When Peach State Bank’s CEO, Ron Quinn, returned from a cybersecurity conference arranged by the FDIC, he had a new appreciation for the risks that banks face. He tasked Charles W. Blair, the bank’s CFO, with an important project—the hiring of a dedicated cybersecurity firm. “It was a direct reaction to hearing from the regulators about what they were going to be requiring banks to do,” Blair says.

While Peach State already had a firewall monitoring company in place, the bank lacked an all-encompassing view of their network. Earlier that year, knowing that the bank’s cybersecurity program needed improvement, Peach State had conducted preliminary discussions with DefenseStorm.

The CEO’s attendance at the FDIC conference added a renewed sense of urgency to the discussion, which ultimately resulted in Blair’s hiring DefenseStorm to augment the bank’s cybersecurity defenses.
An early and unintended test of DefenseStorm’s optics

Steven Pettit, an Assistant Vice President with Peach State Bank with day-to-day responsibility for the bank's cybersecurity program, worked directly with DefenseStorm throughout the implementation process. “DefenseStorm did a lot of vulnerability testing to get familiar with our environment and to get an initial assessment of any holes that they could detect,” notes Pettit.

According to Pettit and Blair, implementing DefenseStorm was a simple process that placed very little demand on their time. However, immediately upon going live, DefenseStorm uncovered a problem. It appeared that several of the bank's devices were communicating with a rogue router in Texas, so DefenseStorm flagged the device as unapproved. In reality, the bank had omitted that asset from its list of approved devices, when in fact it was part of the bank's IT infrastructure.
Better threat intelligence with less effort

Having deployed DefenseStorm, Peach State Bank has significantly improved its ability to protect the bank and its customers.

“With our prior company, all they were monitoring was server traffic and the firewall. DefenseStorm is monitoring the entire network,” Pettit says.

Further, with their previous security provider, the bank would get a lot of information, but it came with no explanation, leaving the IT staff in a quandary as to what to do next. Often, that meant calling and placing a support ticket, hoping that somebody would call back in a timely manner. Now, they work with Guardian, DefenseStorm’s team of security experts, to receive a more service-oriented approach that delivers actionable recommendations and insight.

At the heart of the problem facing Peach State Bank was an inability to separate routine, run-of-the-mill information from critical threat detection. “Our prior provider had no way of us just setting up alerts that we cared about. I don’t really care about seeing alerts on port scans, unless someone is actually able to penetrate the firewall,” explains Pettit.

In comparison, Peach State Bank views DefenseStorm’s user interface as robust and tailored to their needs. Today, the bank can configure an alert related to any aspect of network activity that comes to mind. The bank can be made aware of emerging threats, such as concerns that a cybercriminal could hijack the employee phone system and redirect incoming customer calls. Using DefenseStorm, the bank now has an alert that notifies the IT department of forwarded calls.

Having made the decision to engage DefenseStorm, Blair knows that the bank made the right choice. Many months after the implementation, he is still impressed with DefenseStorm’s focus on Peach State’s needs. “We still get a lot of attention from them. I don’t see that in a lot of vendors. Once they get your check and get you set up, then you have to call them. These guys call us. They have continued to be extremely engaged with us as a client.”