

ThreatX Protects Oncology-focused BioTech Company's Websites from Advanced Attacks

The Challenge

A fast-growing biotech company focused on developing and bringing to market novel cancer treatment therapy, began with a need for a simple but powerful application protection solution that could protect their corporate website from online attacks. As the organization grew and began to commercialize new oncology products and services, the security team realized that they needed a solution to protect their growing catalog of sites that managed clinical trial information, health care provider registration, and more, from a growing list of increasingly dynamic threat actors.

"We needed a more robust platform to offer protection without disrupting the normal flow of expected operations. But really, I was concerned about preventing the bad actors and bots from populating the fields with possible injection attempts as well as generally abusing the system." said the Chief Information Security Officer. "We went from one static site to dozens of sites very quickly that varied with everything from employee information for benefits, to information about trials, information on drug research and development.

Once we went commercial and became FDA approved, everything changed to accommodate for new labeling requirements, reporting for pharmacovigilance, and safety for adverse events- all spawning the need for multiple sites and multiple purposes." When the CISO considered market options, he opted for a known and trusted solution like ThreatX vs further exploring alternative solutions.

"As a CISO, knowing that my team doesn't have to spend time worrying about attacks against dozens of our websites is a huge relief for me.

I'm confident we have the right technology and the right people watching that even if something bad does happen, ThreatX has our back – that was huge."

- Chief Information Security Officer
at biotech company

Extension of my own Team

The biotech company's information security officer considers the ThreatX SOC team to be an extension of their own team. "The 24/7 SOC is a big part of why we've enjoyed working with ThreatX over the years," he said. "We don't have a lot of interaction with the ThreatX SOC from a day-to-day perspective. But when we did and needed to engage them, they were always there and responsive. The 24/7 SOC is essentially an extension of my own team. It's also a relief knowing that the SOC is there, they're experts in our field, and they're dedicated to monitoring bots and bad actors, tracking them and alerting the security team only when necessary. Getting that additional coverage, additional protection, that additional security bench strength gives my already small team an extra boost."

Easily Investigate Security & Operational Events

With the ThreatX solution, the security team could quickly and easily dig into security as well as operational events to analyze performance issues. It was important to understand and see where malicious traffic was coming from, report on different types of attacks, and be able to communicate the targets. An Information Security Analyst on the team noted that, "We had a few directly targeted attacks that dropped around the same time as news articles were being published about the company or a new oncology drug we were producing. Through my investigation, what happened was that we were being hit three hours after a news article was published, somebody started trying to crack into our websites. As we were seeing those attacks, ThreatX blocked it, giving me time to dig into the data and I worked with the ThreatX SOC to permanently block those attackers."

Proactive, Risk-based Blocking

For this biotech firm's lean security team, having a solution that was easy to use and didn't create additional manual work was key to their success. "The proactive, risk-based blocking is another key benefit for me when working with the ThreatX technology because it doesn't require much manual work," said the lead security engineer. "I liked the proactive blocking because our opinion is that I'd rather stop everything that's suspicious, then reverse it later if I have to. I've never had to manually block something or have the SOC manually block because of the technology's accuracy and 3-strikes before you're out approach not requiring any intervention."

Ease of Management & Reporting

The chief information security officer highlighted that he regularly used ThreatX reports to communicate improvements in the organization's protection mechanisms when communicating with numerous internal committees and leadership. When setting up the ThreatX solution, the lead security engineer stated, "I like using ThreatX specifically because it's a

"In the past, I was frustrated that I had to go into other solutions to check things and make sure that something was actually got blocked. **With ThreatX, I've never had to manually block something. The technology's three temporary blocks before you're out, or permanently blocked saved me so much manual effort.**"

- Lead Security Engineer at biotech company

fire and forget solution, we deployed the sensor, I managed the SSL certs and configured DNS, then I left it alone." The ease of management and access of information helped their chief information security officer explain to the organization's leadership the increase the awareness of threats and risk across their web presence.

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.