proofpoint.

SA Power Networks Stops Threats and Forges Stronger Security Culture With Proofpoint

SA Power Networks

The Challenge
- Stop phishing and other advanced attacks
- Foster a proactive culture of security
- Protect vital energy infrastructure systems

The Solution
- Proofpoint Email Protection
- Proofpoint Targeted Attack Protection
- Proofpoint Threat Response Auto-Pull
- Proofpoint Security Awareness

The Results
- Effective, automated solution reduces email threats and manual analysis
- Training extends security best practices across entire company
- Security insights helps ensure government regulatory compliance

The Organization

More than 1.7 million customers in South Australia depend on SA Power Networks to build and maintain their energy infrastructure. This leading utility takes its responsibility to all these customers extremely seriously. So it turned to Proofpoint to minimize risk to email—and the entire organization.

The Challenge

Protecting Australia's vital energy grid

SA Power Networks employs more than 2,000 people and supplies power to local households and businesses across the region. Its network infrastructure is key to keeping the lights on for customers, and helping staff stay productive. And to keep its operations safe, the company knows a key focus of its security strategy is email.

"Protection of email is critical to protecting our end users," said Nathan Morelli, head of cybersecurity and IT resilience at SA Power Networks. "Like most organizations, our end users are our weakest point, and they will likely get phished. We think that 70 to 80% of our threats come from phishing. So it's important for us to stop potential entry points for ransomware or business email compromise (BEC) attacks from bad actors."

Like most organizations, SA Power Networks, faces resource constraints. That means it needs to do what it can to free its staff from time-consuming, manual security processes.

"During my first six months at SA Power Networks, we had two analysts just responding to phishing emails," said Lindbergh Caldeira, manager, cybersecurity operations at SA Power Networks. "One of our biggest challenges was how to get a bit more control over that."

"Automation is critical to our evolution," added Morelli. "In our current financial environment, we don't have endless buckets of money. That means we're always looking to find efficiencies to minimize our time to detect and respond to threats."

Thankfully, SA Power Networks had never experienced a serious phishing attack. But the company knew it was important to strengthen its email security to avoid becoming a victim. Morelli and his team needed a solution that provided advanced, automated email security. It also needed best practice training and knowledge sharing that it could apply across the company.

"We've come a long way with what we have accomplished in our awareness program, and we've seen real results with Proofpoint. Over the past three years, we've seen an 80% decrease in people entering passwords into our phishing exercises."

Nathan Morelli, head of cybersecurity and IT resilience, SA Power Networks

The Solution

Building a more risk-aware company
To provide the protection the company needed against phishing, malware, ransomware and other advanced attacks, SA Power Networks deployed Proofpoint Targeted Attack Protection (TAP). TAP stops both known and never-before-seen attacks, building on Proofpoint threat visibility from more than 200,000 customers.

The utility also deployed Proofpoint Threat Response Auto-Pull (TRAP). This enables Morelli and his team to streamline email incident response processes. When malicious emails are detected, TRAP will analyze and automatically remove them. Even after an unwanted email has reached a user, TRAP will quarantine that email and any other instances of the message across the organization.

Morelli and his team understand that it takes more than intelligent technology to provide a robust security posture. Strong best practices are also a key element. Proofpoint Security Awareness offers tailored online cybersecurity education that's targeted to the specific needs and vulnerabilities of all its users.

"Our organization is about 40% office workers and 60% field workers," said Morelli. "Office workers are generally digital natives, while field workers are more hands-on. That means there's a different education process needed for each group and their different journeys. Proofpoint lets us build a program around that and gives us multiple ways of educating our users."

The Results

Better compliance and faster, smarter processes

Proofpoint TRAP has delivered impressive results through its multilayered email protection and analysis. With its Closed-Loop Email Analysis and Response (CLEAR) workflows, TRAP allows the company's users to quickly identify and report potentially malicious emails. All reported emails are sent to an abuse mailbox, and then automatically analyzed against Proofpoint Threat Intelligence and other sources to see if they contain malicious content.

"When Proofpoint TRAP discovers phishing, it still goes through an analysis engine after someone reports it," said Caldeira. "That analysis engine helps us reduce our manual steps. We have someone who's recently joined our team from the service desk. That person has been able to go into the system and pick it up really fast, and work through the tickets without much involvement."

"Our previous solution required manual checking, and we'd probably be responding to something like 20 to 30 emails a day," added Karley Donnelly, cybersecurity analyst at SA Power Networks. "Now, since moving to the CLEAR process with Proofpoint automation, we usually have fewer than ten emails that require our intervention each day. The volume of emails we need to look at has gone down so much and has made the whole process of getting them cleared out each day a lot faster."

Proofpoint Security Awareness augments the company's security technology, and it enables SA Power Networks to mobilize more than 2,000 users to track suspicious emails, with impressive results.

"Our human sensors provide some of our strongest early protection," said Morelli. "We had 3,758 suspicious emails reported last year. And 3,602 of those were malicious."

Security regulations are another top concern for a critical infrastructure provider like SA Power Networks. Proofpoint helps provide the company with the visibility and insights it needed to keep pace with mandates and verify compliance.

"We have to align to the Australian Energy Sector Cybersecurity Framework, which is mandated through government regulation," said Morelli. "Proofpoint and its dashboards are really good at telling us how well we align our awareness to the threats we are currently seeing, and then providing us with an evidence chain."

With Proofpoint quarterly service reviews, SA Power Networks is also gaining insights into its overall security posture. And now it can better understand its risks and strengthen its entire strategy.

"Proofpoint quarterly service reviews are really valuable for us in terms of getting feedback about how we've configured the product, and what's coming up," said Morelli. "We've shared those insights with our other vendors, such as CrowdStrike, to let them know what we need from their security solutions."

With Proofpoint security and training in place, SA Power Networks has the protection it needs. And now the company can spend more time focusing on providing dependable energy to people and businesses, and less time worrying about cyber threats.

LEARN MORE

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

---

proofpoint.