proofpoint.

CUSTOMER STORY

The University of Oklahoma Controls Phishing Attacks with Proofpoint

The Challenge

- Block email-based phishing attacks and cloud app threats with minimal false positives
- Integrate email and cloud security under a single umbrella for all campuses and users
- Increase IT efficiency with automated analysis and remediation

The Solution

- Proofpoint Enterprise Protection with Targeted Attack Protection (TAP) and Threat Response Auto Pull (TRAP)
- Proofpoint Email Data Loss Prevention (DLP) and Encryption
- Proofpoint Cloud Application Security Broker (CASB)

The Organization

There aren't many universities that are as far-reaching as the University of Oklahoma (OU). Founded in 1890, the school is rich in history. Located just outside of Oklahoma City, this public research school has three campuses and multiple remote-learning locations throughout Oklahoma. And it also has a global presence. It offers study abroad opportunities at several campuses overseas. And it supports a total of more than 35,000 students across its various facilities. OU is also home to Oklahoma's premier College of Medicine. This is a teaching hospital and the only Level 1 Trauma center in Oklahoma. What's more, the Oklahoma Medical Center was recently named the state's top facility for cancer care by U.S. News & World Report.[1] But with all of this growth and diversity comes an increasing set of cybersecurity challenges.

The Challenge

Apply a single, integrated solution to stop phishing attacks across all locations

Over time, OU has expanded from one to multiple campuses to meet growing demands and the desire to broaden its educational curriculum. The sites often serve various types of users, with each group having different security needs. For example, there's a main campus, along with a research campus that's rated as an R1 Carnegie research institute. And the medical center supports not just medical students, but doctors, patients and hospital administration staff. And they all require high levels of security to meet compliance regulations.

[1] https://www.ouhealth.com/find-a-location/ou-health-stephenson-cancer-center/; https://health.usnews.com/best-hospitals/area/ok/ou-medical-center-6730024/cancer

The Results

- Significantly reduced phishing attacks while avoiding false positives
- Successfully integrated all university email and cloud app security under Proofpoint
- Increased productivity of IT team

OU appointed a new president in 2019. And one of his goals was to reduce duplication of investment and resources in administrative areas across OU's multiple campuses. This new structure included finance, administration and—of course—IT.

Despite diverse user groups, each campus shared common problems. And email security was at the top of the list. "Phishing attacks were a major problem for us," explained Aaron Baillio, OU's chief security officer. "Given our distributed structure, we lacked visibility into the overall scope of the problem." The lack of standard tools for automating analysis and remediation also created a burden on the support teams. "Each campus had its own IT staff and infrastructure," added Baillio. "We had hundreds of vendor contracts across the many campuses. So there was a huge opportunity for savings and efficiency by standardizing on common platforms."

> We were drowning in phishing attacks. We needed help reducing not just the quantity of attacks, but also the amount of time spent responding to attacks.
>
> **Aaron Baillio,** chief information security officer, The University of Oklahoma

The Solution

Proofpoint selected to deploy university-wide security

Given its complex security requirements and the associated email infrastructure, the OU team went looking for a single partner to protect them from message-based attacks. They invited several vendors to a "bake-off" that evaluated a wide range of functionality. This included a trial using live data. Proofpoint met their requirements and exceeded many. The team also spoke with several Proofpoint university customers. And these positive references gave OU a high level of confidence in their choice.

The OU security team chose Proofpoint Email Protection with TAP and TRAP to lay the foundation for their email security architecture. TAP uses static and dynamic techniques to continually adapt and detect new cyber-attack patterns. And it analyzes potential threats using multiple approaches to examine behavior, code and protocol. TAP also detects threats and risks in cloud-based applications and connects email attacks related to credential theft or other attacks. It does this by using machine learning to observe the patterns, behaviors and techniques used in each episode. TRAP analyzes messages against multiple intelligence systems and shares the results with the security team. TRAP can automatically delete or quarantine messages above a certain risk threshold, or it can provide the security team with the information needed to decide manually. Once analysis identifies a malicious message, TRAP automatically removes the harmful content. And it even follows phishing messages that have been forwarded to distribution lists.

“Before, we were drowning in phishing attacks,” Baillio emphasized. “We needed help reducing not just the quantity of attacks, but also the amount of time spent responding to attacks.”

And there were other critical factors in choosing Proofpoint. The team was looking for the ability to protect cloud- and email-based proprietary data using email-DLP, encryption and CASB. The seamless integration of CASB into the TAP dashboard gave Baillio’s team the end-to-end visibility they sought from their email and cloud security solution.

The Results

Move to Proofpoint yields tangible results

Once they moved to Proofpoint, the OU team saw immediate and concrete results. Proofpoint identified between 50%-70% of all email sent to OU as malicious, bulk or unwanted and stopped it from being delivered to users. From October to December of 2020, for example, OU received more than 108M emails. Proofpoint passed along some 20M of these emails immediately, as they originated from safelist sources. Of the remaining 88M emails, Proofpoint Protection Server with TAP identified almost three-quarters as threats and filtered them out. Only some 25% of the total emails received passed rigorous Proofpoint analysis to be sent on to end users.

Summarized Baillio: “Today we have a single place to go to protect email users, secure critical environments, and react to incidents. We can set one policy in one place to secure all those environments. And with that visibility, we can identify key areas to address. This level of integration has increased our IT team’s productivity. We now see valuable, tangible results.”

LEARN MORE

For more information, visit **proofpoint.com**.