AGARI

Neustar UltraGeoPoint Decisioning Data for Agari Boosts Confidence in Pinpointing Security Threats

The Challenge

Agari is the Trusted Email Identity Company™, protecting brands and people from devastating phishing and socially-engineered attacks. Chief among its products is Agari Phishing Defense™, tailored for enterprise users seeking to stop inbound spearphishing, business email compromise (BEC), vendor email compromise (VEC) and email account takeover-based attacks from ever reaching their employees.

As a leading security company with a steady growth trajectory, Agari is continuously innovating and adopting the latest best-in-class resources to maintain its reputation and ensure its phishing defense solutions offer full protection to enterprises and their employees. Its product suite is built on predictive Artificial Intelligence (AI) that continuously detects, defends against and responds to advanced email attacks by leveraging massive data sets, data science and cloud computing.

Central to Agari's technical architecture for Agari Phishing Defense is a machine learning approach that focuses on sender-receiver identity behavior — determining what constitutes good behavior so it can effectively identify and alert enterprises to bad actors. As cybercriminals adjust their behaviors to bypass protection systems, Agari must continuously update its algorithms with the most relevant data available to stay one step ahead of the bad actors.

> "The Neustar team was extremely knowledgeable and hands on. They were able to demonstrate the geolocation process with us on a technical level, which made us feel confident in the data. In our search for the right solution, the other companies we spoke with were not able to provide this level of insight."
>
> **– Abhijit Dey**
> Sr. Vice President,
> Product Development,
> Agari

The Neustar Solution

To ensure a robust modeling system that aggregates and incorporates as much applicable data as possible, Agari turned to Neustar for its UltraGeoPoint IP decisioning data. Neustar's services had been integrated with another Agari product with great success. Now, with Agari Phishing Defense, engineers saw the potential to introduce greater accuracy in identifying the geographic origin of emails and better spot suspicious patterns of behavior that trigger an alert to clients to take action.

A market-leading IP address geolocation service, UltraGeoPoint delivers enhanced insight to where an IP address is located (both IPv4 and IPv6), how it is connected to the Internet and its associated metadata. The level of detail available helps Agari to create more complete profiles of anonymized users and entities, enhancing the overall effectiveness of Agari Phishing Defense.

UltraGeoPoint integrated seamlessly with Agari's systems. Neustar's technical support also provided highly responsive service, including demonstrations detailing the IP identification process to underscore the level of data quality involved and insights to optimizing the product.

The Outcome

By incorporating Neustar UltraGeoPoint data, Agari has enhanced the performance of Agari Phishing Defense and expanded its capabilities, improving the product's ability to identify email attacks before they reach the enterprise and its employees.

Agari depends on UltraGeoPoint lookups during its review of millions of email messages every day. Even though most messages wind up being legitimate, these lookups help the company determine legitimate behavior in order to identify malicious attempts. Additionally, unlike competitive offers, UltraGeoPoint offers compelling potential for Agari's engineers, such as anonymous proxy information that is expected to prove valuable in future development.

From isolating social engineering attacks to detecting impersonations of brands and entities, Agari's integration of Neustar UltraGeoPoint decisioning data has increased its level of accuracy and helped return confidence to the electronic communications channel.