Contents

[3] Introduction

[6] Executive Summary

[7] Key Learnings

[8] "Data in the Wild"

[9] Curated Data: Verified & Attributed

[14] The year of the Accidental Exposure

[24] Conclusion

[27] Definitions

[29] About 4iQ
Introduction

Media attention to data breaches is nearly ubiquitous. Despite the constant drum-beat, it's difficult to appreciate the aggregate scale of privacy violations. A hundred thousand passwords lost here. A million social security numbers exposed there. But where do they end up? What about the unreported or undiscovered breaches? Is there any way to understand the sum of so many disparate parts?

Now, the answer is yes.

Using proprietary platforms, 4iQ continually monitors and manually hunts the Surface Web, Social Media, Underground Communities, Black Markets and the Deep and Dark Web for identity records exposed in data breaches. And the picture is not pretty.

In 2017 alone, 4iQ identified and verified more than 3 billion identity records, which represents an increase of more than 64 percent over 2016. The 3 billion records were curated from more than 8.7 billion raw records stemming from nearly 3,000 unique breaches 4iQ discovered.

The volume of private information dumped onto the web, where it can be exploited by bad actors, has grown nearly exponentially. Exposing private information for illicit gain is not a new phenomenon. Even before the Target and Home Depot breaches of 2013/2014 forced terms like “malware” and “personally identifiable information” into the average American’s lexicon, cyber criminals were on the lookout for ways to steal and sell private information.

Over the years, however, the numbers of records per incident have gone from tens of thousands to millions and even – like in the case of Yahoo – billions. Likewise, the quantity of breaches per year has increased.

A worry once reserved for the largest institutions is now a reality for even the smallest companies including law firms, accountants, doctors’ offices and other organizations. Cyber criminals attack without prejudice, giving rise to the phrase, “It’s not if you’ll be breached, it’s when.”

With the flood of exposed records, identity and credential trading have flourished in underground communities and the dark web.

To be sure, the sheer volume of data stored online is part of the equation. The more information available, the more likely some of it will be stolen, especially as cloud computing becomes the modus operandi in many industries. But criminals’ penetration, extraction and utilization methods have also evolved.

Techniques like credential stuffing – breaking into accounts with reused passwords – put users at risk for complete account takeovers, which in turn opens their employer to lateral attacks.
Simultaneously, organizations trusted with private information have mismanaged their security by failing to patch known vulnerabilities, trusting information to third-party vendors, inadvertently publishing files or simply storing information on unsecured, public databases. The latter problem has become so widespread that 2017 may become known as the year of accidental exposures.

Anonymously accessible servers provided criminals with unfettered access to billions of files, including health records, corporate documents and even security camera streams. Many of the databases remain unsecured today.

The following report is a deep-dive into the contents, sources and exposure methods of more than 8.7 billion raw records.

Whereas other reports typically consider only data available from public disclosure and media reports, 4iQ discovered each of these records in open sources, through its proprietary intelligence platforms.

Some were newly exposed in 2017, others resurfaced from old breaches, and still others were fakes or duplicates.

Collecting, analyzing and understanding the data allows us to better understand the risks faced by companies and individuals alike. By knowing where we are today we can better prepare for the threats of tomorrow.
1.1 KEY FINDINGS

Breaches With Identity Records
2,940 Curated from 3,525 Raw Breaches

Identity Records Breached In 2017
3,007,379,870 Curated from 8,700,000,000 Raw

64% increase over 2016

Where Raw Identity Records were Found
44% Underground 56% Accidental

FTP Servers Leaking PII
188,916 Servers with 2,100,000,000 Documents

69% increase

3X increase

MongoDB Servers Leaking PII
19,716 Servers; 4,900,000,000 Raw Identity Records
Executive Summary

This report is based on breaches found in 2017 from open sources, using automated crawlers and subject matter experts monitoring the Surface Web, Social Media, Underground Communities, Black Markets and the Deep and Dark Web.

Unlike some reports that track breaches that have been reported to regulators, by the media, or referenced in public sources, this data is from open sources and known to be exposed and accessible to bad actors.

4iQ authenticates and verifies the data to understand more about the nature and size of risks consumers and companies face, and alerts the impacted parties so that they can mitigate those risks.

To compile this report, we analysed the:

- Number of breaches
- Number of individuals impacted
- Authenticity of the data
- Countries affected
- Impact of accidental exposures

What’s Not in this Report

This report does not include breaches - that may have made headlines - if the data was not found by our team, in open sources.

It is important to note that evidence of a breach may not be seen for some time. That doesn’t mean that the information isn’t compromised; in fact, we acknowledge that by focusing only on the information we know to be openly accessible, we are significantly underestimating an already serious risk.
Key Learnings

Before we dive into the numbers, let’s take a look at the top breaches reported in the news in 2017.

1. **December 2017** - A single database of 1.4 Billion credentials (username and clear text password pairs) aggregated from 252 previously known breaches like Exploit.in and Anti Public, as well as 133 additional breaches, was discovered.

   The discovery of the Trove gives us new understanding of the potential risk and impact of aggregated breach data. The Trove is an interactive database that allows for fast access and searching for clear text passwords from more than 380 unique breaches. To the extent data in the Trove is accurate (read the 4iQ “Insights into the 1.4 Billion Clear Text Credentials Trove” report for a more in-depth examination), cyber criminals with access to this database are now able to execute attacks on individuals and companies faster and more efficiently than ever before.

2. **RNC June 2017** - An unsecured Amazon S3 bucket managed by a data firm exposed 198 Million U.S. voter data records (PII, party affiliation, etc.) in the largest known breach of voter information ever reported.

   Not only does this breach serve as a reminder of the types of sensitive personal information that can be impacted, it serves as a poignant example of the potential impact of accidental exposures. In this case, the mere failure of implementing proper security measures for a database stored on an external server put personal information for 198 million registered voters at risk.

3. **Equifax July 2017** - Cybercriminals hacked one of the nation’s largest credit bureaus and stole sensitive credit score data (Social Security numbers, credit card numbers and other personal information) of 145 Million U.S. and Canadian citizens.

   The Equifax breach was one of the most highly publicized of the year, and provided a couple key of insights. First, it proved that even the companies that are perceived as being the most secure by consumers can fall victim to data breaches. The risks are evolving and cyber criminals are actively targeting companies that hold our most sensitive information.

   Second, the breach is a headline grabbing example of just how large the impact on a company can be, not just in terms of records exposed, but business losses due to loss in customer confidence and damage to reputation.


   This breach demonstrates how mistakes or vulnerabilities of third party vendors and supply chain partners can result in data losses for companies and organizations. While this was an accidental exposure - a breach attributed to human error or inadequate security measures - the impact was significant for 105 million people.
To provide perspective on the data and analysis presented in this report, we first looked at our collection of raw identity records - data exposed and shared in open sources, by hackers, fraudsters, and cyber criminals. This provided us with broad visibility of what’s out there, but not necessarily an indication of the validity or accuracy of the data.

**Raw Identity Records**

In 2017, we saw an increase of 182% in raw identity records discovered by our team, compared to 2016. There are two primary reasons for this significant increase.

First, we continue to see an increase in the number and size of breaches that impact personal data, including usernames and passwords and other sensitive and confidential information. In underground communities, these breaches add up to 3.8 billion, or 44%, of the 8.7 billion raw identity records identified in 2017.

The second is the explosion in the number of accidental exposures, caused by lapses in security measures, for example, that result in data being openly accessible to third parties. These errors resulted in the exposure of 4.9 billion raw identity records, or 56 percent of identity records exposed last year. To look deeper into the growing prevalence of accidental exposures, we have included specific analysis in Section 6 of this report.
While the number of raw identity records accumulated provides insight into the sheer volume of data points out there, it is not the best indicator of overall risk. This is because not all of the data gathered is authentic or unique.

Some cyber criminals collect and compile breach corpses from multiple sources into a single database, resulting in duplicate data and an inflation in file size. In other cases, hackers seeking notoriety may fill documents with fake credentials or information that poses no real risk at all.

To more fully understand the risk and help protect digital identities, 4iQ uses an industry-leading process that not only gathers data but verifies it and assigns it a risk score.

Our process begins by implementing a combination of automated crawlers and subject matter experts to hunt for data leaks, accidental exposures, and dumps containing credentials and other personal information.

After we gather the raw data, our next step is to analyze the details. 4iQ has machine learning algorithms that quickly identify real, sensitive data, remove duplicate records and redundant information and normalize the information for further analysis.

The breaches then undergo a verification process where our analysts and experts use numerous research and investigation methods to make sure the domain and information are real and valid.

Once a breach is verified, the 4iQ platform calculates a risk score based on a number of variables such as type of attributes, date, and strength of password. The system then sends alerts so that action can be taken to change passwords and prevent attacks like account takeover, identity theft or identity fraud.
In 2017, we analyzed more than 3,525 “breach corpuses” and found that 2,940 of them were authentic. The others were either duplicates from other breaches (like Antipublic, Exploit.in, memoraleak, etc.) or were fake. In other words, the curated data revealed that identity records from close to 3,000 breaches were available to bad actors at some time or another. That’s equivalent to 245 breaches every month, or eight breaches every day.

2,940 Curated Breaches Found in 2017

245 every month

8.05 every day

5.2 GEOGRAPHIC DISTRIBUTION OF BREACHES

The following map represents the total number of curated breaches we detected in 2017. The percentage of breaches affecting each continent are included, as well as percentages for each of the top five countries affected in each continent.
Top 5 Countries Affected Based on Number of Records

While the number of detected breaches is insightful, the size of the breach and the number of identities affected is more important.

Identities in the United States represented 40 percent of all curated records detected in breaches - that’s almost twice the number of identities impacted in China, the next most affected country - while the top five countries affected accounted for more than 80 percent of all identities affected.

Out of 8.6 Billion raw records found, we added over 3 Billion curated records to our data lake that were found in close to 3,000 curated breaches. This represents a 64% growth from 2016. We can attribute that growth to the sheer number of people connecting and engaging online, the increasing amount of organized cyber criminal activity, as well as the increasing frequency of accidental exposures, which we will look at in more detail later in this report.
The infographic below represents the type of exposed personal information, or attributes, that we look for every day. While not all of these can be found in every breach or record, each piece is valuable to cyber criminals, and the more data they collect on an individual, the more valuable each set becomes.

**Personal Data Attributes**

**BANK INFORMATION**
- Income Tax Number
- Bank Account Number
- Iban
- Bank/Credit Card Number

**IDENTIFIABLE INFORMATION**
- Passport Number
- Drivers License
- Social Security Number
- National Id Number

**MEDICAL INFORMATION**
- Medical Insurance Provider
- Medical Insurance Number
- Insurance Account Number
- Insurance Provider

**PERSONAL INFORMATION**
- Name
- Username
- Password
- Surname
- Phone Number
- Email
- Date Of Birth
- Home Address
- Mother’s Maiden Name

**BUSINESS INFORMATION**
- Company
- Domain
- Brand

Of the raw identity records we analysed, a significant number contained emails and passwords.
5.5 CURATED BREACHES BY INDUSTRY

- **41.48%**
  News, Media, Entertainment

- **15.61%**
  Social and Dating

- **12.88%**
  eCommerce

- **7.02%**
  Services Providers

- **4.51%**
  Professional and Business Tools and Services

- **4.16%**
  Technology

- **3.78%**
  Education

- **3.28%**
  Healthcare

- **3.12%**
  Government

- **2.04%**
  Adult

- **1.27%**
  Hacking

- **0.6%**
  Financial and Banking

© 2018 4iQ, Inc. All rights reserved.
The Year of Accidental Exposures

4iQ defines an accidental exposure as a data breach that can be attributed to human error or inadequate security measures. The good news about these types of breaches are that they are largely preventable. But unfortunately, we cannot secure what has already been compromised.

2017 may go down in history as the year of Accidental Exposures.

In recent years we’ve heard a lot about the prevalence of cyber issues being the result of human error. Often, people are referring to lost electronic devices or documents, sending information to the wrong person or organization, or other oversight that may cause information to be shared with the wrong party.

But, in 2017 there was a proliferation of new types of accidental exposures - ones where adequate security measures are available but not utilized. Two specific types of these exposures took off last year: breaches of organizations that improperly utilized anonymous FTPs and default settings associated with open datastores and devices, like MongoDB, Amazon S3 buckets, misconfigured websites, etc.

6.1 ANONYMOUS FTPs KEEP EXPOSING MILLION OF IDENTITIES

Anonymous FTP Servers

Anonymous FTP Servers are set up in such a way that anyone can log on to the server using an anonymous username and without a password. Once in the server, the user is able to search for and download data. These public folders are convenient when sharing large files with people outside your organization.

However, companies and individuals sometimes misconfigure FTP Servers or unintentionally put private data in these public folders using this anonymous-mode, thus publishing sensitive files to the Internet.

Anonymous FTP ports keep exposing millions of documents, we saw a 69% increase in 2017.
FTP Servers Exposed In 2017

Our scanners analyzed 2.6 million FTP servers in 2017. Of those devices, 188,916, or more than 7%, were not secured, leaving content on the server open to being accessed anonymously by anyone.

100%
2,644,324
Total FTP servers scanned in 2017

93%
2,455,408
Number of FTP servers found to be secure

7%
188,916
Unsecured FTP servers open for anonymous access

How Many Files?

We estimate that there are currently 21 Billion files exposed in unsecured FTPs.

Approximately 2.1 Billion, or 10%, are exposing personal information.

File Size

Approximately 272 Million GB of data was leaking from open FTPs.

Out of 188,916 anonymous FTPs, over one third were larger than 1GB
Of the 2.1 Billion documents exposing identity information from FTP servers, nearly 35% contained financial data, 19% contained insurance information, 16% contained health records, and 17% contained usernames and passwords.
Examples Of Exposed Documents Found

Apart from identities, anonymous FTP servers are exposing corporate information including backup files, databases, and confidential corporate documents. Below are some examples of documents exposing financial information, health records, Insurance documents, etc.

HEALTH INSURANCE CLAIM FORM
APPROVED BY NATIONAL UNIFORM CLAIM COMMITTEE 2605

READ BACK OF FORM BEFORE COMPLETING & SIGNING THIS FORM.

12. PATIENT'S OR AUTHORIZED PERSON'S SIGNATURE: I authorize the release of any medical or other information necessary to process this claim. I also request payment of benefits either to myself or to the party who accepts assignment below.

SIGNED SIGNATURE ON FILE

SPRAIN: WRIST

A sprain is an injury to the ligament or capsule that holds a joint together. There are no broken bones. Most sprains take about three to six weeks to heal. If the ligament is completely torn (severe sprain), it can take months to recover.
Know your Customer

Questions to ask the Customer
(Private Individuals)

Account No. 
Representative 
Rel. Manager 
Form flow → 1 Representative 2 Account Officer 3 Branch Manager 4 Compliance 5 CIF

Client’s occupation or principal line of business (→ see example sheet)

is a lawyer specialized in labor subjects, he has been living in , where he initiated with his legal practice.

is partner of a consultant firm named , group of professionals dedicated to the fiscal, accounting and legal consultant(s) office.

He also have a firm at with more than 25 attorneys dedicated to give legal assistance in labor matters, have clients like

Since started a TV Cable service in 25 small cities arround , those earlier operators grow in a new market of TV options, and get a lot of subscribers. In , started the sale of its businesses, to a company named , the company is characterized being a company of national service cover in the scope of Telecommunications, with more than 750 thousand subscribers of . This company has a very aggressive growth plan and has been interested in acquiring companies. He is settling the rights and obligations of a concession serve of . The total value of the 25 business is worth in dollar.
IoT video intercoms in a Korean City residential building captured photos of the guests with the date and time of entry, the apartment they were visiting and other information. This data was exposed in the deep and dark Web, likely by accident.
Exposed FTP Servers By Country

North America
- United States 94.46%
- Canada 5.18%
- México 0.41%

South America
- Brazil 61.35%
- Chile 16.83%
- Argentina 12.73%
- Colombia 5.87%
- Venezuela 3.23%

Europe
- Germany 63.88%
- France 7.64%
- United Kingdom 7.02%
- Netherlands 3.30%
- Russia 2.57%

Asia
- China 31.43%
- South Korea 26.03%
- Hong Kong 18.13%
- Taiwan 10.79%
- Japan 4.68%

Oceania
- Australia 88.03%
- New Zealand 11.97%

Top 10 Countries with Exposed FTP Servers

<table>
<thead>
<tr>
<th>Country</th>
<th># Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>93,298</td>
</tr>
<tr>
<td>Germany</td>
<td>35,649</td>
</tr>
<tr>
<td>China</td>
<td>8,185</td>
</tr>
<tr>
<td>Republic of Korea</td>
<td>6,780</td>
</tr>
<tr>
<td>Canada</td>
<td>5,113</td>
</tr>
<tr>
<td>Hong Kong</td>
<td>4,722</td>
</tr>
<tr>
<td>France</td>
<td>4,264</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>3,918</td>
</tr>
<tr>
<td>Taiwan</td>
<td>2,810</td>
</tr>
<tr>
<td>Netherlands</td>
<td>1,840</td>
</tr>
</tbody>
</table>

FTP servers are associated with IP addresses. Although these IP addresses may or may not map directly to the location of a company or server, this map provides a view as to where FTP servers may be leaking personal data.
In 2017, there was a big increase in attacks on MongoDB servers due to default settings that allowed remote access without authentication. The number of breaches due to open MongoDB devices alone (not including open FTP servers or S3 buckets) almost doubled from 2016 to 2017.

In November 2017, MongoDB introduced a localhost network default binding in version 3.6, to ensure that MongoDB ports will no longer be exposed by default. As a result, the number of open MongoDBs is decreasing and, in just the first first quarter of 2018, we have already seen a 18% decline.

This is great news, but these exposure incidents should have raised awareness and served as a warning to companies about risks that must be managed when moving to the cloud and outsourced hosting providers.

Unfortunately, password protection in MongoDB is still not enforced by default and we are still seeing around 30,000 non-password protected MongoDB servers.

October 2017 Scan of MongoDB Servers

After MongoDB version 3.6 was released, in October 2017, we found around 87,231 open MongoDB servers. Out of these, over 50,620 could be accessed without credentials, and around 19,716 MongoDB servers were leaking sensitive PII.

87,231
MongoDB Servers

58%
or 50,620 MongoDB servers, were not secured and could be accessed anonymously.

22%
or 19,716 MongoDB servers, contained identity information.
Open Device Breakdown for MongoDB

There was a **50%** increase in MongoDB servers that were **not secured**.

**40%** of unsecured MongoDB servers contained **sensitive PII**.

**11.2%** of the MongoDB servers linked to **Open Cloud storage** resources resulting in even more leaks of data from Amazon S3, Azure Storage and Google Cloud.

**Quick Comparison from 2016 to 2017**

We found **three times more** raw identity records exposed due to MongoDB misconfigurations than the year before. MongoDB is often used to store not only login credentials and customer lists, but also spam email lists.

**In 2017, we detected 4.9 Billion Raw Identity Records** from leaking MongoDB servers vs **1.6 Billion** in **2016**
6.4 MONGODB BREACHES BY LOCATION

MongoDB servers are associated with specific IP addresses. Although these IP addresses may or may not map directly to the location of a company or server, the map below shows which continents may have the most MongoDB servers leaking personal data.

Percentages in each continents are % of MongoDB servers exposed and Percentage in each country is % of MongoDB servers in that continent.
Conclusion

New data dumps and breach corpuses containing personal information are constantly being exposed and we often have little insight into how information is leaked and whether it is accurate. However, by analyzing these breaches, we can gain a better understanding of the risks companies and individuals face and help mitigate these new and ever evolving threats.

Compromised passwords put companies at risk from automated credential stuffing attacks and account takeover.

People often reuse passwords and criminals know this. They automatically test passwords exposed in one account to try to break into other accounts - a technique called credential stuffing (OWASP Automated Threat (OAT) Identity Number OAT-008). While this may seem inefficient, Credential Stuffing actually has a success login rate of 0.01% - 0.02%, according to OWASP.

- To prevent account takeover, we recommend that consumers don’t reuse passwords, use strong passwords, password managers, and consider subscribing to Identity Theft Protection Services that include insurance. Companies should use use multi-factor authentication among other

- NIST publication 800-63B recommends that companies check user passwords and make sure that they have not been exposed in a previous breach corpus.

- Companies should monitor corporate credentials and force password resets if a corporate email is found exposed in a breach. The same standards should also be extended to customer emails, by forcing a password reset or implementing dynamic risk based access control to exposed user information.
Identity Theft is getting more sophisticated each day.

As technology continues to evolve and become more sophisticated, so do the methods used to compromise it. In 2017 we saw an increase in sophisticated attacks, including the use of synthetic identities and exposure of children’s data.

- There has been an increase in synthetic identity attacks where fictitious identities are created by combining elements of real and fabricated identity information and used to open bank accounts, obtain legal documents (passports and driver’s licenses), etc. Synthetic Identity Fraud now accounts for 80-85% of all identity fraud in the US, according to the Federal Trade Commission.

- Another trend in synthetic identity fraud involves your children. Children’s SSNs are prime targets for criminals, as they are unlikely to discover that their identity has been stolen until they come of age and apply for credit. SSN breaches greatly increases the pool of identity components criminals can use. These bad actors mine “good credit scores” from these hacked and formed identities, open new accounts and raise credit limits before they disappear with the money.

Cyber criminals are after more than personal information and can lead to the compromising your whole organization.

Cyber criminals look for intelligence that allows them to exploit organizational weaknesses and even create large scale disruption. The intention is not always about identity theft or fraud, though the irony is that the intrusion could occur as a result of identity theft or compromised credentials. Stolen sensitive data can include healthcare records, social security numbers, birthdates, passport numbers, financial information, intellectual property, building plans, and more. That’s why it’s so important to educate and train employees about security, not only in terms of protecting their own identity, but also the impact it could have on the organization. It is important to remember that:

- Account takeover is a path to greater things. Even if it’s a personal account, criminals will steal confidential information to perform lateral attacks, acting like a door into your corporation.

- Using stolen identities, scam attacks like impersonated emails, phishing, or social engineering, can be used to gain further access.

- Companies should check exposure levels early in their customer interactions, for example, at account creation time or during call center verification, and require additional validation if the risk is found to be high.
Accidental Exposures continue to climb at a rapid rate.

In 2017 we saw an increase in accidental exposures, with a 3x increase of exposed identities (4.9 Billion) in open MongoDB exposures, as well as a 70% increase in FTPs exposing documents with sensitive data including ~34% financial documents, ~16% healthcare records and ~17% passwords. Here are a few steps that can be taken to help mitigate risk:

- Review and make sure file sharing services are properly configured, as they tend to contain more personal and sensitive data.
- Be sure to keep software updated at all times, new versions of the software could include security fixes, for example, ports that may be left open by default.
- Due to the growing IT Shadow and steady move to cloud, mistakes will continue to happen, leaving services and devices temporarily open. Companies need to continuously monitor their sharing services to detect data exposures as early as possible.
- We’re seeing an increase in APIs and Web applications exposing sensitive customer or company information. Organizations should review and test their APIs and Web applications to control abusive crawling that collects sensitive information.

PII is often exposed not from the company itself, but from breaches of third party vendors and supply chain partners.

With the proliferation of shadow IT, outsourcing and global supply chains, executive, employee, and customer PII is more likely to be exfiltrated from more vulnerable third parties. Audit reports that assess third party credential exposures can help companies understand the scope and source of the breach and measure this risk.
## Definitions

### Identity Records Defined

#### Identity Record

Identity Records are pieces of information, or identity attributes linked to a single individual that expose any type kind of personal identifiable information (PII). Each record typically includes a number of identity attributes related to the same person such as name, username, password, address, phone, etc.

#### Raw Identity Record

A Raw Identity Record is a record we find in the wild that has not been curated and validated. That means we could find exactly or partially the same information multiple times, or, even worse, the data could be fake.

#### Curated Identity Record

A Curated Identity Record is an Identity Record that has been validated to be authentic (not fake) and not duplicated (not exposed or seen in another data dump or breach corpus before).
What is an Incident?

4iQ defines an incident as an event when a company has a vulnerability but there is no confirmation of whether anything was stolen.

What is a Data Breach?

4iQ defines a data breach as a confirmed incident where credentials, personal, medical, financial or other records with sensitive data have been accessed or disclosed due to being hacked or leaked, either deliberately or by accident.

What is an Accidental Exposure?

4iQ defines an accidental exposure as a type of data breach that can be attributed to human error or inadequate security measures. Examples range from default or misconfigurations of anonymous FTP servers and cloud-based databases (e.g. MongoDB) to lost laptops, tablets or mobile phones that contain or provide access to sensitive information.
Back in 2005, driven by curiosity and passion for Open Source Intelligence, 4iQ co-founders started building OSINT+, a Unified Investigation Platform that supports multiple departments, objectives, missions and units. The Platform supports the full Intelligence lifecycle - data collection, fusion with internal sources, entity extraction and enrichment, dynamic taxonomies and data classification, to automatic linking, tracking, collaboration and generation of reports.

Meanwhile, in 2007, Julio Casal co-founded Alienvault, a company that went on to become a leader in Unified Security Management and Threat Intelligence. In 2011, Julio began to specialize in searching the Deep and Dark web for identity threats, discovering where to look for the freshest information in well-known and not commonly known sources. This resulted in the development of what is now the 4iQ Identity Threat Intelligence Platform.

Using the 4iQ OSINT+ Unified Investigation Platform together with the 4iQ Identity Threat Intelligence Platform, organizations can monitor risks to protect people, property, brand and other business assets from adversaries.

When we find breach incidents, we avoid disclosure of active vulnerabilities or open devices that are still leaking data. We first reach out to the security contacts of a company and if those are not listed, we use public contact information. If we get no response, we reach out to professionals in sites like Linkedin and Crunchbase and if there is still no response, we reach out on Twitter.

Our team uses an extensive verification process to determine that information in dumps is real, not duplicate or fake. We try to attribute the breach source and only report breaches when confidence levels are high. Each exposure alert sent to a consumer or company includes information on the breach and a risk rating of the potential impact of the exposure so that appropriate actions can be taken.

We acknowledge that this report is based on our findings, what we have seen and have been able to analyze. It is by no means a complete picture, simply our view and contribution to helping people and their companies protect themselves.