proofpoint.

CUSTOMER STORY

New Zealand Ministry of Education Protects Thousands of Schools With Proofpoint

MINISTRY OF EDUCATION
TE TĀHUHU O TE MĀTAURANGA

The Challenge

- Protect students and faculty from email threats
- Balance individual school needs with standardized approach
- Offer email security option at minimal cost to schools

The Solution

- Proofpoint Email Protection
- Proofpoint Targeted Attack Protection

The Results

- Up-to-the-minute email security minimizes advanced threats
- Improved email visibility supports more proactive security
- Proofpoint enables smooth integration with various environments

The Organization

How do you keep a nationwide school system with more than 900,000 students and staff secure? For the New Zealand Ministry of Education, the answer starts with protecting email communications. The organization is the government's lead advisor on the country's education system, shaping direction for agencies and providers to help the government achieve its goals for education.

The Challenge

Protecting student and faculty communications nationwide

In New Zealand, primary and secondary schools and kura (state schools in which teaching is based on Māori cultures and values) continually balance local needs with national standards. Schools in New Zealand operate under their own school board, which is locally elected and specifies many of the rules and operating behavior of schools. But modern email threats can easily extend beyond geographic boundaries, and the New Zealand Ministry of Education realized it needed to offer a standardized option to protect their students, teachers and staff.

“A few years ago, there was a fairly major cybersecurity breach in New Zealand with of one of our district health boards,” said Andrew Hood, chief advisor of cybersecurity at the New Zealand Ministry of Education. “So we were asked what we could do to improve the cybersecurity maturity of New Zealand schools.”

New Zealand schools have the flexibility to choose their own office productivity tools, and generally opt for Google with Workspace Plus or Microsoft 365—or a combination of both. The Ministry of Education pays for licensing, while the schools configure individual tenancies.

"We have approximately 3,500 different Google and Microsoft tenancies spread across our schools," said Hood. "We were concerned that their default out-of-the-box configuration was not doing enough to protect against the kind of email-based threats that we thought were occurring in schools. We couldn't know what threats were hitting our tenancies, but we saw users getting compromised. For example, we were seeing mailboxes being used to generate phishing campaigns and attacks against other schools, and against the wider community. So we were pretty sure something was going on, but we had no insight into it."

The Ministry of Education wanted to offer a centralized solution that campuses could adopt for mail filtering, which would not only remove a significant risk to schools, but would also give the organization better insights into threats.

"We wanted the ability to see statistically what was going on and the volume of attacks that were occurring, to help better advise schools on how to defend against them," said Hood. "We needed a tool that could work in that separate but collective way, and would also work with thousands of different tenancies."

> "Proofpoint Email Protection has been very effective at blocking malicious emails. It enables us to see the types of attacks, and know that our schools are being protected against them."
>
> **Andrew Hood**, chief advisor of cybersecurity, New Zealand Ministry of Education

The Solution

A centralized yet flexible solution for schools

As part of its procurement process, the Ministry of Education performed an in-depth market evaluation to choose the best solution for its schools. After considering factors like compatibility with the schools' Google and Microsoft productivity tools, as well as cost and performance, it chose Proofpoint Email Protection.

"We did a market evaluation and Proofpoint came out as the winner," said Hood. "To deploy the solution to schools, we work with a company called Network for Learning (N4L), a crown-owned company that the Ministry of Education funds to provide digital services into New Zealand schools. N4L rolls it out to schools and acts as that contact point for schools for the service capability."

Email Protection helps schools secure and control their inbound email, using multilayered detection techniques to identify and block malicious email. It also dynamically classifies the latest threats and nuisances. Delivering the solution through N4L was a cost-effective, convenient approach to protecting a large number of schools, fast.

"Approximately 2,500 schools are already dealing with N4L for services like networking and firewalls, so we envisioned Proofpoint as an extension of that," said Hood. "School principals already have a lot of challenges on their plates. Email security shouldn't be one of them. We let them know we can centralize this and look after it for them."

Working with Proofpoint and N4L for deployment was a smooth process, and the Ministry of Education worked closely with the organization to make it easy for schools to support their specific environments and productivity applications. Schools can sign up at any point to use Email Protection, and its primary role is classic mail filtering—taking out and blocking high-risk attack threats that arrive via email.

Proofpoint Targeted Attack Protection (TAP) also plays an important role as part of the solution. It defends against business email compromise (BEC), attachments and cloud-based threats, while providing insights and visibility into targets, to help the Ministry plan more strategically.

“One of our challenges was because schools can manage their own tenancies, we didn’t know what each specific site’s existing Google and Microsoft configuration would be,” said Hood. “We needed to test a number of circumstances for what we believed the schools needed to do to make sure that we got a reliable service. So N4L had to do an extensive amount of variations testing. That took a few months to work through, at which point we started piloting some schools on the service. And then we started a quick ramp-up process. Within nine months, we had gotten 60% of schools signed up for the service.”

The Results

Gaining protection and deeper visibility

As more schools continue to adopt Email Protection, the Ministry of Education is acquiring strong insights into the volume and types of threats its schools face—and proactively stopping them before they can reach students or staff.

“The numbers show us just how much Proofpoint is needed,” said Hood. “We tend to run somewhere between 80 and 100 million messages a month through the platform. Most are blocked as low-grade spam, but a disturbing number of them—approximately 80,000 to 100,000—are threats that we’re taking out of the Proofpoint detonation chambers. We’re finding malicious URLs and content that requires more advanced scanning to pick up, and that’s what Proofpoint does. The biggest success of this is being able to demonstrate each time a threat has been blocked, and it has not reached a mailbox and tempted a user to click.”

Email Protection protects New Zealand schools with stronger email security. “We’ve had no issues with faculty and staff seeing delays or performance issues,” said Hood.

Proofpoint not only blocks threats as they emerge, but it enables the Ministry of Education and the schools it supports to move to a more proactive security posture.

“We have N4L monitoring the platform, and they have been doing a lot of work with Proofpoint around API integration—they can actually ingest the logs from Proofpoint into their security operations center,” said Hood. “They are looking for unusual behaviors and patterns, such as sudden spikes in certain types of attacks. These insights also give us the ability to know whether a school has engaged with a potentially malicious email. We can proactively go to the school and say, ‘We’ve seen you doing something, we believe it’s high risk, and you might need to take some action.’”

With its centralized solution in place, the Ministry of Education has freed educators and administrators to focus more on learning, instead of cybersecurity.

The Proofpoint Attack Index provided by TAP also helps identify Very Attacked People™ (VAPs) to help the Ministry identify top targets, and keep them apprised of threats.

“Being able to look at the VAP list and correlate people who are being attacked with public sources of email addresses for schools gives us insight into attackers’ behavior,” said Hood.

“Proofpoint offers us a more cost-effective way of email filtering, while removing that burden on the school,” said Hood. “Individual campuses don’t have to worry about configuration and keeping it up to date, or worry about the latest threats. They know a solution is there, it’s protecting them, and it’s doing a great job.”

LEARN MORE

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

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations’ 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 organizations of all sizes, including 85 percent of the Fortune 100, 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.