SMX INTEGRATES VADE ACROSS ITS EMAIL SECURITY, ARCHIVING, AND PLATFORM SOLUTIONS AND SERVICES

Partnering with Vade improved phishing catch rates and helped to evolve the SMX product line.

ABOUT SMX

SMX is the largest locally owned and operated provider of email security for companies, government departments, and organizations in New Zealand. With more than one thousand customers and one million mailboxes protected across New Zealand alone, SMX provides cloud email filtering, compliance and archiving software, as well as managed services, email security, and hosting for telcos.

THE CHALLENGE

SMX successfully migrated the largest telco in New Zealand to its own email management platform purpose-built for the customer. However, while the initial email security product layered into the platform was sufficient at filtering spam, it struggled to address a new wave of dynamic threats, including phishing emails, which were increasing exponentially.

New Zealand-based phishing attacks in particular were escalating. “What we find in New Zealand,” said Jamie Callaghan, product manager at SMX, “is that we are typically the first to see a lot of threats. We’re almost a test platform before things go global.”

With a population of around 5 million, New Zealand has a small but established group of brands that consumers trust, including supermarkets and telecommunications providers. Rewards-based phishing emails impersonating those trusted brands were increasingly targeted and personalized for consumers who had signed up for email alerts and other subscriptions.

Continual adaptations to the current solution were required to address the growing sophistication of phishing emails. “We spent considerable time working with the vendor and countless operational hours addressing the issue,” said Callaghan. This was not sustainable, and it became clear another level of analysis was required, said Callaghan. SMX decided that they needed to implement a second, more modern solution.

SOLUTION

To solve the issue, SMX began searching for a new email security filter. Among the evaluation criteria, a modern, automated approach to email security topped the list: “We were looking for a new breed of engine, said Callaghan, “a solution that protects us and looks at new threats in a different way.”

What SMX did not want was a traditional solution that relies on fingerprint-based

WHY SMX CHOSE VADE

- ✓ Improved catch rates
- ✓ Ability to fine-tune the engine
- ✓ Personalized support and account services
- ✓ Granular reporting

detection to block email threats. Those legacy solutions, Callaghan said, led to a delay between new threats going out and engines ultimately catching up. "We needed to reduce that lag time."

Vade's Content Filtering SDK leverages artificial intelligence and heuristics-based behavioral analysis to block dynamic email threats, including phishing, malware, and spear phishing. Combining local and global analysis, the Content Filter SDK examines the origin, content, and context of emails to block dynamic email threats and classify graymail. More than ten elements of emails and webpages are computed via heuristic analysis and artificial intelligence to render a verdict on safety and classification.

RESULTS

During POC, SMX saw immediate results in phishing detection. "Vade solved the problem," Callaghan said. "But there was the consequence of false positives." To solve the issue, SMX worked closely with Vade on adjusting the filter to adapt to the customer's email environment—as well as the nuances of the region.

"We worked with Vade to fine-tune the engine to the New Zealand landscape," Callaghan said. Words and keywords specific to the region, for example, were used to train the engine. "Vade has a great way of profiling the platform, learning from what it sees, and finding a good balance between detecting unwanted emails and ensuring we don't reject legitimate emails."

"Vade has a great way of profiling the platform, learning from what it sees, and finding a good balance between detecting unwanted emails and ensuring we don't reject legitimate emails."

In addition to reporting an increase in catch rate, SMX reports a significant reduction in escalation and support from their customer. Overall, Callaghan said, the reduction in escalation and support requests provides a cost advantage and reduces reputational risk.

SMX has a layered approach to email security, allowing them to stack Vade with other solutions and provide more comprehensive protection to their customers. "We take threat indicators from Vade alongside other vendors and use a combination of three or four layers to protect the customer."

As a result of the success of the project, SMX decided to integrate Vade's content filter into its multi-tenanted business platform for its telco customer and into its own SMX multi-tenanted business platform that sits across New Zealand and Australia. "On those platforms, we were already using two engines. Because we had seen the value of the more modern detection of Vade, we swapped one engine for Vade. It was a pretty simple decision based on raw catch rates."

"Vade helped us evolve from binary decision-making in threat detection and evolve our product as a whole, helping us develop a customized, linear approach—an evolution of our own product using Vade."

SMX worked closely with Vade to adjust the filter to SMX's business customers. It's financial services customers, in particular, see high levels of email traffic related to financial transactions, which can set off red flags and cause false positives. "They are very sensitive when it comes to blocking legitimate email. We worked closely with the customer and with Vade to resolve false positives," Callaghan said, "We turned off and on a number of rules to make things more lenient and fine tune the SMX business profile for our customers."

SMX ultimately integrated Vade into several other SMX products and services, including quarantining, URL Analysis, and SMX's advanced rules-based engine that feeds in indicators and conditions that allow businesses to implement data loss prevention and compliance policies.

"Vade helped us evolve from binary decision-making in threat detection and evolve our product as a whole, helping us develop a customized, linear approach—an evolution of our own product using Vade."

Additionally, SMX integrated Vade's reporting capabilities into its products, Callaghan said, because it offers a high level of detail and provides more granularity about email categorization—results and verdicts. "We can show our customers the types of threats they're seeing and show them their risk profile. It's important to SMX to communicate the value we offer our customers, and the information provided by Vade helps us with that."

Finally, it was the combination of people and technology that ultimately made the project successful—a personalized approach to both email security and account services.

"The catch rate of New Zealand-based phishing attacks—that's what your competition could not deliver at the time. And the support and account services that we have with Vade is very good. We get very good levels of personalized report. We definitely do not get that from our other vendors."

Jamie Callaghan, Product Manager, SMX