THREATX

CASE STUDY

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

The Challenge

Protecting customers and their data is a priority for a leading critical infrastructure supplier and recent ThreatX customer. When the Head of Product Security at the supplier started in his role, he was charged with ensuring their SaaS application and all the many APIs it interacts with were protected from attackers. "All our web applications and mobile applications are API-driven," he says. "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 partnership with ThreatX.

A New Level of Confidence

The biggest problem ThreatX solves for this critical infrastructure supplier? Real-time protection against API and application attacks with an unprecedented level of visibility into the attack surface and attacker activity. For the Head of Product Security personally? "Sleep," he says. "ThreatX helps me sleep at night."

"ThreatX is our first line of defense. Developers are human, and they make mistakes. If there's a vulnerability in our APIs or applications, SQL injection for example, I know ThreatX is there, and it will block attempts to exploit that vulnerability and give us a chance to fix it."

– Head of Product Security

Greater Attack Visibility

The visibility into the organization's attack surface is another benefit of working with ThreatX. "ThreatX does a great job showing you which APIs are being called and how they're being attacked," he says. 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 Head of Product Security has experienced from his ThreatX partnership is the ability to show colleagues the risks or the attempted attacks. "I can tell people that we're getting attacked constantly," he says, "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 that an unexpected benefit of working with 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," he says. "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," he says. "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," he says. "They are so responsive, and you can access them 24/7." He says he didn't fully comprehend the power of Protection-as-a-Service until the emergence of the Log4J vulnerability last year 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," he says. "I was like, wow, that's awesome. 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."

> "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

About ThreatX

ThreatX is managed API and app protection that means you'll never stress about when the next attack is coming. You'll know your APIs and applications are safe with risk-based, real-time protection – backed by experts who do the worrying for you. To learn more, visit threatx.com.

Try It for Yourself

Ready to stop threats and get more time back in your day?

Take the next step. Request a demo today and see how you can effortlessly protect your APIs and apps against today's sophisticated threats while reducing the burden on your security team.

ThreatX's team of experts have your back, anytime of the day

Mean time to detect:
ThreatX Platform detects threats within seconds

Mean time to respond:
ThreatX Protection-as-a-Service will begin triage in just minutes