CASE STUDY

Cofense Case Study

Home Security Giant Tabs Cofense for Phishing Defense Program

COFENSE

Cofense Case Study

COFENSE AND HOME SECURITY GIANT

Background

As one of the biggest home protection brands in North America, ADT Security Services is synonymous with security. When it came to building their enterprise wide phishing defense program, the company knew it needed to partner with a proven leader with the ability to scale to meet ADT's evolving security needs.

Cofense quickly became the clear choice as ADT's partner in phishing defense. Jerry Magginnis, an ADT security architect, was familiar with Cofense's phishing simulation and behavior conditioning technology, having worked with the vendor at a previous job. There, he had seen Cofense PhishMe® significantly decrease phishing attacks. "When I joined ADT, I shared my previous experience and success with Cofense with my new management team," he recalls.

Executive Summary

Client: Home Security Services, a $3.4 billion electronic security provider

Challenges: Build a scalable, anti-phishing program to reduce attack susceptibility

Solutions: Cofense PhishMe, Cofense Reporter

Results: Reducing time allocated to stopping phishing threats, improving susceptibility rates across the enterprise

Challenges

As a large organization with more than 20,000 employees across North America, Magginnis says ADT needed an industrial-strength solution to help prevent phishing attacks.

Cofense PhishMe is an easy-to-use and effective SaaS solution that instructs users on the dangers of phishing by periodically testing them with simulated phishes and supplying immersive training content for users during the simulation. When users receive a simulated phish, they must decide whether the email is legitimate or report it as a suspected phish. This teaches them to recognize the telltale signs of phishing emails, and soon they become adept at identifying and reporting phishes.

> "It simply came down to who is the most advanced in the industry and who is the most effective. We felt that Cofense is the clear leader in this space."
>
> **Tom Dennison, Chief Information Security Officer, ADT Security Services**

Having worked with Cofense before, Magginnis was familiar with the content quality and scalability that Cofense provides, so he didn't hesitate to recommend it when the subject was raised. Still, ADT had to issue an RFP as per company policy. Tom Dennison, Chief Information Security Officer at ADT was involved in the early RFP stages, but soon identified that Cofense stood out from the competition. "It simply came down to who is the most advanced in the industry and who is the most effective," notes Dennison. "We felt that Cofense is the clear leader in this space."

Solutions

Smooth Rollout

Having made the decision to implement Cofense PhishMe, ADT developed a phased rollout plan that included an initial implementation limited to the 20 members of the IT security department. A rollout to the 200-employee IT staff followed. The next phase covered about 1,000 employees at company headquarters, after which Cofense PhishMe was implemented company-wise. Currently 21,000 employees are using it, and another 4,000 from a recent acquisition soon will be added.

This methodical approach allowed the security team to evaluate users' responses and make adjustments as needed. "You want to make sure that you have a successful launch, and that you've worked out all the details," Magginnis says.

Thus, the user adoption for Cofense across the organization has been quite positive. If the launch went awry, it would irritate users, who would question the program's value, he says. "You really want people to embrace it and feel they're getting value as opposed to being bothered by it. We involved all the tech teams, and the legal and HR staff as well. They all felt all involved. And since we did that early, they all felt like they were partners in the process."

That's why the security team started small – and used itself as guinea pigs. "Along the way, we kind of worked out any potential issues and decided what the future content of the program was going to be," Magginnis says.

The first simulation brought relief and confirmation because the solution worked "exactly like you think it's going to work" and proved to be "as easy as it looks," Magginnis adds. "That's a huge feeling of success."

Crafting Successful Scenarios

That first simulation targeted the security team and consisted of a fake email pretending to be an installation of Microsoft Office 365, which the company was in the midst of rolling out. It was a custom scenario created by the security team – one they knew would work well. ADT has since used a combination of custom and Cofense pre-set scenarios in subsequent simulations. With each one, Magginnis says, susceptibility to phishing has decreased.

In addition to Cofense PhishMe, ADT has rolled out Cofense Reporter®, which organizes and normalizes user reports of phishing attempts to strengthen threat-detection capabilities. Reporter works by placing a button on emails that users can click whenever they suspect a phish. The email is then routed to the security team, which checks if it is a simulation, a legitimate email or a phish.

Before deploying Cofense Reporter, users had to create attachments of suspicious emails that they then would send to the security team. "That's quite a bit to ask of most users – and not always done correctly." The button makes the whole process easier, and users get an immediate response after clicking it. When users correctly report a simulated or real phish, they receive a "job well done" acknowledgment.

Business Results

Quick ROI

The anti-phishing program has been well received, Magginnis says. “From our CEO on down, everyone recognizes the value of this because even the executives themselves have been subject to phishing attacks.”

Dennison and other technology management have been so pleased with the initial anti-phishing program that approvals have been granted to expand the program. ADT is exploring adding Cofense Triage™, which automates prioritization, analysis and response to phishing threats. “Improving our incident response efforts is a major priority for us,” notes Dennison. “Cofense Triage provides opportunities to clearly automate and prioritize threats that could positively impact incident response times.” The company also has augmented its anti-phishing efforts by asking users to take advantage of Cofense’s complimentary computer based training modules explaining the dangers of phishing.

As for a return on investment, the Cofense solutions already have proven their worth by reducing staff time allocated to responding to phishing threats. According to Magginnis, those staff hours have been cut in half. “This isn’t conjecture. We’ve made the calculations based on the lost productivity due to time spent by the mail, proxy and SOC groups on phishing attack responses.”

> “Cofense has cut our incident response time in half, based on calculations we’ve made to avoid losing productivity.”
>
> **Jerry Magginnis, Security Architect, ADT Security Services**

Conclusion

Magginnis enjoyed a positive experience working with Cofense staff and engineers taking the anti-phishing program from deployment to maturity. “Since the initial rollout, the Cofense support team has proven always helpful and accessible, making sure we’re crossing all the Ts and dotting the Is. The results speak for themselves.”

Magginnis has high praise for the Cofense team. “There seems to be a special culture at Cofense. You find people that genuinely care and put the word ‘partner’ back into the relationship. We’ve really partnered with Cofense because they’re willing to do whatever it takes to help us create an anti-phishing culture at ADT.”

Thanks to the combination of technology and people, Magginnis would be glad to recommend Cofense to any of his peers.

COFENSE

W: cofense.com/contact **T:** 703.652.0717
A: 1602 Village Market Blvd, SE #400
Leesburg, VA 20175