

## ThreatX Protects Segpay's Apps and APIs With Accuracy and Visibility

### About Segpay

---

Digital payment processing company, Segpay, offers a Payments Platform that specializes in online credit card processing for e-commerce merchants and subscription-based content providers who intend to operate globally.

### The Challenge

---

Segpay is in the payment space and, therefore, attracts a fair amount of cyberattacker 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."

This past fall, Segpay 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.

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

## SEGPAY

### AT A GLANCE

**Customer:**  
Segpay

**Industry:**  
Payment processing

**Challenge**  
Protect against expensive and time-consuming bot attacks

**Solution**  
ThreatX API and Web Application Protection Platform

**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 attackers are becoming smarter, and more evasive.”**

– Marco Escobar, Senior Director of Operations, Segpay

## 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 their technology, is their attention to detail and support throughout the process.”

In addition, ThreatX gave Segpay details and insights into their 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 their technology, is their 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 them 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 of time. But, that isn't always accurate, and didn't help them 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 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.”

“

**We look at our ThreatX dashboard and pinpoint whether attackers are just getting their feet wet, or 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

---

## 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.

## ABOUT THREATX

ThreatX's API protection platform makes the world safer by protecting APIs from all threats, including DDoS attempts, BOT attacks, API abuse, exploitations of known vulnerabilities, and zero-day attacks. Its multi-layered detection capabilities accurately identify malicious actors and dynamically initiate appropriate action. ThreatX effectively and efficiently protects APIs for companies in every industry across the globe. For more information, visit: [www.threatx.com](http://www.threatx.com).

To learn more

**REGISTER FOR A DEMO**

[www.threatx.com/request-a-demo](http://www.threatx.com/request-a-demo)