COMPANY
LendingHome

INDUSTRY
FinTech

PRODUCT
Area 1 Horizon Email Protection

SECURITY ISSUE
BEC Phishing Attacks

CUSTOMER STORY

Area 1 Security Keeps LendingHome's Email Clean and Free of Phishing Threats

BACKGROUND

As an innovative and growing financial technology startup, LendingHome is concerned about email vulnerability to phishing attacks. Email is a key resource for the company, which has funded more than $1 billion in loans to date. The company has enabled homebuyers to finance more than 5,000 homes while returning $540 million to its investors.

LendingHome turned to Area 1 Security to protect the integrity of its email, realizing how phishing attacks opened the door to Business Email Compromise (BEC) and other frauds. BEC allows a criminal gang to pose as a company officer and swindle users into forwarding company funds or confidential data.

"We can't exaggerate the importance of keeping those clever ploys and phishing messages from landing in front of our staff." said Donovan Bray, Senior DevOps Manager.

"Freeing employees from the need to examine, report, and authenticate suspicious emails lets them focus on their core roles and responsibilities, all while knowing that their email is safe."

CHALLENGE

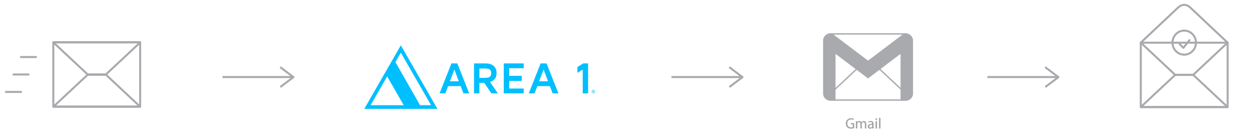
LendingHome knew that it was only a matter of time until the company became a target for spear-phishing emails. Worse, it could also be only a matter of time until one of those attacks succeeded. For every ten phish sent out, it takes just a minute and forty seconds before one of the recipients clicks on a malicious link, for example. So the company needed a robust, innovative solution to detect incoming attacks and neutralize the danger.

LendingHome started with using Google's Gmail system alone, believing that Gmail's spam filter and rules would catch phishing emails in addition to spam. But that was far from true. **Even the best spam filter is not engineered to recognize highly targeted phishing emails.** Unlike the avalanches of spam released 24/7, which can be flagged and filtered effectively, phishing campaigns are extremely sophisticated. They are purposely constructed to present a low-volume attack profile that doesn't appear on a spam filter's "radar." So hackers can actually steal right past spam defenses and arrive in employee inboxes with an apparently innocent request.

The attackers often do their homework and appear to know the company well. This ability to masquerade as legitimate communication is one of the many reasons why phishing is responsible for 97 percent of breaches causing unrecoverable losses in the billions.

In addition to BEC, phishing is the root cause for a spectrum of email attacks. **Two notorious phishing attacks faced by companies in 2017 were the DocuSign malware and the "Google Docs" worm** — which posed as email from a trusted contact and tricked users into yielding their permissions, while infecting their contacts too. Relying on a spam filter alone to find and stop phish is similar to leaving doors and windows unlocked when a burglar is in the neighborhood.

In addition to the danger of phishing itself, LendingHome employees had to take the time to report potential phishing attempts to Information Security.



INCOMING MAIL → BLOCK TARGETED PHISHING ATTACKS → MAILBOX ANTI-SPAM, ANTI-VIRUS → USER INBOX

SOLUTION

LendingHome reviewed a number of anti-phishing solutions before turning to Area 1 Security. Of course they had employee training to recognize phishing attacks, but they wanted to ensure they had the highest levels of protection. So they decided to augment their efforts with Area 1 Security's powerful preemptive capabilities, and keep phishing emails from arriving in employees' inboxes. Although training can lower malicious intrusions to 30 percent of their previous figure, just one click on a phishing email can result in a catastrophe, which makes the figure of 30 percent far from reassuring.

With Area 1 Security, phishing attacks are comprehensively and preemptively stopped. The service acts upon live attacks, which are discovered globally using distributed sensors at specific attack relay points. **Sophisticated analytics and innovative web crawling capabilities deliver advance visibility into emerging and active phishing threats,** so they can be proactively shut down before even reaching LendingHome's perimeter. The company also appreciates Area 1 Security's push notifications that warn of phish in real time, as well as the versatile dashboard.

LendingHome wanted to keep users from being bombarded by suspicious emails and expending time and energy to evaluate messages that could be phishing. Yet, each one had to be checked, because phish are getting more and more professional.

RESULTS

"I'm happy to say that Area 1 Security exceeded all of our expectations," Donovan says. **"It took less than half an hour to get the service up and running."**

Results were assessed by how often a user reaches out with suspect email to be investigated. LendingHome now goes weeks without a single report—instead of multiple reports per day as in the past. It would have been impossible to reach someone at Google to report the problem—much less having a resolution immediately in place.

> **"Even though Google spam filtering does an okay job, we now see plenty of malicious emails caught by Area 1 Security after passing through Gmail's filters," Donovan says.**
>
> Donovan, Senior DevOps Manager

Phishing and spoofing are two areas where LendingHome sees a big improvement in Area 1 Security's service versus Google spam filtering alone. Now, the company sends all malicious, suspicious, and spoof emails automatically to Google quarantine, saving substantial time.

Prior to Area 1 Security, even with Google's Gsuite Spam and Phishing rules, far too many phishing attempts made it to user inboxes. Now, thanks to Area 1 Security's hyper-vigilance and effectiveness, phishing concerns have eased dramatically. "We rolled it out with virtually no trouble, and it's now stable and effective, requiring little to no attention," Donovan notes.

ABOUT AREA 1

The industry's most comprehensive anti-phishing solution, Area 1 Horizon identifies threat campaigns, attacker infrastructure, and delivery mechanisms to give an advance warning to stop targeted phishing attacks during the earliest stages of an attack cycle.

Backed by top tier investors, Area 1 Security is led by security and data analytics experts coming from NSA, USCYBERCOM, Cisco/IronPort, and FireEye who realized a pressing need for a proactive solution to targeted phishing attacks. Area 1 Security works with some of the most sophisticated organizations in the world, including F500 banks, insurance companies, and health care providers, to preempt and stop targeted phishing attacks at the outset, improve their cybersecurity posture, and change outcomes.

▸ Learn more and get in touch with us for a free preview:
INFO@AREA1SECURITY.COM