NuData Security
mastercard

Case study: How a major U.S. bank fights mass-scale account takeover attacks

NUDATA SECURITY

CASE STUDY: NUDETECT

As mass-scale attacks become more sophisticated, leading organizations are benefiting from behavioral biometrics to protect their most valuable assets. But how?

At a glance

Client: Top 10 U.S. bank

Size: 500 million logins monthly

Problem: Sophisticated account takeover attacks

Product implemented: NuDetect

Result: +99% fraud prevention accuracy, under 0.1% false decline rate

Who is the client?

Major U.S. bank

This major U.S. financial institution offers a wide range of services, including personal, business banking, insurance, corporate finance, and private banking. Their platforms and services have grown over the years making this bank the leader in the industry they are today. Evolving with the digital times, they offer web-based services and product-specific native apps. Along with this broad range of online services and access points comes the responsibility of impeccable security solutions to protect their number one asset: their customers.

NuData Security
mastercard

What was their problem?

This institution was onslaught with a daily stream of attacks that their solution at the time was not able to identify. The institution was relying on a coarse filter automation detection tool at the login that was letting attacks through.

The bank, with over 500 million legitimate logins monthly, was suffering constant account takeover attacks, that multiplied the volume of their regular traffic. The automation detection tool they were using had proven to be efficient at catching unsophisticated automated account takeover attempts. However, when bad actors realize their attacks are blocked it doesn't take them long to look for another way in; evolving the script ever so slightly to get their attack success rates back up again.

With a login attack success rate varying from 0.05% to 1.5%, account takeover losses were a hefty bottom-line problem for this institution. They decided to implement a solution that would not only stop simple-script attacks but also evolve along with them as they shift, no matter how sophisticated.

How does NuData solve the problem?

The best way to expose evolving sophisticated attacks is by leveraging multiple layers that can look at online traffic from a 360-degree angle. NuData's multi-faceted technology looks at hundreds of threats based on their location, IP, connection, behavioral signals, passive biometric patterns, and a consortium that compares these data points to billions of past recorded events.

Attackers are experts at dressing up like your legitimate traffic – they don't wear a black balaclava and striped shirt anymore – making a multi-layered solution crucial to block threats before they turn into fraud losses.

NuData deployed its solution to protect one of this institution's most sensitive placements: the login.

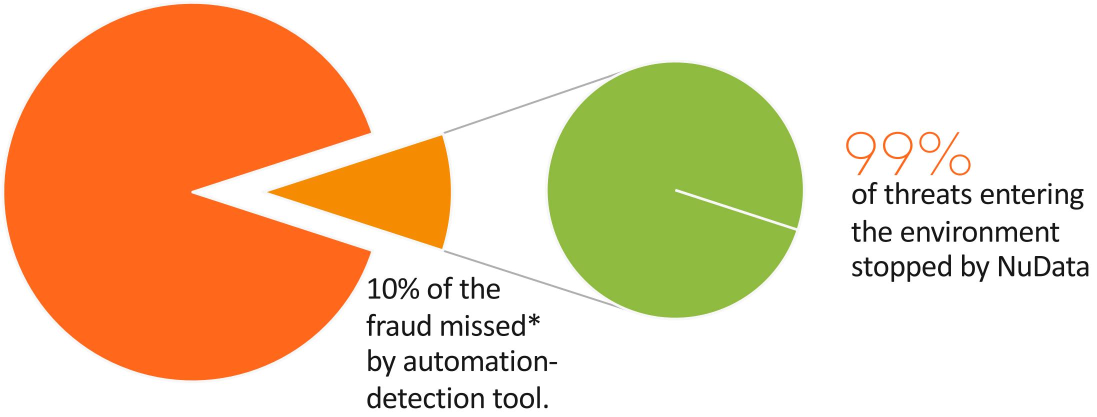
The NuData commitment

- Detect suspicious input patterns.
- Analyze individual behavior and overall traffic changes.
- Monitor subtle pattern changes in real time.
- Make module adjustments to block evolving attacks as they happen.
- Trigger interdictions based on the bank's requirements.
- Analyze fraudulent behavior to prevent future attacks.

First results

After implementing NuData the client found out that the existing automation detection tool was missing 10% of the fraudulent traffic, amounting to millions of attacks that were allowed into the protected environment. Upon deployment, NuData identified over 99% of these threats coming into the environment and mitigated them in real time.

This is an example of how NuData technology can be combined with other tools to enhance and manage online security.



* The pre-existing coarse-filter automated tool was missing 10% of the fraudulent traffic

NuData Security mastercard

Expanding beyond the login – Continuous validation

Login is not everything

Banks, like other industries, know that login is not the origin and end of all their fraud problems. Other threats are designed to bypass the login placement completely.

For example, malware on a device allows a bad actor to take over an active session once the legitimate user has logged in; this is known as account hijacking. Application fraud, on the other hand, uses fake or stolen identities to apply for credit or create an account, making the security at login useless since the fraudulent user is, ironically, legitimate.

These many faces of fraud are the reason why financial institutions are starting to include continuous verification platforms that monitor their traffic across different placements: account creation, login, money movement, etc.

From login to other placements

This bank realized the importance of extending its security solutions to other placements, especially as their services kept growing and expanding. They offer their online services through an app but also have product-specific apps such as savings services which are incredibly attractive for new and seasoned hackers.

To secure all flanks, the client deployed NuData at several placements (login, native app, savings app, new application, money movement…) not only to block threats but to learn from them.

Today, our client has access to a 360-degree view of their environment, across all channels and services, and is blocking over 99% of all the attacks.

Attacks grow, protection multiplies

Over a three-month period NuData delivered robust security and scalability by processing over one billion events, while maintaining a near 100% success rate.

1.079B

MITIGATED

1.08B login events reported as malicious and mitigated

99%

DETECTION RATE

<0.1% false positive rate

Size of the attacks targeting the institution over those three months

Most prominent attacks occurred on mobile

5M

IP ADDRESSES TARGETED

48M

USER ACCOUNTS TARGETED

Learning from attackers; the ultimate twist

This robust and highly sophisticated security platform allows our client to mitigate attacks while learning from their attackers – to uncover slowly-simmering threats before they come to a boil. The interesting twist is that the more they attack, the more we learn about them – and the better we block them.

More than one client

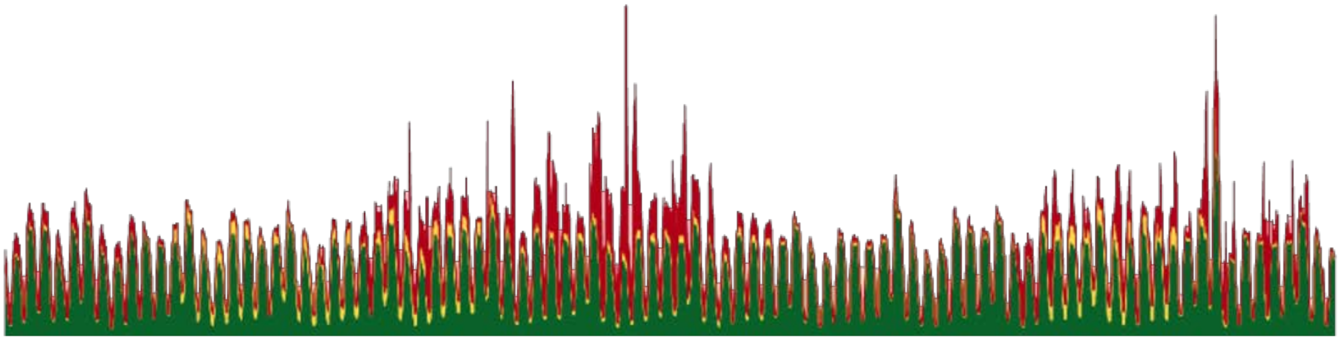
These results go beyond this particular client. All the financial institutions using NuData technology benefit from a sub 0.5% false positive rate.

We consistently deliver sub-0.5% false decline rates, with over 99% accuracy rate.

Risk Mitigation Rate	99.55%
False Negative Rate	0.45%
False Positive Rate	0.42%

__Risk Mitigation Rate:__ The rate of attack events that were served either an interdiction that was not solved, or an interdiction block signal: 99.55%

At login across FI clients, we consistently perform with a __false positive rate under 0.50%__



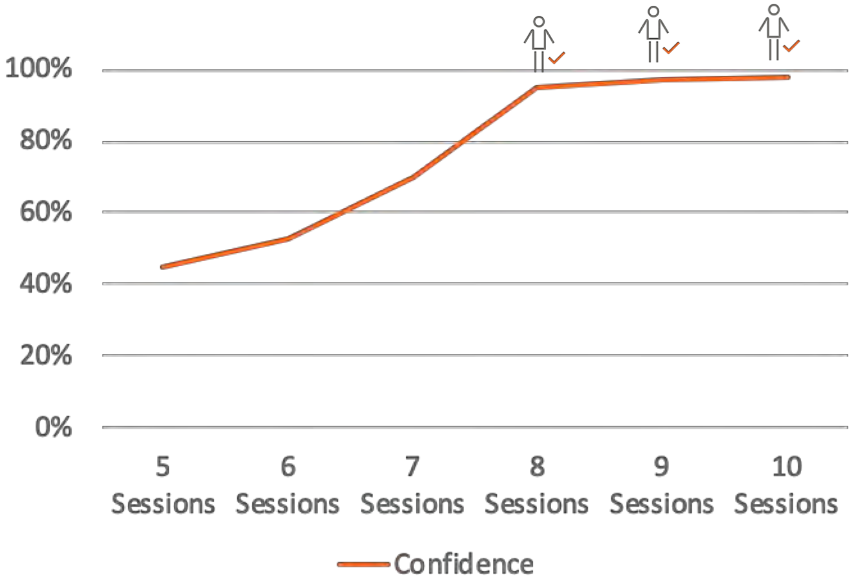
Behavioral biometrics treats your customers better

With continuous validation security, our client has a sub 0.1% false positive rate, removing the need for manual reviews. The institutions can now use that time to focus on their customers and innovation without worrying about security.

NuData's passive biometrics layer alone recognizes returning customers, with over 95% accuracy, removing the need for any additional friction to verify them. This means that customers can just tap their app and go, regardless of the type of activity or transaction.

NuData's passive biometrics layer reaches over 95% accuracy after only 8-10 assessments of the same user:

> "The NuData team processes the most demanding, multi-dimensional issues faced by the industry. They proficiently determine the heart of the problem, sensibly translate it into a strategic plan, and then into a coherent message understood by all."
>
> **— Major U.S. bank**



NuData Security
mastercard

About NuData Security

NuData Security, a Mastercard company, is an award-winning provider of behavioral biometrics and device intelligence solutions and is trusted by some of the world's largest brands across eCommerce, digital banking, and beyond. NuData helps companies stop account takeover, prevent new account fraud, and reduce unnecessary friction in real time.
With over 20 billion risk assessments and 4.5 billion devices processed yearly, businesses across the globe benefit from the power of NuData's Trust Consortium to validate good users without disruption and stop bad actors before they can cause damage.

Click here to read about the successes of other companies with NuData.

Email us to book a consultation with one of our fraud prevention and security experts at hellonudata@mastercard.com

NuData Security
mastercard.