromise: The Dangers of Third Party Hosted Content

“With code being “blindly” included from 3rd party sites, it is possible that a compromise of this 3rd party site will affect your site’s security”

JS libraries are delivered by CDN


motherboard.vice.com/read/this-is-how-the-syrian-electronic-army-hack...
MOTHERBOARD
Watch ▾
Sections ▾
Washington Post
Washington Post

This Is How the Syrian Electronic Army Hacked the Washington Post

Written by LORENZO FRANCESCHI-BICCHIERAI

May 14, 2015 // 01:50 PM EST

The Syrian Electronic Army, the notorious hacking group that has hit several high-profile media companies such as the Associated Press, The New York Times, and CNN, hacked the Washington Post mobile site on Thursday afternoon.

For a brief period of time, visitors to the Post's mobile site (m.washingtonpost.com) saw pop-up alerts with messages such as "You've been hacked by the Syrian Electronic Army."

> Washington Post
>
> — Andrew (@_andrew_griffin) May 14, 2015

SEA:

“We hacked **InStart CDN** service, and we were working on hacking the main site of Washington Post, but they took down the control panel,” Th3 Pr0 told Motherboard in an email.

“We just wanted to deliver a message on several media sites like Washington Post, US News and others, but we didn't have time :P.”

Your web footprint is not a static environment

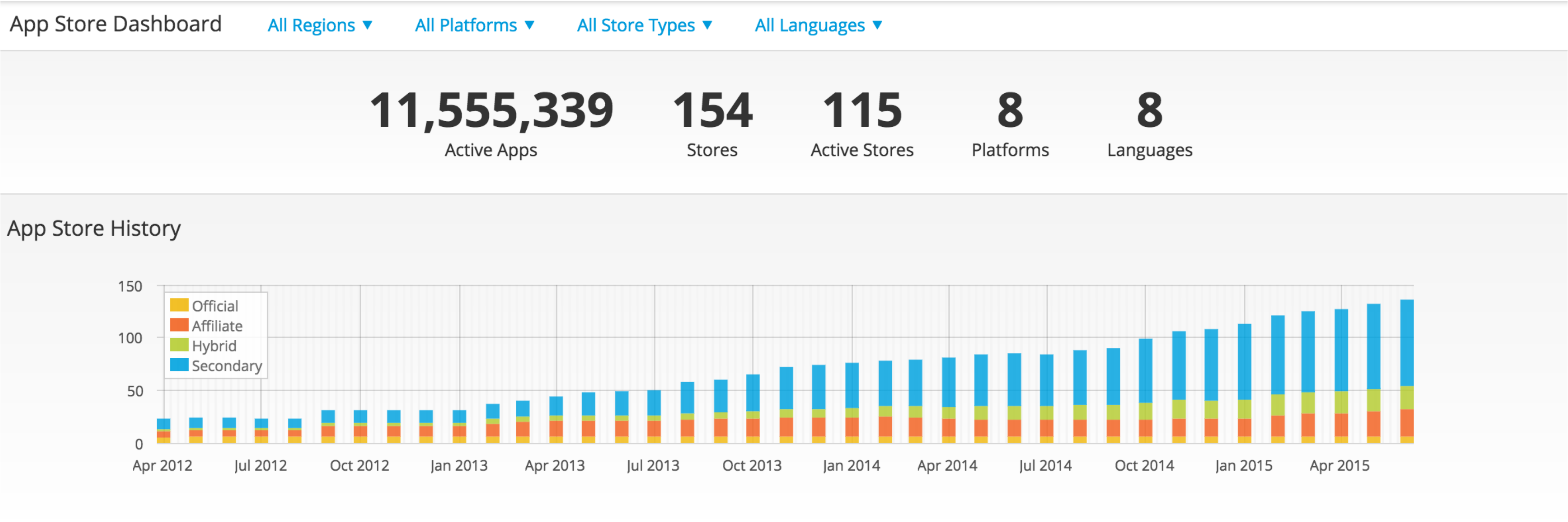
Monitoring Categories:

- New Asset Discovery
- External Threat
- Indicators of Compromise
- Infrastructure
- Mobile App Compliance
- Social Media Compliance
- Web Compliance

Start with out of the box policies

Extend to customer specific policies

The mobile ecosystem is a scary place



App Store Dashboard

All Regions ▼ All Platforms ▼ All Store Types ▼ All Languages ▼

11,555,339 Active Apps

154 Stores

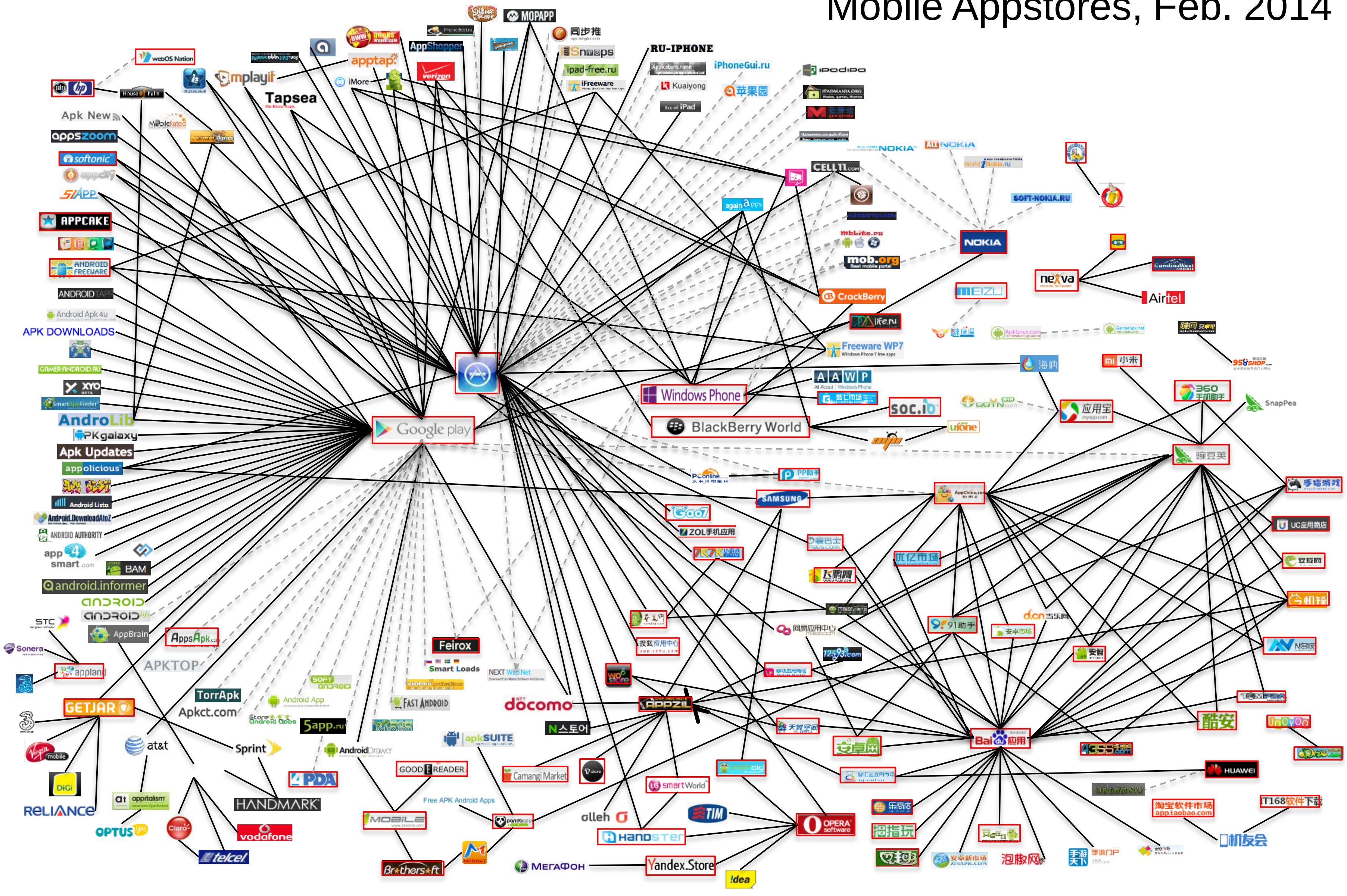
115 Active Stores

8 Platforms

8 Languages

App Store History

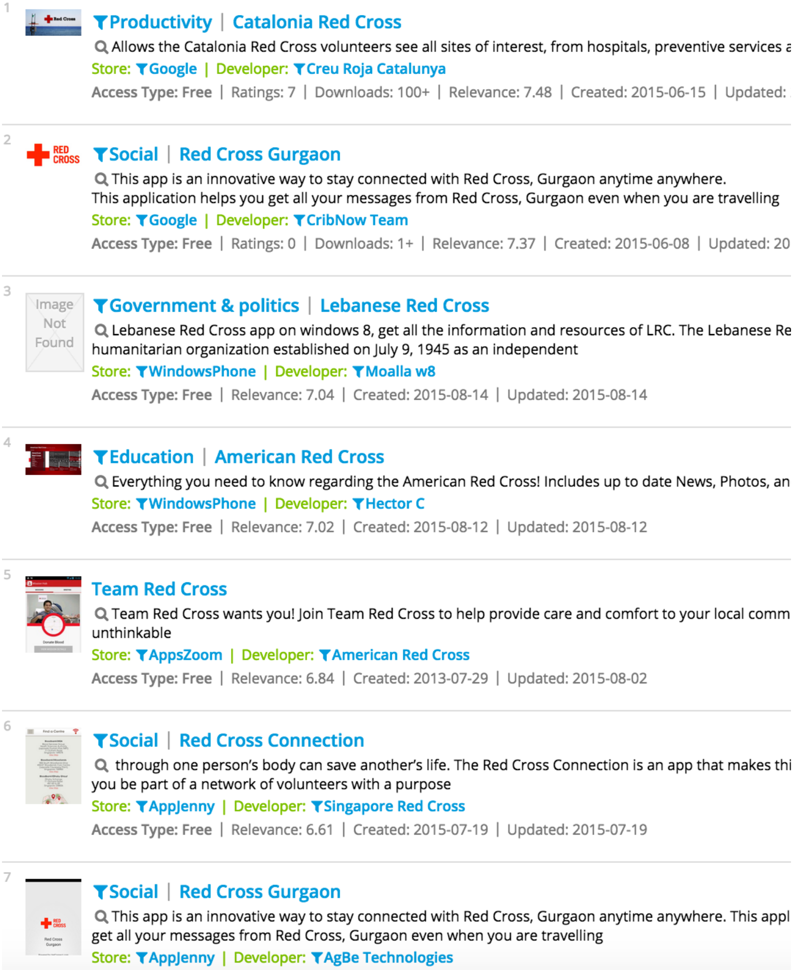
Mobile Appstores, Feb. 2014



What is my mobile footprint?

Searching for “Red Cross”:

- 1000’s App references
- 250 ‘Red Cross’ Developers
- 120 Different Stores



1 Productivity | Catalonia Red Cross
Allows the Catalonia Red Cross volunteers see all sites of interest, from hospitals, preventive services a
Store: Google | Developer: Creu Roja Catalunya
Access Type: Free | Ratings: 7 | Downloads: 100+ | Relevance: 7.48 | Created: 2015-06-15 | Updated:

2 Social | Red Cross Gurgaon
This app is an innovative way to stay connected with Red Cross, Gurgaon anytime anywhere.
This application helps you get all your messages from Red Cross, Gurgaon even when you are travelling
Store: Google | Developer: CribNow Team
Access Type: Free | Ratings: 0 | Downloads: 1+ | Relevance: 7.37 | Created: 2015-06-08 | Updated: 20

3 Government & politics | Lebanese Red Cross
Lebanese Red Cross app on windows 8, get all the information and resources of LRC. The Lebanese Re
humanitarian organization established on July 9, 1945 as an independent
Store: WindowsPhone | Developer: Moalla w8
Access Type: Free | Relevance: 7.04 | Created: 2015-08-14 | Updated: 2015-08-14

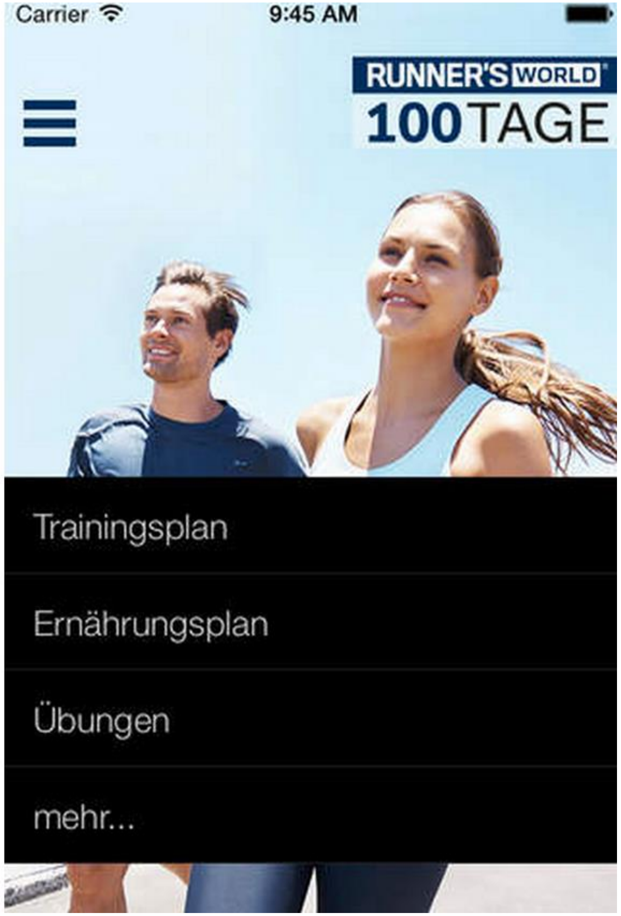
4 Education | American Red Cross
Everything you need to know regarding the American Red Cross! Includes up to date News, Photos, an
Store: WindowsPhone | Developer: Hector C
Access Type: Free | Relevance: 7.02 | Created: 2015-08-12 | Updated: 2015-08-12

5 Team Red Cross
Team Red Cross wants you! Join Team Red Cross to help provide care and comfort to your local comm
unthinkable
Store: AppsZoom | Developer: American Red Cross
Access Type: Free | Relevance: 6.84 | Created: 2013-07-29 | Updated: 2015-08-02

6 Social | Red Cross Connection
through one person’s body can save another’s life. The Red Cross Connection is an app that makes thi
you be part of a network of volunteers with a purpose
Store: AppJenny | Developer: Singapore Red Cross
Access Type: Free | Relevance: 6.61 | Created: 2015-07-19 | Updated: 2015-07-19

7 Social | Red Cross Gurgaon
This app is an innovative way to stay connected with Red Cross, Gurgaon anytime anywhere. This appl
get all your messages from Red Cross, Gurgaon even when you are travelling
Store: AppJenny | Developer: AgBe Technologies

Is this in line with my mobile policy?

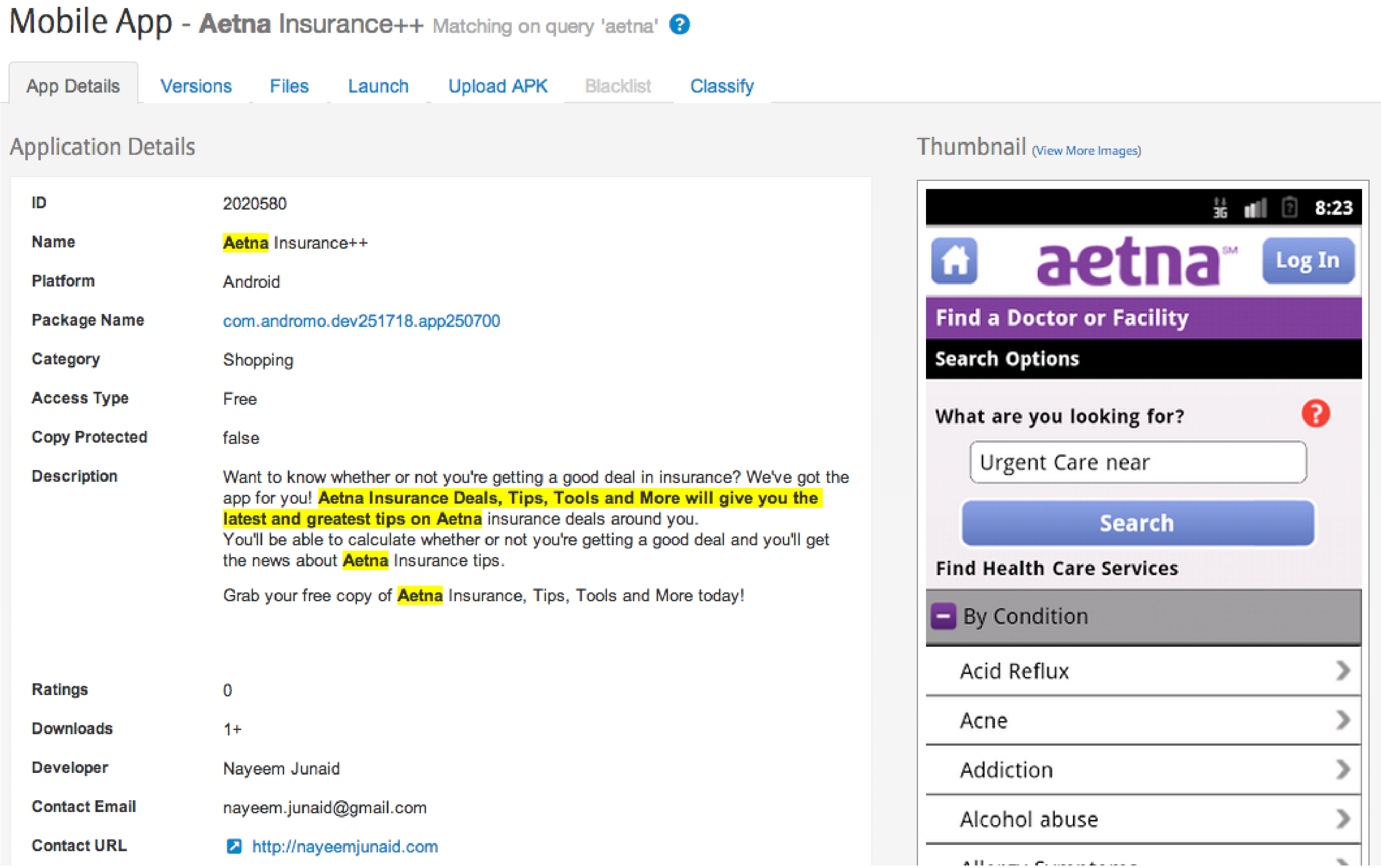


Apple store

Developer:	The Customer Inc.
Supports:	account logins and credit card purchases

Is this a legitimate app?

Aetna Rogue App



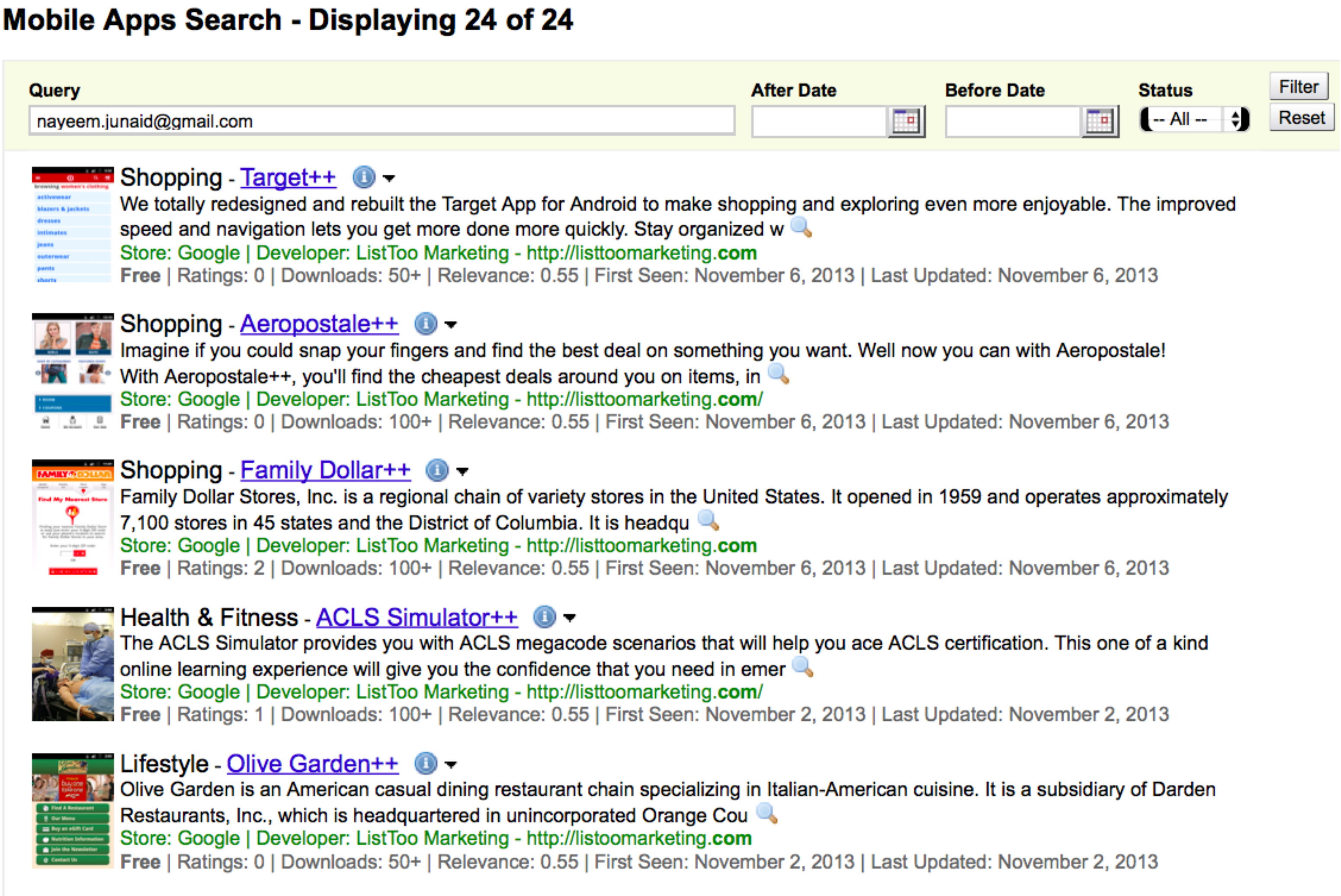
Mobile App - **Aetna** Insurance++ Matching on query 'aetna'

Application Details

ID	2020580
Name	**Aetna** Insurance++
Platform	Android
Package Name	com.andromo.dev251718.app250700
Category	Shopping
Access Type	Free
Copy Protected	false
Description	Want to know whether or not you're getting a good deal in insurance? We've got the app for you! **Aetna Insurance Deals, Tips, Tools and More will give you the latest and greatest tips on Aetna** insurance deals around you. You'll be able to calculate whether or not you're getting a good deal and you'll get the news about **Aetna** Insurance tips. Grab your free copy of **Aetna** Insurance, Tips, Tools and More today!
Ratings	0
Downloads	1+
Developer	Nayeem Junaid
Contact Email	nayeem.junaid@gmail.com
Contact URL	http://nayeemjunaid.com

Thumbnail (View More Images)

Developer for Aetna Insurance++



Mobile Apps Search - Displaying 24 of 24

Query: nayeem.junaid@gmail.com

Shopping - Target++
We totally redesigned and rebuilt the Target App for Android to make shopping and exploring even more enjoyable. The improved speed and navigation lets you get more done more quickly. Stay organized w
Store: Google | Developer: ListToo Marketing - http://listtoomarketing.com
Free | Ratings: 0 | Downloads: 50+ | Relevance: 0.55 | First Seen: November 6, 2013 | Last Updated: November 6, 2013

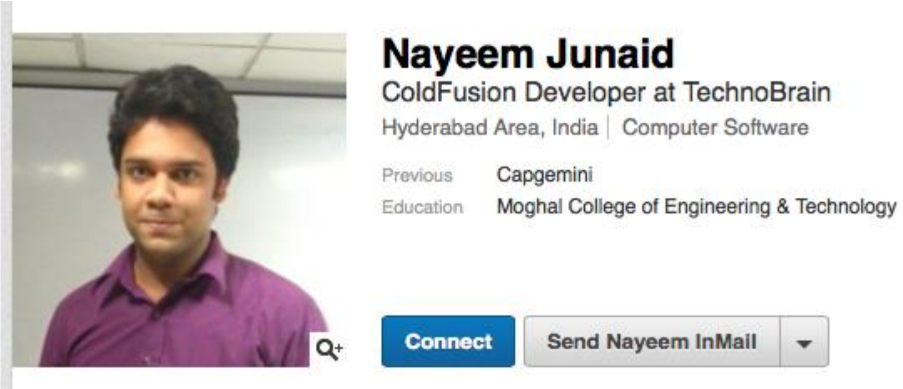
Shopping - Aeropostale++
Imagine if you could snap your fingers and find the best deal on something you want. Well now you can with Aeropostale! With Aeropostale++, you'll find the cheapest deals around you on items, in
Store: Google | Developer: ListToo Marketing - http://listtoomarketing.com/
Free | Ratings: 0 | Downloads: 100+ | Relevance: 0.55 | First Seen: November 6, 2013 | Last Updated: November 6, 2013

Shopping - Family Dollar++
Family Dollar Stores, Inc. is a regional chain of variety stores in the United States. It opened in 1959 and operates approximately 7,100 stores in 45 states and the District of Columbia. It is headqu
Store: Google | Developer: ListToo Marketing - http://listtoomarketing.com
Free | Ratings: 2 | Downloads: 100+ | Relevance: 0.55 | First Seen: November 6, 2013 | Last Updated: November 6, 2013

Health & Fitness - ACLS Simulator++
The ACLS Simulator provides you with ACLS megacode scenarios that will help you ace ACLS certification. This one of a kind online learning experience will give you the confidence that you need in emer
Store: Google | Developer: ListToo Marketing - http://listtoomarketing.com/
Free | Ratings: 1 | Downloads: 100+ | Relevance: 0.55 | First Seen: November 2, 2013 | Last Updated: November 2, 2013

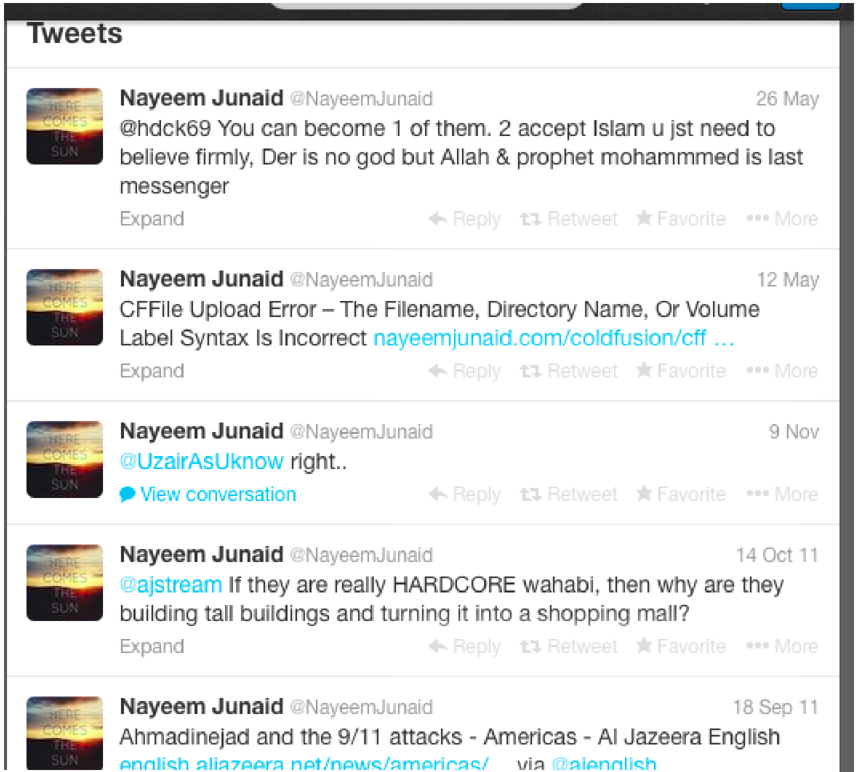
Lifestyle - Olive Garden++
Olive Garden is an American casual dining restaurant chain specializing in Italian-American cuisine. It is a subsidiary of Darden Restaurants, Inc., which is headquartered in unincorporated Orange Cou
Store: Google | Developer: ListToo Marketing - http://listoomarketing.com
Free | Ratings: 0 | Downloads: 50+ | Relevance: 0.55 | First Seen: November 2, 2013 | Last Updated: November 2, 2013

Developer for Aetna Insurance++



Nayeem Junaid
ColdFusion Developer at TechnoBrain
Hyderabad Area, India | Computer Software

Previous Capgemini
Education Moghal College of Engineering & Technology



Tweets

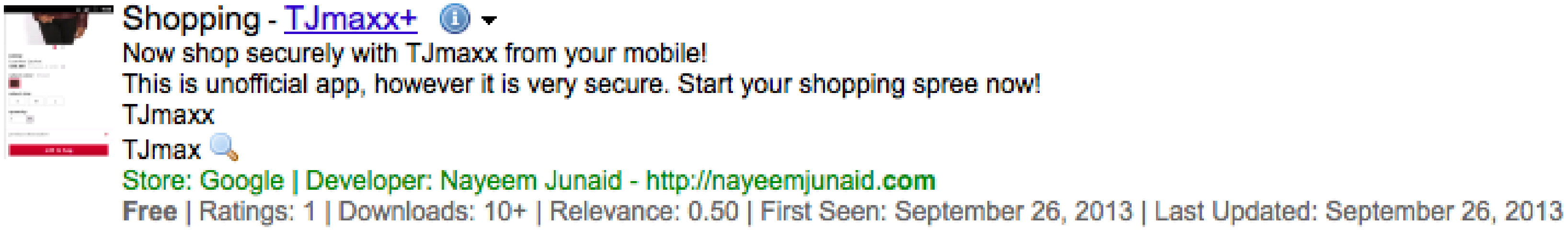
Nayeem Junaid @NayeemJunaid 26 May
@hdck69 You can become 1 of them. 2 accept Islam u jst need to believe firmly, Der is no god but Allah & prophet mohammmed is last messenger

Nayeem Junaid @NayeemJunaid 12 May
CFFile Upload Error – The Filename, Directory Name, Or Volume Label Syntax Is Incorrect nayeemjunaid.com/coldfusion/cff …

Nayeem Junaid @NayeemJunaid 9 Nov
@UzairAsUknow right..

Nayeem Junaid @NayeemJunaid 14 Oct 11
@ajstream If they are really HARDCORE wahabi, then why are they building tall buildings and turning it into a shopping mall?

Nayeem Junaid @NayeemJunaid 18 Sep 11
Ahmadinejad and the 9/11 attacks - Americas - Al Jazeera English
english.aljazeera.net/news/americas/… via @ajenglish

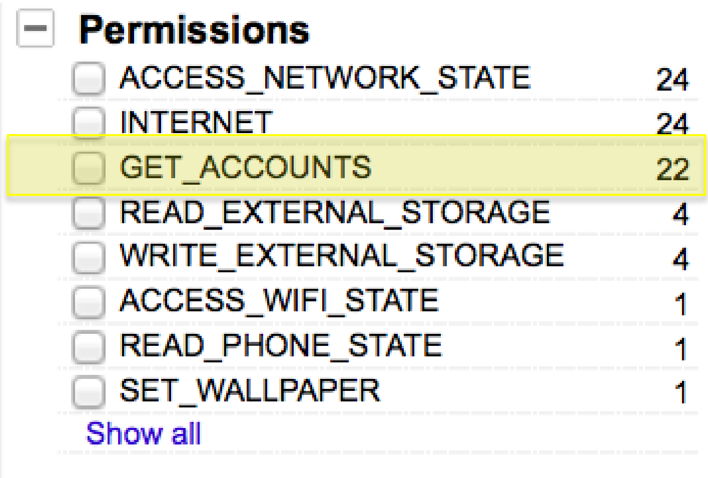


Shopping - TJmaxx+
Now shop securely with TJmaxx from your mobile!
This is unofficial app, however it is very secure. Start your shopping spree now!
TJmaxx
TJmax
Store: Google | Developer: Nayeem Junaid - http://nayeemjunaid.com
Free | Ratings: 1 | Downloads: 10+ | Relevance: 0.50 | First Seen: September 26, 2013 | Last Updated: September 26, 2013

Aetna++ Permissions

22 of the apps are requesting the GET_ACCOUNTS permission

GET_ACCOUNTS lets you see various accounts on a phone via account manager, including Google, Facebook, Twitter, etc.



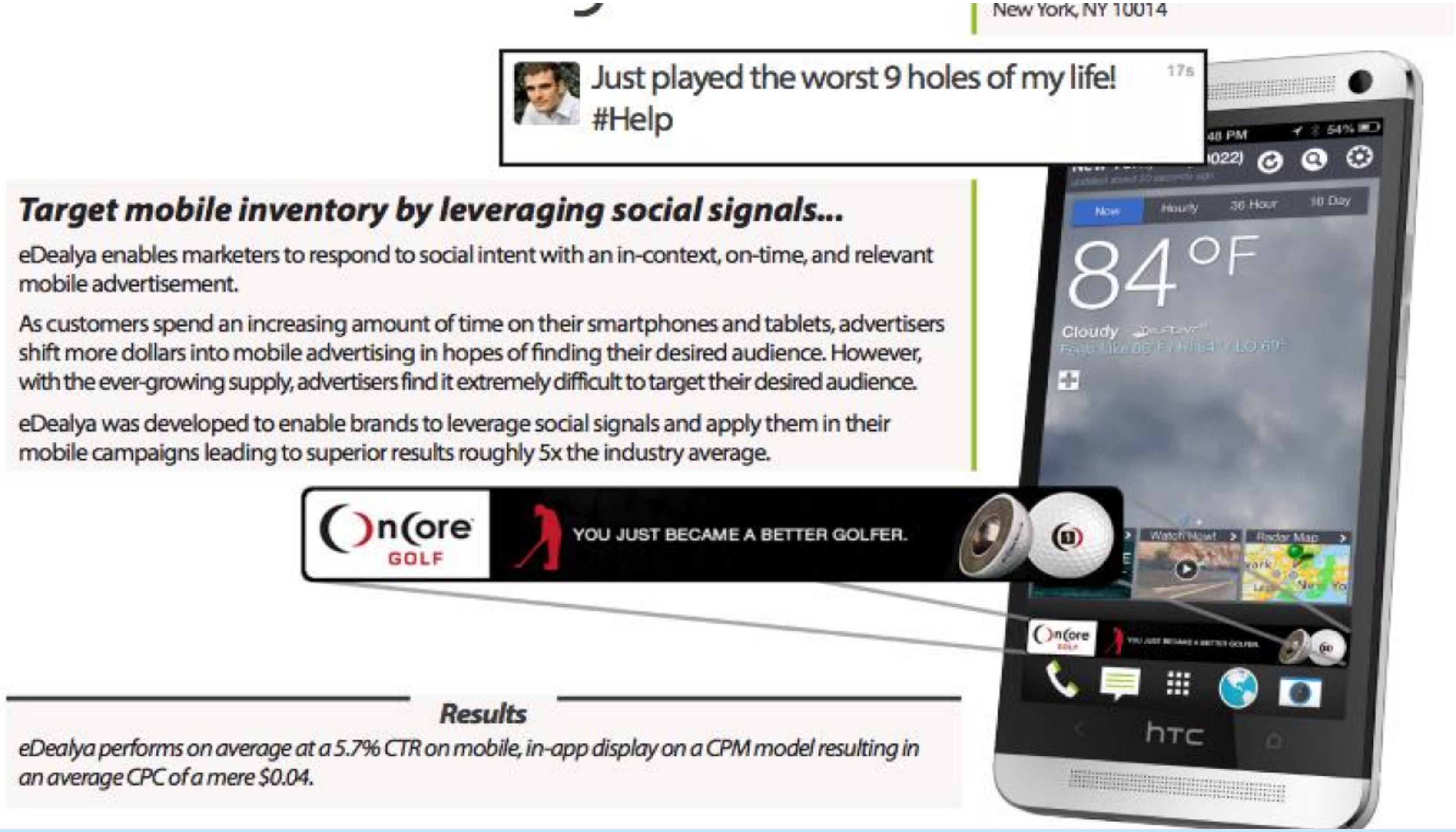
Permissions

□	ACCESS_NETWORK_STATE	24
□	INTERNET	24
□	GET_ACCOUNTS	22
□	READ_EXTERNAL_STORAGE	4
□	WRITE_EXTERNAL_STORAGE	4
□	ACCESS_WIFI_STATE	1
□	READ_PHONE_STATE	1
□	SET_WALLPAPER	1

In this app, it is used by ad library called "com.edealya", seemingly for ad tracking and targeting, quote:

“eDealya enables marketers to respond to social intent with an in-context, on-time, and relevant mobile advertisement.”

eDealya



New York, NY 10014

Just played the worst 9 holes of my life! #Help

17s

Target mobile inventory by leveraging social signals...

eDealya enables marketers to respond to social intent with an in-context, on-time, and relevant mobile advertisement.

As customers spend an increasing amount of time on their smartphones and tablets, advertisers shift more dollars into mobile advertising in hopes of finding their desired audience. However, with the ever-growing supply, advertisers find it extremely difficult to target their desired audience.

eDealya was developed to enable brands to leverage social signals and apply them in their mobile campaigns leading to superior results roughly 5x the industry average.

OnCore GOLF

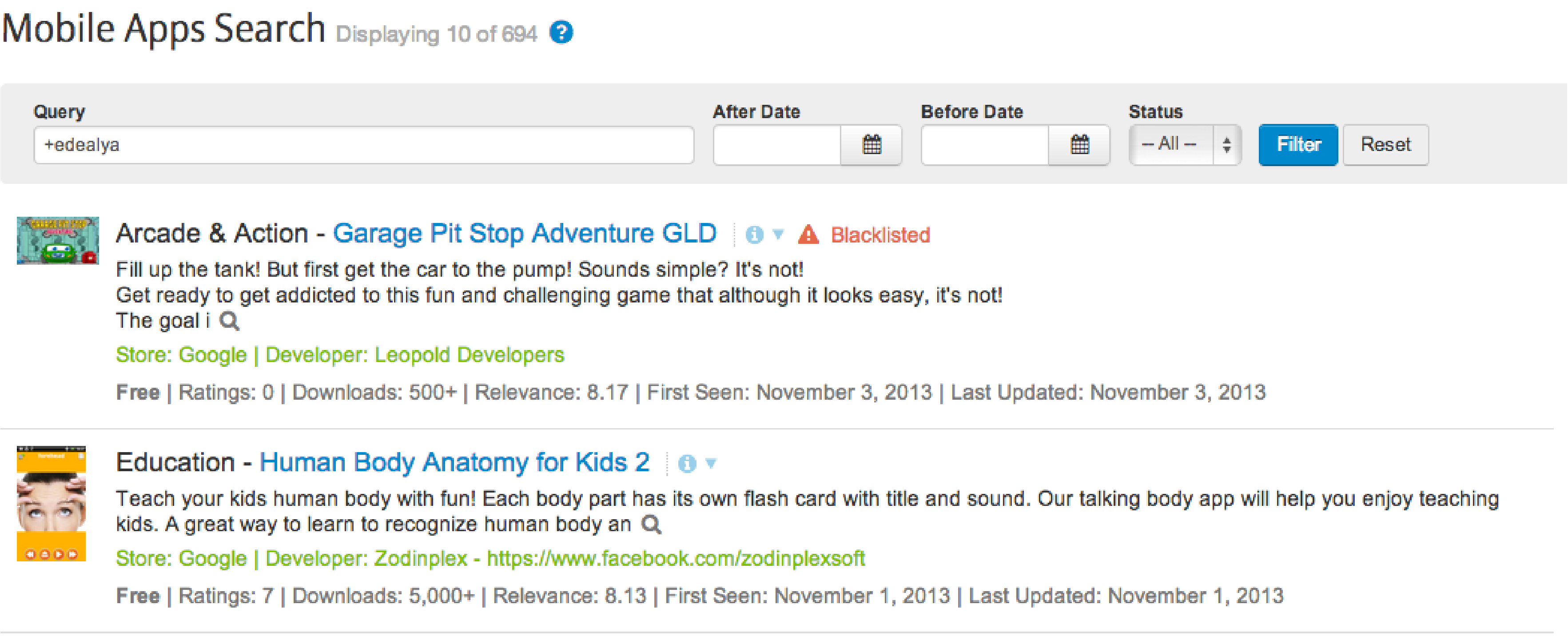
YOU JUST BECAME A BETTER GOLFER.

Results

eDealya performs on average at a 5.7% CTR on mobile, in-app display on a CPM model resulting in an average CPC of a mere $0.04.

Reference: eDealya Website - https://www.e-dealya.com/wp-content/uploads/2013/07/eDealya-One-Pager-v4.3.1.pdf

694 more eDealya Apps



Mobile Apps Search Displaying 10 of 694

Arcade & Action - Garage Pit Stop Adventure GLD ⚠ Blacklisted

Fill up the tank! But first get the car to the pump! Sounds simple? It's not!
Get ready to get addicted to this fun and challenging game that although it looks easy, it's not!
The goal i

Store: Google | Developer: Leopold Developers

Free | Ratings: 0 | Downloads: 500+ | Relevance: 8.17 | First Seen: November 3, 2013 | Last Updated: November 3, 2013

Education - Human Body Anatomy for Kids 2

Teach your kids human body with fun! Each body part has its own flash card with title and sound. Our talking body app will help you enjoy teaching kids. A great way to learn to recognize human body an

Store: Google | Developer: Zodinplex - https://www.facebook.com/zodinplexsoft

Free | Ratings: 7 | Downloads: 5,000+ | Relevance: 8.13 | First Seen: November 1, 2013 | Last Updated: November 1, 2013

Your mobile footprint isn’t a static environment

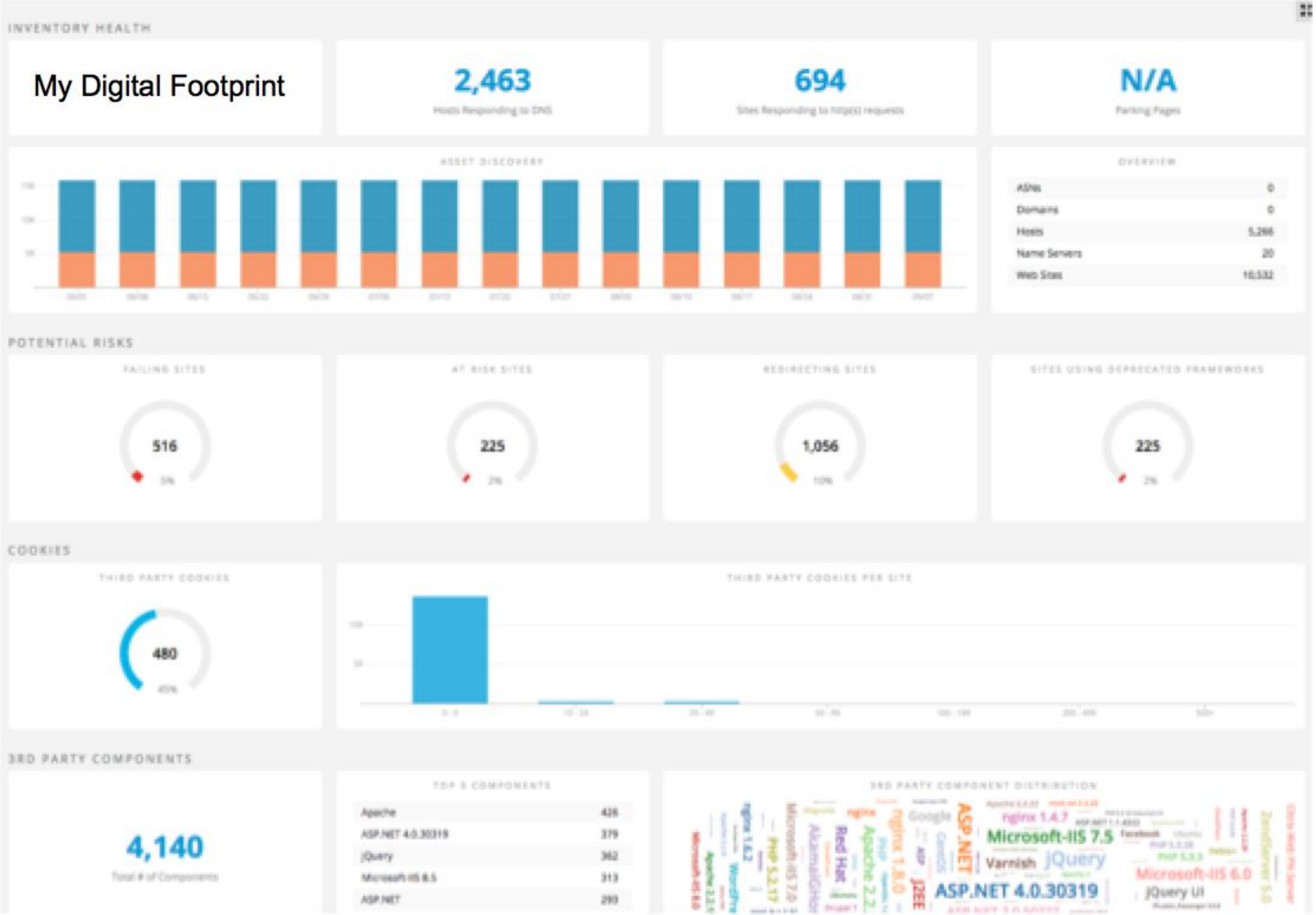
Mobile App Monitoring:

- Expired App Version
- Modified Legitimate App (Copycat)
- Non-Standard App Posting
- Missing Privacy Policy / Legal Notice
- Risky App Permissions
- Blacklisted App

Start with out of the box policies

Extend to customer specific policies

Pulling it all together



INVENTORY HEALTH

My Digital Footprint

2,463
Hosts Responding to DNS

694
Sites Responding to http(s) requests

N/A
Parking Pages

ASSET DISCOVERY

OVERVIEW

ASNs	0
Domains	0
Hosts	5,266
Name Servers	20
Web Sites	10,532

POTENTIAL RISKS

FAILING SITES
516
5%

AT RISK SITES
225
2%

REDIRECTING SITES
1,056
10%

SITES USING DEPRECATED FRAMEWORKS
225
2%

COOKIES

THIRD PARTY COOKIES
480
45%

THIRD PARTY COOKIES PER SITE

3RD PARTY COMPONENTS

4,140
Total # of Components

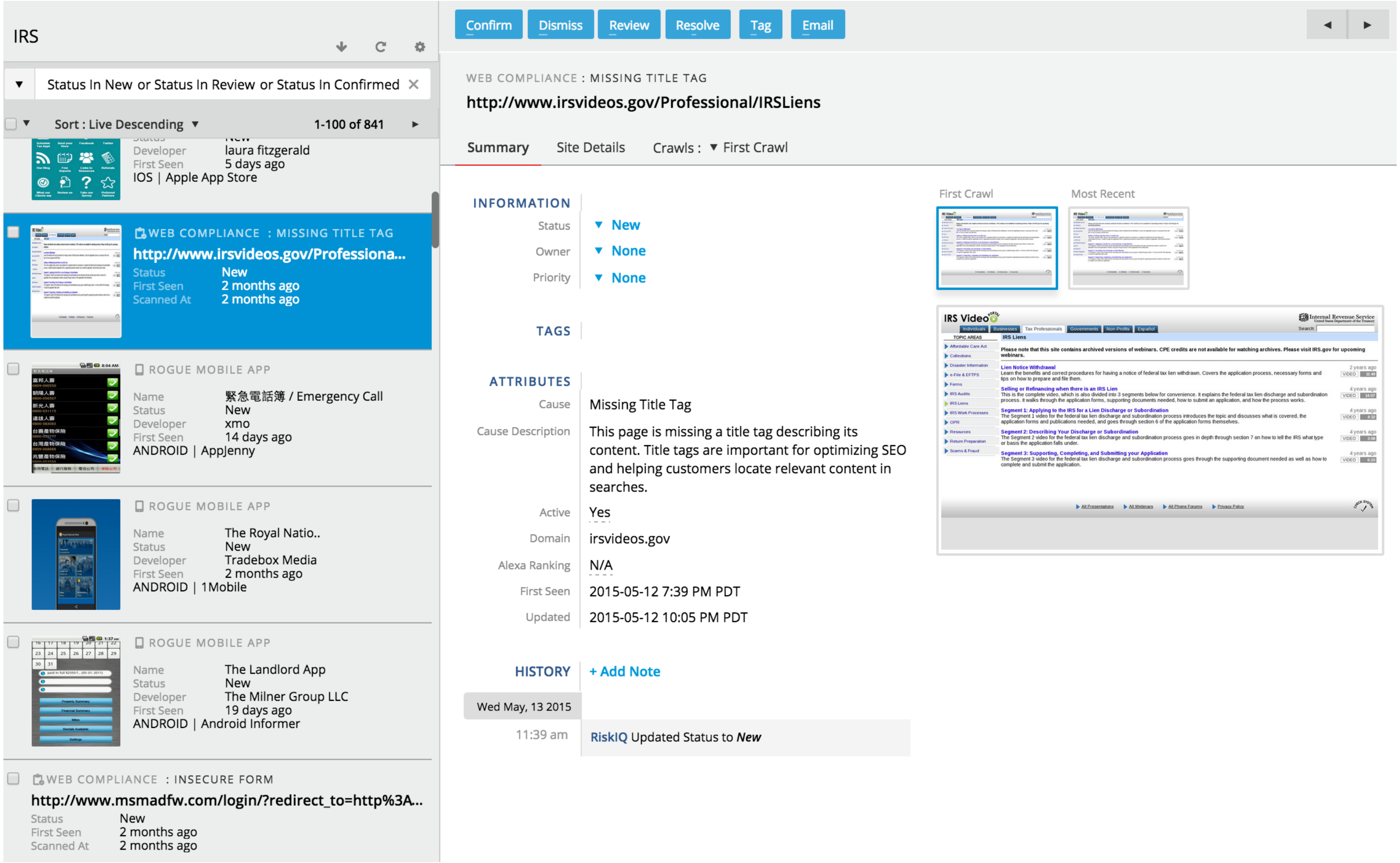
TOP 5 COMPONENTS

Apache	426
ASP.NET 4.0.30319	379
jQuery	362
Microsoft-IIS 8.5	313
ASP.NET	293

3RD PARTY COMPONENT DISTRIBUTION

RISKIQ

Providing actionable data



IRS

▼ Status In New or Status In Review or Status In Confirmed ✕

□ ▼ Sort : Live Descending ▼ 1-100 of 841 ▸

Developer laura fitzgerald
First Seen 5 days ago
IOS | Apple App Store

□ WEB COMPLIANCE : MISSING TITLE TAG
http://www.irsvideos.gov/Professiona...
Status New
First Seen 2 months ago
Scanned At 2 months ago

□ ROGUE MOBILE APP
Name 緊急電話簿 / Emergency Call
Status New
Developer xmo
First Seen 14 days ago
ANDROID | AppJenny

□ ROGUE MOBILE APP
Name The Royal Natio..
Status New
Developer Tradebox Media
First Seen 2 months ago
ANDROID | 1Mobile

□ ROGUE MOBILE APP
Name The Landlord App
Status New
Developer The Milner Group LLC
First Seen 19 days ago
ANDROID | Android Informer

□ WEB COMPLIANCE : INSECURE FORM
http://www.msmadfw.com/login/?redirect_to=http%3A...
Status New
First Seen 2 months ago
Scanned At 2 months ago

Confirm | Dismiss | Review | Resolve | Tag | Email ◀ ▶

WEB COMPLIANCE : MISSING TITLE TAG
http://www.irsvideos.gov/Professional/IRSLiens

Summary | Site Details | Crawls : ▼ First Crawl

INFORMATION
Status ▼ New
Owner ▼ None
Priority ▼ None

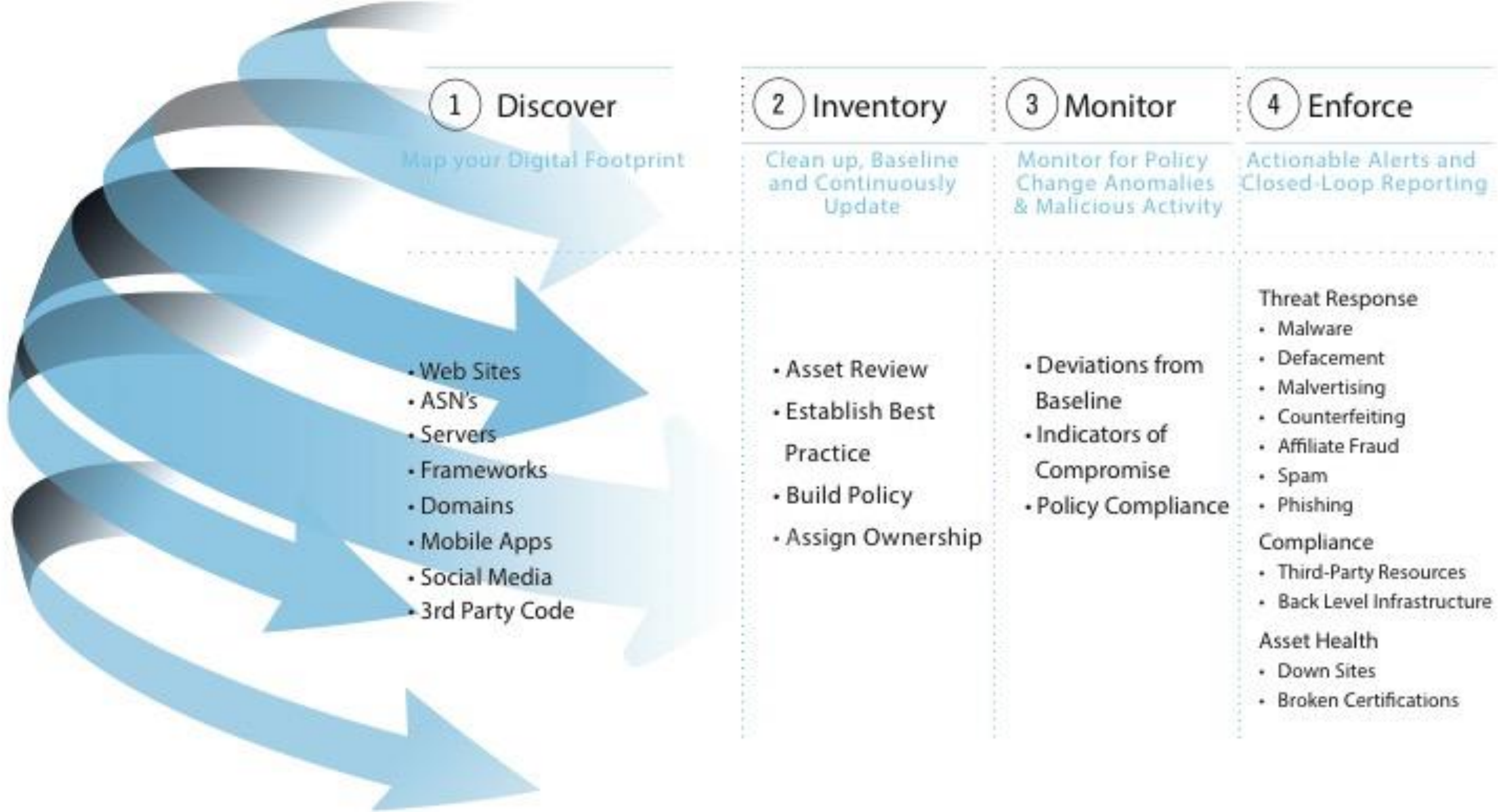
TAGS

ATTRIBUTES
Cause Missing Title Tag
Cause Description This page is missing a title tag describing its content. Title tags are important for optimizing SEO and helping customers locate relevant content in searches.
Active Yes
Domain irsvideos.gov
Alexa Ranking N/A
First Seen 2015-05-12 7:39 PM PDT
Updated 2015-05-12 10:05 PM PDT

HISTORY + Add Note
Wed May, 13 2015
11:39 am RiskIQ Updated Status to *New*

First Crawl | Most Recent

RiskIQ digital footprint approach



1 Discover

Map your Digital Footprint

- Web Sites
- ASN's
- Servers
- Frameworks
- Domains
- Mobile Apps
- Social Media
- 3rd Party Code

2 Inventory

Clean up, Baseline and Continuously Update

- Asset Review
- Establish Best Practice
- Build Policy
- Assign Ownership

3 Monitor

Monitor for Policy Change Anomalies & Malicious Activity

- Deviations from Baseline
- Indicators of Compromise
- Policy Compliance

4 Enforce

Actionable Alerts and Closed-Loop Reporting

Threat Response

- Malware
- Defacement
- Malvertising
- Counterfeiting
- Affiliate Fraud
- Spam
- Phishing

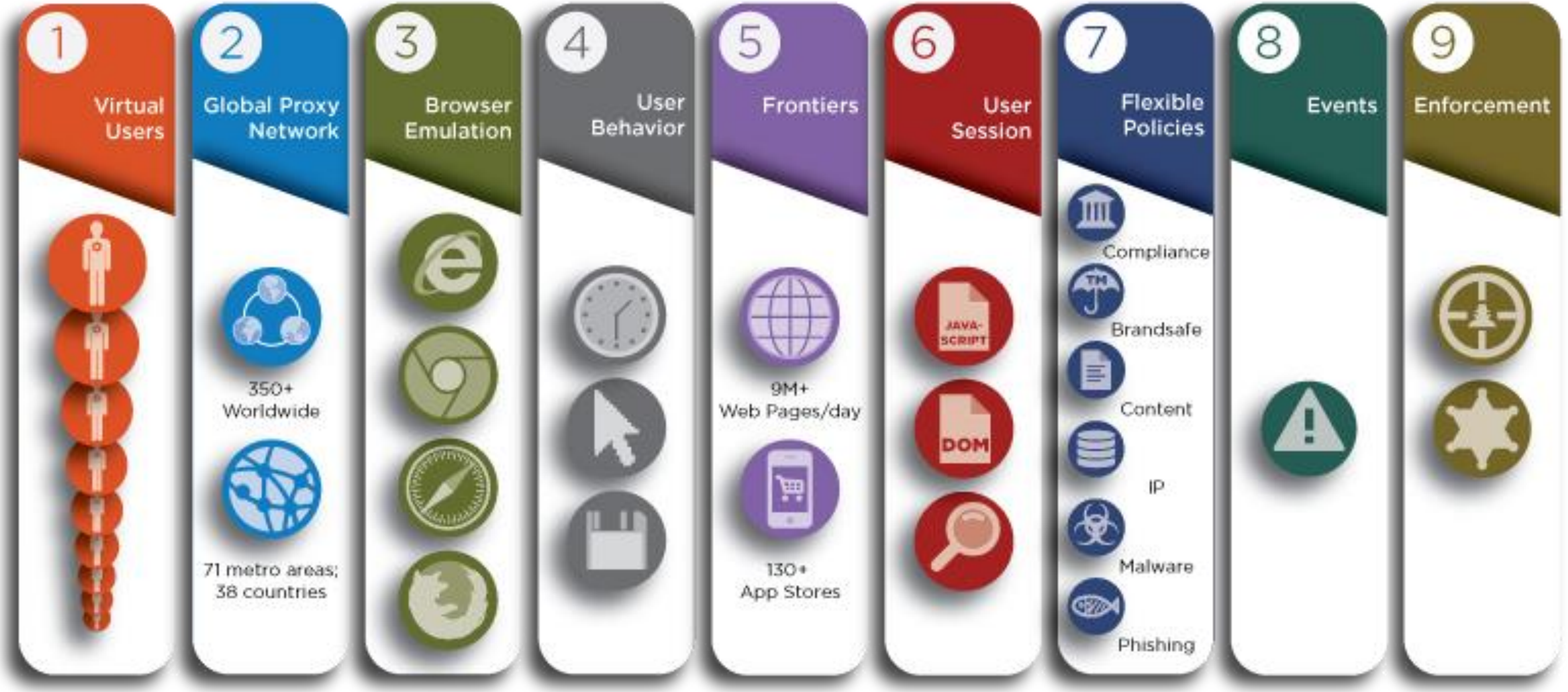
Compliance

- Third-Party Resources
- Back Level Infrastructure

Asset Health

- Down Sites
- Broken Certifications

How we do it


1
Virtual Users
2
Global Proxy Network
350+ Worldwide
71 metro areas; 38 countries
3
Browser Emulation
4
User Behavior
5
Frontiers
9M+ Web Pages/day
130+ App Stores
6
User Session
JAVA-SCRIPT
DOM
7
Flexible Policies
Compliance
TM
Brandsafe
Content
IP
Malware
Phishing
8
Events
9
Enforcement

Interested in knowing more?

till@riskiq.net

RISKIQ™

KNOWING IS THE BEST DEFENSE™