From the perspective of Sandra M. Teixeira, the CFO of Lusitania Savings Bank, the community bank had a problem: it lacked an effective cybersecurity management tool. To complicate matters further, the newly released FFIEC Cybersecurity Assessment Tool (CAT) recommended that banks identify an incident response provider to help the bank recover from a breach. The bank hadn’t identified a suitably qualified firm for that role either. In short, Teixeira needed to find a cybersecurity firm that could bolster the bank’s efforts to thwart attacks while simultaneously ensuring that its program reflected the latest FFIEC guidance.

Teixeira’s search for a cybersecurity partner quickly lead to DefenseStorm. “At the time, no one really understood the CAT tool or what it was about. DefenseStorm was one of the first to come out with a worksheet to facilitate that process.” She found that the proprietary tool that DefenseStorm created to help banks interpret and apply the FFIEC CAT was easy to use, and it provided actionable results. “That’s how I got drawn into the company. Then, once I actually heard what they had to offer, which was so tailored to the banking industry, especially for small banks like ours, I presented it to our bank’s senior executives,” adds Teixeira.
CUSTOMER TESTIMONIAL

While Teixeira conducted her search for a suitable cybersecurity provider that would help the bank implement the FFIEC’s guidance, news of high-profile breaches continued to pop up frequently. “There was a lot of talk about financial institutions being breached, smaller ones more specifically, because the bigger ones have expensive infrastructure in place to protect against these threats,” says Teixeira. “We didn’t feel secure, is basically what it came down to.”

A partner that watches over our bank

While the Lusitania always had access to plenty of data, it didn’t have the time or expertise to derive value from it. “I wasn’t doing anything with it. I wasn’t connecting it. I wasn’t analyzing it. It was too time intensive and, honestly, a lot of it was beyond my understanding,” remarks Teixeira.

Having selected DefenseStorm as its cybersecurity partner, Lusitania evolved from spending weeks to identify and counter a threat, to enjoying an almost immediate response.

Prior to adopting DefenseStorm Teixeira would typically spend twenty to twenty-five hours a month reviewing and maintaining the bank’s security-related reports. Post-implementation, she spends five to ten hours a month.

Most of the time, Teixeira allows DefenseStorm to function as designed—a centralized platform that analyzes the bank’s entire threat landscape. “It’s good to know that I have DefenseStorm monitoring and detecting all the different logs, putting them all together, detecting normal patterns of behavior on our system or not, and then notifying me when something goes wrong. That’s a huge value, especially when we don’t have a person dedicated to monitoring. I pretty much sit back and wait for someone to tell me I have a problem. It’s a real peace of mind,” notes Teixeira.

A flawless implementation

“The implementation process was a breeze. I thought it was going to be complicated, but we finished everything in two days,” she explains.

During the implementation process, in addition to deploying the technology, Teixeira noted that DefenseStorm’s security team conducted extensive testing of the bank’s network. “They gave us many recommendations on how to lock down our network. We took all those recommendations and activated them right away.”

In order to underscore its commitment to customer security, Lusitania Savings Bank recently publicized DefenseStorm by dedicating an entire section in its customer newsletter to highlighting the new program. Teixeira’s experience reaffirms why DefenseStorm’s approach continues to attract new customers.

“I think they really have a sense for what banks need. It’s like they’ve designed their systems specifically for small banks.”

I spoke to many other companies, and no one had figured out exactly what community banks, like mine, needed,” says Teixeira.
Exceeding regulatory expectations

As part of a recent examination, Lusitania received very positive feedback from regulators regarding the bank’s proactive approach to cybersecurity. In addition to impressing regulators, the reporting capabilities provided by DefenseStorm allow the bank’s executives to provide monthly reports to the Board of Directors. These reports not only demonstrate the effectiveness of the bank’s cybersecurity program, they also show the board that the investment in DefenseStorm continues to detect anomalies, as well as provide support to pinpoint and mitigate a broad range of threats.

With DefenseStorm deployed within Lusitania’s security infrastructure, Teixeira’s peace of mind comes from knowing that the DefenseStorm team is always in position, monitoring the bank’s environment around the clock, ready to put a stop to any attacks directed the bank’s way.