



Business challenge

To help consumers protect themselves from identity theft and related crimes, Intersections Inc. needed to rapidly analyze huge volumes of news articles, social media posts, geolocation and other digital data.

Transformation

Intersections Inc. chose IBM® Watson® to build an insight engine for its first-of-its-kind offering, Identity Guard. Now, with real-time insights into threats and individual risk profiles, the organization can proactively warn customers of potential problems before criminals can act.



Melba Amissi
Chief Operating Officer
Intersections Inc.

Results

3 seconds to dispatch alerts

tailored to individual risk profiles and providing specialized advice

≤16% drop in identity theft risk

for customers that take proactive action after receiving threat alerts

Helps businesses

attract and retain employees with identity protection features powered by AI

Intersections Inc.

Helping consumers avoid identity theft with real-time threat alerts powered by IBM Watson offerings

Based in Chantilly, Virginia, [Intersections Inc.](#) offers award-winning identity theft protection products and services to help consumers and businesses proactively safeguard their sensitive information against theft or compromise. Its offerings include the first identity protection solution with embedded Watson AI technologies for monitoring constantly changing digital data in real time. A global provider of identity risk management services, Intersections Inc. has more than 47 million customers and approximately 500 employees.

“Using the Watson platform, we have found a way to proactively work with consumers to help them take back their privacy and personal information.”

— Melba Amissi, Chief Operating Officer, Intersections Inc.

Share this



Preempting identity theft

Digital technologies have changed people's lives in a remarkably short time, including how they shop, socialize and bank. Unfortunately, the ease with which people now use mobile devices or go online to communicate and transact also significantly heightens their risk of identity theft. Never before have criminals been able to get hold of such vast quantities of once tightly protected information—including social security numbers, birth dates and passwords—and use it for fraudulent purposes.

Identity theft has risen dramatically since the late 1990s, when Intersections Inc. helped establish the identity and privacy protection industry by facilitating consumer access to their annual credit reports. Now, the company estimates that as many as 15 million Americans have their identities compromised every year. Melba Amissi, Chief Operating Officer (COO) of Intersections Inc., attributes the huge and rapid spike in identity theft to the birth first of e-commerce and then social media.

“Just prior to five years ago, our personal information was not really that exposed,” she explains. “When e-commerce took off in the early 2000s, companies from which we bought products and services

started collecting our data, including our name, address and payment details.” Soon after, she says, social media initiated the next upsurge in exposure, throwing open the door to a wealth of information about individuals, such as where they shopped and other habits and preferences. “Those two waves have made so much of our lives public and broadly collected and shared,” she says.

Grant Gelven, Product Development Scientist at Intersections Inc., agrees. “Our digital footprint has become so much more expansive,” he says. “It doesn't primarily consist of your name, address, social security number and birth date, which make up your identity in the classical financial sense. Now, you might use electronic payment methods 20 times a day, have half a dozen social media accounts, buy something online a few times a week. Each time you do that, it leaves a little piece of you behind. This is now what makes up your identity.”

And criminals seemingly help themselves to private information that businesses and organizations hold, leaving consumers feeling helpless to protect themselves. For example, in 2016 Yahoo! reported two major data breaches, including one in 2013 in which hackers gained access to the names, email addresses, account passwords and other personal data of all three billion users. In 2015,

criminals stole the data of 80 million American adults and children stored in Anthem Healthcare systems. And in 2017, Equifax suffered a data breach that potentially exposed the personal information of 145.5 million Americans, including their social security numbers.

Intersections Inc.'s executive team witnessed these disturbing trends and set out to help consumers avert fraudulent use of their personal data by helping them take precautions to prevent its theft. “In traditional credit monitoring, we're looking at events that occur relative to that specific set of financial data, and it's always after the fact that the notification occurs,” Gelven explains. “We wanted to engage and warn customers before their identities could be stolen.”

The leaders recognized that because individuals act in unique ways, they face unique risks. They sought to cater to this reality by giving customers specialized tools and personalized advice required to proactively protect themselves.

However, identifying specific threats pertinent to each individual and recommending appropriate actions based on multiple, ever-changing factors required new AI technologies. Specifically, the company needed the ability to rapidly monitor more than data from credit bureaus, public record monitoring companies and other providers, which makes up a

small percentage of available online data. It needed to also efficiently analyze massive amounts of less structured data, including news articles, social media posts and geolocation data.

The organization sought a flexible, open AI platform on which it could rapidly and continually develop new, personalized services to help consumers proactively protect themselves against financial and other crimes.

Protecting consumers with AI

Intersections Inc. selected IBM Watson offerings to build an insight engine for powering its [Identity Guard](#) service. The Watson toolset, which combines cloud-based cognitive search, machine learning, relevancy training, natural language processing (NLP) and query functions, outperformed multiple other open source solutions the company tested. “It came down to a matter of efficacy, accuracy and ease of use,” says Gelven. Using Watson offerings, Intersections Inc. built, tested and refined the Watson insight engine on the IBM Cloud™ platform over the course of approximately two years.

Now, the business offers consumers one of the industry's most comprehensive identity protection services, the first of its kind to capitalize on Watson AI technologies. The Identity Guard service provides several novel capabilities to help consumers and their families thwart identity fraud and misuse before it occurs. These capabilities include a personal risk-assessment score created using each customer's unique digital footprint. Customers can study their score as it changes over time to better understand how their online and offline activities affect their risk of identity theft.

In addition, a threat alert feature detects security incidents and notifies customers who have corresponding risk factors, all in real time. Intersections Inc. developed the feature's monitoring and notification pipeline with Watson offerings. IBM Watson Discovery News is one of four feeds the company uses to search and scan huge volumes of unstructured data, finding information related to potential identity threats, such as data breaches, point-of-sale (POS) malware attacks and software vulnerabilities. A public data set of pre-enriched news content, Discovery News analyzes and annotates millions of English language news and research articles and blogs from over 100,000 sources each day. The business also gathers information about emerging threats from other credible sources.

Next, IBM Watson Natural Language Understanding interrogates the data for concepts, sentiment, context and other details. It extracts critical pieces of information relevant to each customer using the organization's proprietary taxonomy, developed with IBM Watson Natural Language Classifier. The solution identifies which customers are at risk by comparing the extracted insights with individual risk profiles. It then immediately sends alerts to each at-risk customer, along with personalized tips the company's cybersecurity experts developed for stopping or mitigating the risk.

"If there has been a hack at a store you frequent or your bank, we give you the specific advice in the moments that the news breaks so that you can take action to reduce your risk back to normal as it relates to the breach," says Amissi.

The solution includes several other innovative features built using Watson. An ID verification alert system notifies customers when someone applies for credit, opens new accounts or accesses existing accounts using their personal information. An internet surveillance feature searches chat rooms, underground forums and "black market" sites for customers' social security, credit card and bank account numbers. And a social insights feature monitors customers' online images and offers recommendations for improvement.

Alerting users in seconds

Having adopted a Watson solution, Intersections Inc. reinforced its industry leadership and competitive advantage by giving consumers new, advanced ways to avoid identity theft and related crimes. "With Watson technology, we've built a solution that's like nothing else on the market," says Gelven. "Our service is like a radar, picking up potential threats before damage is done and providing advice to mitigate those threats. We offer our users comprehensive layers of protection they can't find anywhere else, the most novel and impactful of which is our threat alert system."

With the solution's threat alert feature, the company can now notify customers of evolving threats in as few as three seconds. Previously, it could only notify customers after their identity had been compromised, and it required 1 – 3 days to do so.

"In virtually seconds after a potential threat emerges, we can tell customers of the risk of that potential threat and help them stop the problem from happening before it actually happens. And I'm not talking about personal information being stolen. It's been stolen, whether at Anthem, Yahoo!, Equifax or elsewhere. I'm talking about the prevention of that information being misused for something nefarious," says Amissi.

"In a traditional credit monitoring scenario, consumers generally receive on average one or two after-the-fact alerts per year," adds Gelven. "Our users receive on average about 1 – 2 alerts of potential threats per week."

Relying on Watson to continually and rapidly process vast amounts of unstructured data, the company can now scan digital footprints that are up to 10 times larger than those covered by traditional monitoring solutions. As a result, it can acquire the timely insights needed to help customers safeguard their identities. The organization estimates that customers can reduce their risk of identity theft by as much as 16 percent by receiving the alerts and acting on the accompanying advice.

The advantages of using Watson AI technologies also extend to employers that offer the Identity Guard solution as part of their voluntary employee benefit plans. Having once again set new standards in identity protection, the company can continue to grow its network of business associates, which gain by offering a highly valued service to employees and their families.

Finally, the Watson offerings provide the business with a versatile, open AI platform on which it can continue to quickly develop and launch industry-leading services. For example, it plans

to soon introduce a feature allowing parents to monitor their children's social media feeds and receive alerts related to cyberbullying and other problems.

Amissi compares the organization's ability to offer timely, personalized identity protection advice with other specialized services consumers expect, such as for their healthcare and finances. "People want to have specialized advice involving their physical and financial health. Why would they not want to have dedicated advice around their privacy and identity health?"

"Using the Watson platform, we have found a way to proactively work with consumers to help them take back their privacy and personal information," she adds. "And in a way that is meaningful to them."

Solution components

- IBM® Cloud™
- IBM Watson® Discovery News
- IBM Watson Natural Language Classifier
- IBM Watson Natural Language Understanding
- With Watson™

Take the next step

To learn more about the IBM solutions featured in this story, please contact your IBM representative or IBM Business Partner.

The With Watson Program is a global client success initiative that can help accelerate your AI vision through exclusive access to Watson experts and education. With Watson, learn how to enhance your products and applications while growing the power of your brand. To find out more, visit us at: www.ibm.com/watson/with-watson/

Increase productivity with Watson.

© Copyright IBM Corporation 2018, IBM Corporation, IBM Watson, New Orchard Road, Armonk, NY 10504. Produced in the United States of America, July 2018. IBM, the IBM logo, ibm.com, IBM Cloud, IBM Watson and With Watson are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at ibm.com/legal/copytrade.shtml. The content in this document (including currency OR pricing references which exclude applicable taxes) is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates. The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions. It is the user's responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs. THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided. The Identity Guard solution is not an IBM product or offering. The Identity Guard solution is sold or licensed, as the case may be, to users under Identity Guard's terms and conditions, which are provided with the product or offering. Availability, and any and all warranties, services and support for the Identity Guard solution, is the direct responsibility of, and is provided directly to users by, Identity Guard. The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation. Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

