Case Study

digital banking • digital banking platform

Jack Henry™ bank stops fraud in its tracks with behavioral security technology

The Behavioral Insights Attackers Hate

jack henry™

Assets
$1.9M

Software Solutions
NuDetect™ by NuData Security, a Mastercard® company

the attack

"The type of attack they used is called a 'password spray,'" begins the Information Security Director at a $1.9M-asset bank.

"It was a slow drip from a variety of different IP addresses," further describes the bank's Digital Banking Specialist. "At first, I couldn't figure out how our website was even staying up with how much traffic was going through it. And then there's where the traffic was coming from. We're not an international bank, so 99.7% of our daily logins are from the United States."

But on this occasion, the Jack Henry client observed close to 800,000 requests (400 times the bank's normal traffic volume) come from 196 countries and more than 105,000 IP addresses. As an organization dedicated to "uncomplicating" people's relationships with money – helping them create simpler, more meaningful relationships with their money so they can get to where they want to go – the bank makes trust and security top priorities.

"When I logged in that day, I actually thought the portal was broken," recalls the Digital Banking Specialist. "NuDetect's dashboard analysis is categorized into red, yellow, and green. There was just so much red.*"

NuDetect, behavioral security technology by Mastercard company NuData Security, confirmed that attackers targeting the bank were using hundreds of IPs and were attempting authentication at a slow rate. Given the rules that were triggered, this was classified as mass credential stuffing.

the technology

"The point of NuDetect is to differentiate good users from bad – so that good users have a good experience on the platform and don't even know we're there; and bad users don't get access to accounts and funds," explains Matt Melnik, Director of Product Development at NuData Security.

"The NuDetect dashboard was the only place showing this fraudulent activity."

Digital Banking Specialist

"Rather than solely focusing on fraud detection and prevention, we're also focusing our efforts on making sure good users have reduced levels of friction throughout their journey," says Matt. "We have enhancements for our 2023 roadmap that are going to build on that and will ultimately help us prevent fraud as attackers evolve and get better at what they're doing. Ideally, the bad users will have no chance."

Beyond NuDetect's main features of device identification and geolocation information are the behavioral insights the technology captures.

why behavioral insights matter

"NuDetect collects how users interact with every touchpoint," says Matt. "Think about the login page: how users are typing in their username and password, how they're clicking around, the amount of time they spend on a page, whether the time displayed matches their time zone, everything. This data helps us differentiate a computer from a human and – as we've been progressing – what human is actually behind the screen. That's how we use behavioral data."

When the bank's Digital Banking Specialist logged in to their NuDetect dashboard that day, their eyes were immediately drawn to the sea of red. "We were at 99% red, United States logins were accounting for about 3% of all total logins, and there were all of these other countries in front of it. And the number of total logins was just through the roof."

Their first course of action was to check in with the bank's business analyst involved in the NuDetect project who confirmed something looked wrong.

Next, they reached out to the Jack Henry team who got in touch with NuData Security for analysis. "It turns out, there were tons of blocked logins, and it appeared the attacker had obtained a list from someone else's breach. It's true what they say," they warn, "Don't use the same user ID and password combination for all of your sites, because if one of those sites gets breached, it can be used elsewhere to find a match."

"The NuDetect dashboard was the only place showing this fraudulent activity," the Digital Banking Specialist continues. "This was a benefit because the vast majority weren't getting through.

Even if the attacker(s) did have an accountholder's user ID and password correct, our two-factor authentication was stopping them from getting into our online banking. It also stopped them from funneling money out by setting up bank-to-bank transfers via Quicken."

the fix

"We'd only had NuDetect turned on for two months when this happened," recalls the Digital Banking Specialist. "Even in just this one particular situation, it was incredibly helpful. NuDetect detected something nothing else could."

"NuDetect detected something nothing else could."

Digital Banking Specialist

By integrating NuDetect with the bank's digital banking platform, the technology was able to detect this ominous activity in the system. It picked up on the deviation from the bank's normal patterns, the spike in traffic, and anomalous behavior – scoring red. After getting in touch with Jack Henry's NuDetect team, Jack Henry was able to take even further action to end the attack, configuring a signature to block the attempts. The bank completely mitigated the risk of traffic – with all attacker requests resulting in 100% failure.

"With NuDetect, you can block certain countries, clean up your traffic, and look for patterns. Without it, you're really missing a big layer of security – for threats that are out there today and those that are growing," concludes the bank's Information Security Director. "From our perspective as a financial institution, NuDetect is a must-have."

"From our perspective as a financial institution, NuDetect is a must-have."

Information Security Director

**Red indicates high-risk traffic.*

protect your organization, your reputation, and your accountholders

For more information about Jack Henry, visit jackhenry.com.

jack henry™