Proofpoint Helps Leading Australian Governance Organization Protect Employees and Citizens

Australian Institute *of* Company Directors

The Challenge

- Protect organization from malware and threats
- Nurture a culture of risk minimization
- Tailor protection for high-profile employees

The Solution

- Proofpoint Email Protection
- Proofpoint Targeted Attack Protection
- Proofpoint Email Fraud Defense
- Proofpoint Security Awareness Training
- Proofpoint Threat Response Auto-Pull
- Proofpoint Internal Mail Defense

The Results

- Protects organization from more than 3 million threats, including targeted attacks
- Insight into employee behavior enhances best practices for security awareness
- Automation capabilities save equivalent of 1.5 full-time employees

The Organization

For a governance company like the Australian Institute of Company Directors (AICD), strong cybersecurity protects not only its employees, but its citizens. Proofpoint solutions help AICD mimize risk, and free up its limited resources to focus on strategic issues.

The Challenge

Strengthening the brand of a trusted advisor

AICD was created to help leaders run their organizations better, providing education and advice, as well as advocating on critical issues on behalf of members. For example, as host of the Australian chapter of the Climate Governance Initiative, AICD supports implementing high quality, climate reporting to help drive national emissions reduction targets.

As a trusted voice of governance, AICD sustains ongoing relationships with a broad community of leaders. Maintaining the reputation of its brand, and protecting it from abuse, are top of mind for the organization's IT group. And stopping email threats like phishing attacks is critical to its cybersecurity strategy.

"Given today's threat landscape, you have to assume that your organization will be breached," said Marco Figueroa, senior manager for cybersecurity and compliance at AICD. "If that happens, and the attack is not detected at the gateway, you need to consider how you will recover, and how quickly can you automate that process."

AICD was seeking a security solution that could protect its Microsoft 365 environment against today's advanced attacks. It also had to be able to proactively respond to them in an automated way.

"For us, automation is paramount," said Figueroa. "We have a very small organization, and we need to enable processes that can work seamlessly by themselves, giving us the results and the outcomes that we want to see. I want to come in each morning and be able to see that we have stopped several malicious events, and tracked them."

The Solution

Mitigating phishing and other threats

The AICD team looked at a variety of options in its search. They chose a complete email security solution that featured Proofpoint Email Protection, Proofpoint Targeted Attack Protection (TAP), and Proofpoint Threat Response Auto-Pull (TRAP).

"First we started with email filtering, and then we augmented it with advanced threat protection," said Figueroa. "We also use TRAP, which is a fantastic piece of functionality. If a phishing attack comes along and it's not able to be caught at the gateway, we can retrieve that email and delete it from Microsoft 365. We use that all the time, because the phishing threat is real, and it often comes when everybody's asleep. The automation of those two capabilities, and the synchronization with Microsoft 365 is fantastic."

"We don't have the resources that you will find in larger organizations, so for us, automation is the key to every solution. Proofpoint automation capabilities are saving us approximately one and a half head count."

Marco Figueroa, Senior manager for cybersecurity and compliance, Australian Institute of Company Directors

The team also deployed Proofpoint Email Fraud Defense to help protect the brand from being abused in email fraud attacks. What's more, Proofpoint helps simplify its Domain-based Message Authentication, Reporting, and Conformance (DMARC) implementation. The company gets guided workflows for every step of the rollout as well as support from knowledgeable consultants.

Figueroa and his team were looking for a sustainable, comprehensive solution that was based not only on security technology, but could also provide them with continual user education on best practices across the entire company. With Proofpoint Security Awareness Training, AICD could take a more proactive security approach with a proven adaptive learning framework. It gives users a more personalized learning experience, and at the same time, it considers user vulnerability and security culture. It also drives behavior change and tracks program performance to continually improve the process.

"Before coming to Proofpoint, we were using an external piece of software that was used for the purposes of phishing more than training, and it was not complete," said Figueroa. "Now we have a fully integrated system."

The Results

Creating a strategic focus on risk management

Together, Proofpoint email security solutions have provided protection against a massive flood of email attacks. In a recent Security Review and Health Check of 3.7 million inbound emails, 80,000 known threats such as phishing attacks, viruses, spam and imposter attacks were blocked over a 90-day period. More than 7,000 targeted threats such as malicious attachments were stopped. And 3.2 million messages were blocked based on IP reputation alone.

If a harmful threat should slip through, TRAP responds with orchestration and automation capabilities to retract malicious emails delivered to user inboxes.

"We needed the ability to retrieve and then delete the email from Microsoft 365 for our environment," said Figueroa. "With Proofpoint TRAP, we're able to do that. It's fairly simple, and it's done automatically. We come in in the morning, review the exception report, and it's all done. There's nothing more to do."

Advanced, customizable Proofpoint Security Awareness Training complements the advanced security technology, providing the broad solution that Figueroa required.

"Proofpoint Security Awareness Training gives us the opportunity to influence better behavior, because at the end of the day, you are on the right track for success, and that's important," said Figueroa. "That's an area where Proofpoint offers substantial value."

Another feature of TAP is the ability for the company to identify its Very Attacked People™ (VAPs). And it provides adaptive, proactive security for the most at-risk users. A recent Proofpoint Security Review and Health Check identified more than 50 VAPs who were nearly three times more likely to be attacked than typical users in the organization.

"Sometimes human behavior can be unpredictable, and Proofpoint gives us insight into those individuals who are being hit the most," said Figueroa. "This allows us to look at the pattern and come up with a more meaningful Security Awareness Training program. We're linking the human behavior with what we observe in terms of threats. And once we determine who are the most vulnerable, then we can put additional protections in place. That is the beauty of the solution."

Together, Proofpoint solutions and training are enabling AICD to focus on more than simply compliance. Now it can forge a stronger culture and strategy that is dedicated to minimizing risk over the long term.

LEARN MORE

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

---

proofpoint.