CASE STUDY

ThreatX Protects Segpay’s Apps and APIs with Accuracy and Visibility

About Segpay

ThreatX customer, Segpay, is a digital payment processing company. It offers a payments platform for online credit card processing for e-commerce merchants and subscription-based content providers who intend to operate globally.

The Challenge

Because Segpay is in the payment space, it attracts a fair amount of cyber attacker attention. “We have this target on our back constantly,” said Segpay’s Director of Operations, Marco Escobar. “And though the attackers haven't been able to penetrate our systems, they're becoming smarter, and more evasive.”

Segpay recently experienced cyberattacks that featured bots inputting a series of different credit card numbers into the system to see if any would get approved. None of the attacks were successful, but Segpay did face thousands of transactions in a short period of time, which obviously required a time- and resource-intensive response.

> *The attackers are becoming smarter, and more evasive.*
>
> **— Marco Escobar**
> **Senior Director of Operations, Segpay**

©2025 A10 Networks, Inc. All rights reserved.

SEGPAY

Industry | Finance

NETWORK SOLUTION

ThreatX API and Web Application Protection Platform

CRITICAL ISSUES

- Protect against expensive and time-consuming bot attacks

RESULTS

- ThreatX allows Segpay to stay one step ahead of attackers with insights into their movements over time
- ThreatX SOC eases the burden on the Segpay IT team through a responsive and hands-on partnership
- Segpay is protecting current APIs and ready for future growth

The Challenge (cont.)

Segpay had a web application firewall solution in place but was looking for an alternative that would help mitigate these attacks ahead of time by being a little more proactive than reactive, and gain additional insights into the attacks.

The Solution

ThreatX was one of four vendors Segpay vetted. Ultimately, the support and service they received from the ThreatX team solidified their decision. “What really drove me towards ThreatX,” said Escobar, “aside from the technology, is the attention to detail and support throughout the process.”

In addition, ThreatX gave Segpay details and insights into the threat landscape that they couldn’t get from other solutions. “We could see query strings, IP addresses, and details on attacker behavior that we couldn’t get from other solutions, and that helped us mitigate future risks.” Escobar said.

> *“What really drove me towards ThreatX, aside from the technology, is the attention to detail and support.”*
>
> **— Marco Escobar**
> **Senior Director of Operations, Segpay**

The Benefits

Accuracy

Segpay found that ThreatX’s attacker-centric behavioral analysis gives it more accuracy, and more flexibility. When bots are carrying out attacks by cycling through multiple IP addresses, ThreatX identifies the behavior as malicious and immediately blocks the attacker without having to block individual IP addresses – which can be both time-consuming and inaccurate. With another WAF solution, Segpay put blocks in place after observing a certain number of hits from an IP address in a defined period, but that isn’t always accurate, and didn’t help watch attackers over time. The attacker could just move on to another IP address. With ThreatX, the team is now following and learning about an attacker’s movements over time. Escobar says, “We look at our ThreatX dashboard and pinpoint whether attackers are just getting their feet wet or if they are really trying to exploit us. It’s a good visual because we can clearly see what to focus on. With other solutions, it was just an immediate block for anything that met a rule.”

Expertise

Escobar noted that the ThreatX SOC team has been responsive, helpful, and hands-on, even during the customer onboarding phase. Escobar said, “My team has sent in requests for some rules, and they were implemented right away. We didn't even have to label them as urgent. Having that team readily available for calls and to answer my team's questions was reassuring, versus other vendors who made us sit around and wait for an email reply. ThreatX were very open and very insightful.”

Protection for an Expanding Set of APIs

ThreatX is currently protecting specific areas of Segpay’s systems that are facilitated through an API call. Customers can access a website to get to the payment page, but they also have merchants that facilitate payment through their own API into the Segpay system. ThreatX adds an additional layer of security for these critical endpoints. “As our API offerings continue to grow, we are increasingly concerned about the security implications of APIs, which are potential entryways for attackers,” said Escobar.

> *“We look at our ThreatX dashboard and pinpoint whether attackers are just getting their feet wet or if they are really trying to exploit us. It’s a good visual because we can see clearly what to focus on. With other solutions, it was just an immediate block for anything that met a rule.”*
>
> **— Marco Escobar**
> **Senior Director of Operations, Segpay**

©2025 A10 Networks, Inc. All rights reserved.

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

©2025 A10 Networks, Inc. All rights reserved. A10 Networks, the A10 Logo, A10 Control, A10 Defend, A10 Harmony, Harmony, A10 Thunder, Thunder, ACOS, A10 SSL Insight, SSL Insight, SSLi, vThunder, ThreatX, and ThreatX Protect are trademarks or registered trademarks of A10 Networks, Inc. or its affiliates in the United States and other countries. All other trademarks are property of their respective owners. A10 Networks assumes no responsibility for any inaccuracies in this document. A10 Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. For the full list of trademarks, visit: A10Networks.com/a10trademarks.

Part Number: A10-CS-80246-EN-01 Apr 2025