proofpoint

CUSTOMER STORY

The University of the Free State Prevents Malicious Email Attacks with Proofpoint

Proofpoint Enterprise Protection blocks attacks, secures email and ends blocklisting

UFS
UNIVERSITY OF THE FREE STATE
UNIVERSITEIT VAN DIE VRYSTAAT
YUNIVESITHI YA FREISTATA

THE CHALLENGE

- Block phishing and malware attacks on university staff
- Prevent credential theft
- Ensure organisational email stability by preventing blocklisting

THE SOLUTION

- Proofpoint Enterprise Protection
- Proofpoint Targeted Attack Protection

THE RESULTS

- Blocked virtually all phishing and malware attacks
- University email servers no longer blocklisted
- Increased productivity of University staff and IT department

The Organisation

Centred in Bloemfontein, the University of the Free State is one of South Africa's leading universities. Founded in 1904, UFS is a research-led, student-centred, and regionally-engaged university. It contributes to development and social justice through its production of globally competitive graduates and knowledge. And it educates more than 40,000 students and supports over 4,200 staff members at 59 teaching facilities across South Africa.

The Challenge

Stop malicious email attacks and prevent credential theft

Over 90% of all cybersecurity attacks start with an email.[1] And attackers often try multiple ways to breach a user's account. These include brute-force attacks and key-logging software. But phishing emails remain the most effective way cyber criminal steal a user's credentials. Criminal groups operate from multiple countries, and they've become increasingly sophisticated. They attempt to lure users into clicking a malicious link and divulging their confidential account credentials. And they frequently make use of topical events to make their emails appear genuine.

Ernst du Plooy, head of information security, governance, and compliance at UFS, experienced this firsthand. Despite providing comprehensive awareness training in email fraud, university staff members continued to click on phishing links and enter their credentials on unauthorised sites. With these stolen credentials, criminals gained access to employee accounts and farmed staff directory services and address books. They then used this information to send spam from a user's valid account to access their contacts' personal information.

According to du Plooy, "The result was that our email servers were blocklisted several times. This destabilised our entire email system by preventing the delivery of valid emails to external parties."

[1] Verizon. "Data Breach Investigations Report." July 2019.

Given the size and stature of UFS, blocklisting could put the university's reputation in jeopardy. And the non-delivery of critical emails risked interfering with the cooperative research programmes underway with other universities around the world.

Added du Plooy, "We needed to ensure the stability and effectiveness of our official email platform, which is a critical corporate resource."

The Solution

Proofpoint Enterprise Protection halts email fraud

To solve their problem, the UFS security team evaluated several vendors using a rigorous selection process. They began their evaluation by looking at a broad range of criteria. This included functionality, technology, vision, future product direction, ease of use, support services and ease of integration. They particularly sought a supplier that could respond immediately to new threats, using artificial intelligence and a global threat-collection database to identify and stop any known or potentially malicious messages.

After a thorough evaluation, they held head-to-head proof-of-concept trials with their finalists, designed to focus on actual results. As du Plooy stated, "We wanted the product that was the most effective in stopping threats with the least number of false positives."

> "Proofpoint has not only stopped virtually all phishing and malware attacks, but also ensured our email platform's stability, increased our productivity and stopped us from being blocklisted."
>
> **Ernst du Plooy,** head of information security, governance and compliance, University of the Free State

That product was Proofpoint. To solve the specific challenges they faced, the UFS security team based its solution on Proofpoint Enterprise Protection with Targeted Attack Protection (TAP). In addition to the product chosen, a key factor was the local presence of a certified Proofpoint partner. UFS wanted a solution that not only met the technical requirements, but provided in-country support. KHIPU Networks, a trusted Proofpoint partner, fulfilled this role and requirement.

Phishing attempts were growing in sophistication and users' confidential information was at stake. So the UFS security team relies on Proofpoint Enterprise Protection for its ability to identify genuine threats without generating a high number of false positives that can reduce users' productivity. Proofpoint MLX machine learning technology, at the heart of Proofpoint intelligent phishing protection filtering, examines millions of attributes in every email to accurately identify phishing messages. It then quarantines these separately from spam and bulk messages for further administrator review. This approach prevents phishing messages from being forwarded by recipients. And it provides a necessary tool to halt any attack and give the around-the-clock security that the university required.

Proofpoint TAP detects and blocks known and unknown threats. It does this by using a variety of techniques to adapt and identify new cyber attack patterns. These attacks include the use of malicious attachments and URLs designed to install malware or trick users into divulging passwords or other sensitive information. When TAP detects an email that may contain a malicious URL or a dangerous attachment, it blocks the entire message. If a phishing email does get through and the user tries to click the link, TAP prevents the user from going to the site and notifies the security team that the user's machine might be affected. TAP also applies machine learning to observe patterns, behaviours and techniques used in each attack. Armed with new information, TAP learns and adapts. This makes the next attack easier to catch.

These intelligent features proved to be a critical factor in the security team's decision to go with Proofpoint. Proofpoint not only met the team's criteria for an email security solution, but excelled over the competition in the trial. According to du Plooy, "Proofpoint performed best at identifying the real threats while avoiding a lot of false positives. Given our goal of increasing productivity, we felt confident in selecting Proofpoint."

The Results

Proofpoint blocked threats, improved overall stability of email platform and increased productivity

Upon implementation, UFS saw the value of their investment in Proofpoint right from the start. The team and the UFS staff noticed an immediate and significant reduction in malicious email.

"The users are much happier," said du Plooy. "We have had almost no email, spam or malware incidents."

These results have also had a positive impact on the university, particularly regarding risk reduction and business efficiency. Since implementing Proofpoint, the university's email servers have been cleared from any blocklists. And both the staff and the IT team have seen productivity increases.

"Proofpoint has not only stopped virtually all phishing and malware attacks," summarised du Plooy. "It has also ensured our email platform's stability, increased our productivity and stopped us from being blocklisted. In addition having the service and support delivered by a trusted cybersecurity partner, KHIPU Networks has provided UFS with a reliable, managed solution that has delivered on our requirements."

LEARN MORE

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

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity company that protects organisations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data and make their users more resilient against cyber attacks. Leading organisations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media and the web. More information is available at **www.proofpoint.com**.

proofpoint.