CASE STUDY

ThreatX Effectively Blocks Credential Stuffing Attacks for Financial Services Organization

Industry | Finance

The Challenge

In late 2018, a midsize financial services organization started suffering from credential stuffing attacks. These attacks were persistent, relentless, and always evolving. Scrambling to put a solution in place to thwart the attackers, the security team installed a web application firewall. But that solution proved less than ideal and left the team once again on the hunt for a way to effectively and efficiently block the attacks. As an information security analyst at the organization said, "We had to put in some Band-Aid® solutions that were not very effective. We were looking for a more proactive solution. We were spending a lot of weekends, late nights, and holidays managing these attacks. It seemed like these attackers would always take my Christmas Day, my New Year's Day. I couldn't sleep at night."

The financial services organization first tried to combat the attacks with geo-blocking and simply blocking traffic from any country where they saw a lot of originating attacks. The information security analyst said that "we were blocking Russia and Poland already. Then we started blocking Brazil, Thailand, Indonesia. The locations kept changing all the time."

> *We had to put in some Band-Aid® solutions that were not very effective. We were looking for a more proactive solution.*
>
> **– Information Security Analyst**
> **Financial Services Organization**

NETWORK SOLUTION

ThreatX API and Web Application Protection Platform

CRITICAL ISSUES

- Rapid increase of credential stuffing attacks, ineffective blocking, negative customer experiences

RESULTS

- Able to block attacks without impacting customer experiences
- Easily accessible security metrics reporting
- ThreatX SOC provides 24/7 extended team

The security team next turned to their database team for help. The database team could see all the failed login attempts from the credential stuffing attacks, so they scripted something that would pull out all the suspicious IP addresses and copy them to a text file. However, their firewall would only automatically import the list every hour, which wasn't frequent enough, so the security team spent a lot of time manually adding IP addresses to be blocked. On top of that, the attackers kept changing their IP addresses. In the end, the security team had to be in non-stop reaction mode to try to keep up. The information security analyst said, "We just couldn't be proactive. As soon as we identified signatures attackers were using, we would start to block based on that information. But then the attackers would modify their tactics again. We sometimes had to just let the attack happen, and after 10 failed login attempts, we would block that IP for a day. That was our solution before ThreatX."

The Solution

In late 2021, the financial services organization began the search for a new, more effective web application firewall (WAF) or web application and API protection (WAAP) solution. The team was evaluating several of the well-known, big players in the space when they heard about ThreatX. A partner of the organization was using ThreatX and spoke highly of the solution, so they added it to the evaluation mix.

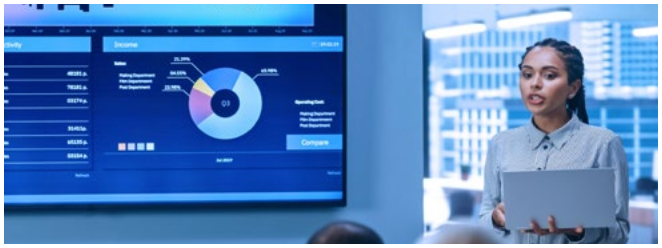
> *"So we decided to test ThreatX, and right away, we saw instant results. Everybody was happy."*
>
> **– Information Security Analyst**
> **Financial Services Organization**

The results from the other vendors couldn't match the level of protection the team saw from ThreatX, so they moved forward with ThreatX.

The Benefits

Getting Time Back

The financial services organization's information security analyst now considers the ThreatX SOC team to be an extension of her team. "It's been easy to work with the SOC team," she said. "I feel, the team feels, like they're an extension of our information security team. Before, I would get all these text messages, at two in the morning or three in the morning. And it was never fun. I felt like I worked 24 by 7, nonstop, not just being on call. I just felt like we were working seven days a week. So, this past Thanksgiving was actually the first holiday that I felt I could actually enjoy with my family."



Easily Reporting on Security Metrics

With the ThreatX solution, the security team can quickly and easily see and report on the attacks they are blocking – where they are originating, the type of attack, the exact targets, and more. The financial services organization's information security analyst noted that she spends a lot of time in the ThreatX dashboard. But not because she is managing attacks, like she was with previous firewall solutions. With ThreatX, she is primarily using the dashboard for reporting purposes. "With ThreatX, actually I'm in the console a lot, but not because I'm trying to troubleshoot and stop threats," she said. "I just like going in there and taking screenshots and showing them, 'look at all the blocks.' Or I'm taking stats for our monthly metrics, and it's not because I'm trying to stop the attack."

Realizing What's Possible

When the financial services organization security team was trying to stop the cyberattacks with geo-blocking, they inevitably impacted traveling clients trying to access their accounts. The information security analyst noted that, "For a client to be overseas, on holiday, on vacation, and not be able to check their account, that's very worrisome. So, we tried geo-blocking, but it was difficult to manage, and we ended up with some very unhappy clients."

In addition, when the team tried to block suspicious IP addresses to thwart the attackers, they also impacted the client experience. When they were blocking IPs after 10 failed login attempts, they ended up with false positives where they were blocking legitimate users who had forgotten their passwords.

With the ThreatX solution in place, the financial services organization is finally blocking the cyber attackers without negatively impacting the experience of clients trying to access their accounts.

> *"With ThreatX, I'm in the console a lot, but not because I'm trying to troubleshoot and stop threats, I just like going in there and taking screenshots and showing them, 'look at all the blocks."*
>
> **– Information Security Analyst**
> **Financial Services Organization**

ThreatX by A10 Networks

An Integrated Cloud Platform for Application and API Protection

Download Data Sheet

Product Demo

Take a Self-led Product Tour

Take a Tour

About A10 Networks

A10 Networks provides security and infrastructure solutions for on-premises, hybrid cloud, and edge-cloud environments. Our 7000+ customers span global large enterprises and communications, cloud and web service providers who must ensure business-critical applications and networks are secure, available, and efficient. Founded in 2004, A10 Networks is based in San Jose, Calif. and serves customers globally.

For more information, visit A10Networks.com and follow us @A10Networks.

About A10

A10Networks.com

Contact Us

A10Networks.com/contact

Part Number: A10-CS-80248-EN-01 Apr 2025