This College Faced COVID-19 Budget Cuts—And Ended Up with a Better Email Security Solution

|  |
| --- |
| **Peach University**Peach University is a mid-sized, public college in  the Southeast. **Requirements**Facing budget cuts due to the COVID-19 pandemic, Peach University wanted to find a more cost-effective email security solution that would allow them to avoid layoffs. As a college, they have been inundated with phishing campaigns, something that has only gotten worse since the pandemic began. Their solution had to be easy to use and able to scale quickly. Peach University needs an email security solution that not only stops phishing and malware attacks, but stops them before they get to the inbox, so that their remote students don’t accidentally click on a malicious email.**Cloud Suite**Microsoft 365**Previous Email Security Solution**IronScales |

Background

David Rose† works as the Director of Information Technology for Peach University, a mid-sized public college in the Southeast.

When the COVID-19 pandemic hit, all departments across his college were tasked with cutting 14% from their budget. Hoping to avoid layoffs, Rose looked at some of the bigger line items to see what he could get rid of or reduce.

He knew he couldn’t cut email security. But he wanted to see if he could reduce how much he spent on it. Peach University had been employing IronScales as an API-based security solution for a few years. And though he generally liked the program, it was far too expensive to keep in this climate.

Further, there were some issues he had with it. Like most API-based solutions, IronScales can remove a malicious email after it has reached the inbox. Sometimes that takes a few seconds; sometimes it takes minutes.

But because Rose deals with a student population that, he admits, doesn't always pay attention to phishing training, even an email sitting in the inbox for five seconds can make a difference.



Rose needed a solution that was more cost-effective. He knew he couldn’t get rid of email security—before he implemented any solution, there was a month where 74 student accounts were compromised.

But he didn’t want to lay anybody off, especially during a pandemic. And he needed a solution that didn’t let malicious mail come into the inbox, even just for a moment. With a rotating cast of young students and transfer students who didn't always keep up on phishing training, he wanted to take it out of their hands.

“They Wouldn’t Tell You How It Worked”

With the pandemic crunching his budget, Rose had to make a quick decision on his email security solution. Ditching it completely was not an option. As a college, he knew that student accounts are often targeted, and they would only be more so as the students scrambled home to finish the semester remotely.

The school had already been using an API-based solution from IronScales. And though they were largely happy with it, Rose and his team were hoping that they could reduce the cost.

The answer: “No.”

“We went to them and said, ‘Hey, you know, is there any way we can get this any cheaper?’” Rose recalled. “And they were like, ‘Well you know, you get what you pay for.’ You know, those kinds of things.”

That sent Rose on a search for a new product. He went through a number of products, ranging from other API solutions to traditional Secure Email Gateways.

What was frustrating to him was some of the answers he was receiving while on introductory calls. Rose wanted to know, in detail, how his school’s email would be protected. Whenever he asked, he got the same response: “Well, you know it’s our Secret Sauce.”

“They just won’t tell you how one thing worked or what features were coming down the pipeline,” he says.

Rose wanted a clear idea of what his new security provider would be doing for his college. So when he connected with Avanan, he was pleasantly surprised.

“When we connected, before we were even customers, the folks at Avanan were telling us about new features coming up.” he says. “That had never happened before.”

The transparency was refreshing. And, of course, the product, in a POC, proved to be a viable solution.

The whole thing, says Rose, “was a breath of fresh air.”

“The Malicious Email Actually Never Reaches the Inbox”

As the decision maker, Rose was concerned with cost and effectiveness. Though he had liked IronScales, he needed something that was more budget friendly. Further, as he reflected on his time with the company, he also wanted a partner that was more responsive, both for general customer service questions, as well as being open to a dialogue about specific features.

And finally, he was hoping he could find an API-based solution that didn’t just respond to malicious threats, but actively prevented them from reaching the inbox.

Because he’s dealing with college students, Rose knows that some may not pay close attention to phishing training. If the email is in the inbox for even a little bit, it could be damaging. “Seconds count,” he says. “It doesn’t matter if it’s gone after five seconds. It doesn’t matter. They have already clicked it.”

Hoping to avoid the hassle and potential danger, especially as his nearly 9,500 students scattered across the region to finish the semester remotely, Rose was pleased as he began his trial with Avanan.

He knew that Avanan was the first vendor to adopt the API-based approach for email security. What he didn’t know is that Avanan, unlike the rest of the API-based vendors on the market, can prevent malicious emails from reaching inboxes in the first place.

All API-based vendors, including Avanan, can retract a message from an inbox if it is determined to be malicious after delivery. This is valuable, but is dangerous if it is your only enforcement mechanism. Most API-based vendors can only respond, removing the email after it has already been delivered, typically after 30 seconds or more. For new, zero-day threats, or for any malware that requires additional analysis, that delay can reach minutes.

That delay is far too much time for the end-user to click on a malicious message. The Verizon Data Breach Investigation Report found that in 93% of breaches, compromise occurred in minutes or less. Further, the median time for the first user of a phishing campaign to open the malicious email is 1 minute and 40 seconds. When thinking in particular of his freshman students, new to college and who may not have much experience recognizing phishing, that was too long. For Rose, any response time greater than zero was too long.

As he went through the POC, he noticed scores of malicious emails being blocked *before* the inbox. “We’d see people sending malware or a phishing email and the malicious email actually never reaches the inbox,” he says.

Further, unlike some of the other vendors he had been talking to, Avanan was straight up. He didn’t get a sales rigamarole, or be referred to as their “Secret Sauce.” Avanan told him, plainly, how the product worked and, to his surprise, features that were on the horizon.

“The money was right,” he says. “And honestly, as I went through the trial, it was like, *‘Wow.’”*

“We’re Really Pleased”

Peach University is glad they made the switch. Not only did they save enough money to stave off layoffs in the department, they were also happier with the protection as a whole. Avanan was consistently blocking attacks before they reached the inbox. As universities across the country dealt with an influx of COVID-19 related phishing attacks, Rose could rest easy that his students were protected.

And with the money saved, Rose was also able to extend protections to SharePoint and OneDrive.

As this shapes up to be the most unusual of school years, with a whole new campaign of phishing and malicious emails expected to head his way, Rose is taking comfort in the fact that he has the right solution at the right place.

“We’re really pleased,” he says.

“We Would Recommend Avanan To Anybody”

Rose and the Peach University IT department were hit with 14% budget cuts in March due to the COVID-19 pandemic. Looking to avoid layoffs, he targeted one of the highest line items in his budget—email security.

Though he had been generally happy with his previous solution, IronScales, there was no flexibility given on budget. He had to make a change.

This gave Rose an opportunity to re-evaluate the email security landscape. When he came across Avanan, he was impressed with their forthrightness. And during the POC, he was amazed to see that Avanan, an API-based solution like IronScales, actually prevented emails from reaching the inbox. IronScales is only able to retract malicious emails afterwards. With some of his students admittedly not always focused on identifying phishing campaigns, an email that lasts in an inbox for even a few seconds is too long.

Now that he’s installed Avanan, Rose is able to keep his employees intact. He’s also able to focus on larger IT needs, particularly as remote learning heats up.

Peach University is a public institution, part of a larger network of colleges and universities in his state. And if any of the other institutions in the state—or for that matter, any higher education institution in the county—asked for his opinion on email security, he knows exactly what he would say.

“We would recommend Avanan to anybody,” he says.

†Company and individual names have been changed, but are available as a reference customer.