CASE STUDY

ThreatX Gives Leading Critical Infrastructure Supplier Confidence That Customer Data Is Safe

Industry | Technology

The Challenge

Protecting customers and their data is a priority for a leading critical infrastructure supplier. When the head of product security at the supplier started in his role, he was charged with ensuring the supplier's SaaS application and all the many APIs it interacts with were protected from attackers. "All our web applications and mobile applications are API-driven. The APIs are the heart of the system. If an attacker gets access to the API, they can get to personal data and even have the ability to do things like turn services off. So, it's really important that we protect that."

The head of product security had used ThreatX at a previous company, and knew he wanted to use it again. At his previous company, he often logged into the ThreatX platform and saw attempted attacks against APIs and applications going on constantly, 24 hours a day. He knew he wanted and needed that level of visibility and protection at his new role. After investigating several vendors' solutions, the team agreed with his recommendation and started a relationship with ThreatX.

> *It's not just a team I can reach out to 24/7, but rather a team that's watching my back 24/7.*
>
> **– Head of Product Security Infrastructure Supplier**

NETWORK SOLUTION

ThreatX API and Web Application Protection Platform

CRITICAL ISSUES

- Needed real-time protection against API and application attacks

RESULTS

- Deep visibility into the attack service and activity
- Visibility into API use to improve protection
- 24/7 support from the ThreatX SOC

Greater Attack Visibility

The biggest problem ThreatX solves for this critical infrastructure supplier is real-time protection against API and application attacks with an unprecedented level of visibility into the attack surface and attacker activity. “ThreatX does a great job showing you which APIs are being called and how they’re being attacked. Even if you have API logging, it doesn't mean you're getting that same visibility; because that log might only take effect when someone is calling the API, not someone doing reconnaissance or other types of less obvious attacks.”

The biggest transformation the team experienced with ThreatX is the ability to show colleagues the risks or the attempted attacks. “I can tell people that we’re getting attacked constantly, but now that I can show them the weekly report from ThreatX that clearly illustrates the number of attacks attempted and the number of blocks implemented. It makes people pay attention and take security more seriously. I've received more support from different teams now that I can show them what's going on.”

Enhanced API Visibility

The head of product security found an unexpected benefit of ThreatX was the visibility into API use, which ultimately improves API protection. “Because ThreatX tells us what APIs are being called, we have a clear picture of what's being utilized. We can now compare the APIs that ThreatX shows being called versus what are actually out on the internet. If we have 100 APIs, but only 30 are being called, that leaves 70 zombie APIs out there that no one's paying attention to. If those 70 have security issues, no one would know.”

That kind of visibility greatly increases API protection. “If APIs aren't being used, they shouldn't be on the internet. Out of sight, out of mind means security holes. But if we know it’s out there, and get rid of it, we just reduced our exposure.”

A True Partner

Ultimately, it’s the partnership with the ThreatX protection-as-a-service team that makes ThreatX a vendor the head of product security wants to keep working with. “This team is why I really wanted to stay with ThreatX. They are so responsive, and you can access them 24/7.” He didn’t fully comprehend the power of protection-as-a-service until the emergence of the Log4J vulnerability while he was at his previous company.

> *“ThreatX immediately sent me an email saying that they had updated their platform to make sure that they were blocking this attack. I woke up to the email already in my inbox. I didn't have to do anything. That’s a pretty big benefit that you don't see with other vendors. When that happened with Log4j, I felt really glad they are out there.”*
>
> **– Head of Product Security Infrastructure Supplier**

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-80251-EN-01 May 2025