CASE STUDY

Reducing Phishing Threats

Fortune 100 Software Company Uses Microsoft Office 365 and Agari to Eliminate C-Suite Imposter Attacks

Executive Summary

A Fortune 100 global technology company selected Agari to protect its executives from being impersonated and to curtail phishing attacks. Email security has the attention of the most senior-level executives because of the perception risks that occur when an attack is successful. By implementing Agari Brand Protection™ and Agari Phishing Defense™, they gained greater insight into its data. Not only is the company improving its ability to protect its brand from being used to trick consumers and from inbound phishing attacks, but also it is able to have detailed insight into what is happening.

The company first migrated to Microsoft Office 365 and then selected Agari to protect employees and provide the company with a powerful one-two, cloud-native punch without the requirements of a traditional secure email gateway.

> "I am able to show how the efficacy is at its highest, when it is Microsoft Office 365 plus Agari, and with that equation there is no requirement to have a legacy hardware-based SEG, which saves money."

Company Snapshot

Industry

- Software

Environment

- 156,000+ global mailboxes
- 365 company-owned domains
- Microsoft Office 365 with Exchange Online Protection
- 96% of mailboxes are in the cloud, but 4% remain on-premises due to customer requirements

Challenges

- Business email compromise and advanced email phishing attacks through executive impersonation
- Brand domain abuse, including brand spoofing and executive impersonation

Solution

- Agari Phishing Defense™
- Agari Brand Protection™

Results

- The efficiencies generated reduced the amount of time employees and SOC analysts spent on identifying and triaging phishing attacks

Murky Waters in Email Security

Email security continues to become more complicated. Nearly 30 percent of advanced email attacks now launch from compromised accounts of trusted individuals, while another 50 percent are sent using display name deception. These statistics define the current operating-environment reality for all companies, in every industry around the world.

These increasing threats ultimately became a motivating factor for the company to shore up its brand reputation by selecting and implementing advanced email security technology innovated by Agari. The reality is a cautionary tale for other companies and security professionals, demonstrating the blunt-force impact malicious actors can have on a business when gold-standard precautions are not taken.

When the CEO or business-level president is impersonated, customers learn not to trust the emails coming from the brand. “Email security has the attention of the CEO and the presidents of our various business units,” said the global service manager for messaging. “That is because they are the ones most impacted by a cybersecurity incident. When an executive’s name and title are used through the email channel to deceive, it’s a perception issue. It causes people not to trust their emails and slows down getting business done, or worse, people act on the content in the email and cost the company money.”

Starting with DMARC to Protect Customers

Shortly after migrating to Microsoft Office 365, the company began exploring security companies specializing in email authentication by leveraging the DMARC standard. With a nod from Gartner and a successful proof of value effort, they ultimately selected Agari as its trusted email security partner of choice. The company has a complex email infrastructure, as do most global companies.

The company attempted a DMARC implementation three years prior without success because they were not ready, and the supplier did not understand DMARC and was ultimately unable to deliver what it promised. To prepare this time around, they onboarded Agari, a strategic move that has proven to be fruitful. “We now have the partner with the right tools, skill set, and knowledge to help with our global implementation. Plus, we’re working with the company whose CEO invented DMARC,” the global service manager said.

He went on to say that, “Like most companies today, we are widely exposed to cybersecurity threats from the external world. Those threats flow through the email channel and take the form of spoofing, phishing, and, of course, brand abuse and executive impersonation.”

He continued, "executive leadership raised the problem and wanted to see significant improvement in the fight to protect our domains from malicious email threats." The plan, as originally envisioned, was to focus on reducing brand abuse by implementing Agari Brand Protection, a technology that would ensure email sending domains implement a DMARC policy at *p=reject* to stop malicious emails from ending up in the inboxes of consumers. "As we dug in, though, we discovered that it needed to be more of an extended project. And so we implemented Agari Phishing Defense™, too." By using both products, we are protecting customers from attacks using our domains and protecting employees from business email compromise, executive spoofing, and other advanced attacks.

Eliminating Cyber Threats Across the Organization

The company tested Agari Brand Protection during 2018 and moved into full deployment in March 2019, while adding Agari Phishing Defense a few months later. The company is securing its entire cloud email ecosystem as the industry goes through significant changes. While the company uses a multi-layered approach for its general security protocols, it leverages an impactful one-two punch approach for email security. In other words, the organization does not have a secure email gateway, simply because it no longer needs one. The combination of Microsoft Office 365 and the Secure Email Cloud has significantly reduced email threats being delivered to customers, employees, and partners and has reduced costs so that funds can be deployed in other parts of security operations.

Meaningful results have been recognized already, said the global service manager, speaking for his global team of more than 40 people. "With the reduction of attacks, we have driven efficiencies throughout the company. Our employees and our SOC analysts are more productive because we have reduced the number of phishing attacks. They are spending less time addressing issues in the email security area," he said. Leveraging Agari Phishing Defense on top of Microsoft Exchange Online Protection has proven to be a best practice.

Furthermore, Agari Brand Protection is enabling consistency within the company's email channel. They have thousands of legacy senders with complicated configurations, and in total, it owns 365 domains, all of which it sought to get to *p=reject*. This effort took on even more importance because they are in the midst of a rebranding effort. The company is aggressively repositioning its brand from the industrials category to the software category. This fundamental strategic shift meant that their domain had to be protected. The global service manager stated, "LinkedIn has a DMARC record, and I've never seen a fake LinkedIn email. We needed to implement the same thing with our domain."

> "Agari provides us with the granularity of data that we couldn't get elsewhere. Through its reporting, Agari is helping us understand what's going on so that we know what a trusted sender looks like or a trusted source as well as DKIM, SPF, and other DMARC attributes."

Lessons Learned Through Data

By implementing Agari Brand Protection and Agari Phishing Defense, the company was able to have greater insight into its data. Not only is the company improving its ability to protect its brand from being used to trick consumers and from inbound phishing attacks, but also it is able to have detailed insight into what is happening. "The Agari tools gave us great information about inbound traffic," the global service manager explained. "And that was the first time we were actually able to see and understand what was proactively attacking us. All the good and bad traffic is now visible to us."

When asked what he was doing with the data, the global service manager explained, "Currently, we are digging through all of the data to see what we have, and we are working to tune our process." This information enables us with our cyber incident response efforts. "If there is an issue, we address it using Agari. We are learning from history; whatever we see through Agari consoles, we are building new policies and protecting our executives. Agari is helping us also to improve our Microsoft Exchange Online Protection console, which is a benefit of having Microsoft and Agari coupled."

> "In Agari, we see our environment naked, stripped from all other rules and that is helping us improve our default gateway. Agari enables us to see simple things that should have been caught at the default level."

Quantifying the cost savings is the next step for the company, according to the global service manager.

In summary, he believes that the reference architecture of choice is Microsoft Exchange Online Protection coupled with Agari. "I am able to show how the efficacy is at its highest when it is Microsoft Office 365 plus Agari, and with that equation, there is no requirement to have a legacy hardware-based SEG, which saves us money."

The value of stronger email authentication and email security became even more apparent when the CSO was impersonated. Bad actors commandeered the CSO's identity with the intention of doing harm by perpetrating fraud. Emails asking for money were sent to more than 40,000 people in the ruse that leveraged the CSO's name and email address and exposed the company brand to abuse. "I told the executives that with Agari, the CSO's executive impersonation attack wouldn't have happened," the global service manager said.

Learn More
www.agari.com