GRAPHUS
A Kaseya COMPANY

TrustGraph

Graphus provides an automated, AI-based email security solution for Microsoft 365 and Google Workspace that combines ironclad anti-phishing defense with personalized anti-spam protection – with no manual IT admin intervention necessary. Using a powerful AI algorithm and machine learning, Graphus stops both known and zero-day email-borne threats, including phishing, business email compromise (BEC), account takeover (ATO) and ransomware attacks. Graphus takes just minutes to deploy via an API – with no MX record changes, email rerouting or agent installation needed.

What is TrustGraph?

Graphus' email security prowess is rooted in a patented AI and machine learning technology that uses graph theory to build trust profiles for each organization, scrutinizing the relationship between the sender and recipient of a message. This technology allows Graphus to perform deep learning analysis of historical and real-time communication patterns between senders and recipients to determine the credibility of communication and to define trustworthy interactions. We call this the TRUSTGRAPH – our rating for trustworthiness. It is the core for identifying and blocking social engineering attacks and protecting users from zero-day threats.

What is Graph Theory?

Graph theory is a fundamental concept in the field of mathematics and computer science that also finds an application in email security. At its core, graph theory involves the study of graphs, which are mathematical structures used to model pairwise relations between objects. In the context of email security, these objects can represent various entities such as email accounts, servers or even specific messages.

How is Graph Theory Used in Email Security?

Graph theory plays a crucial role in enhancing email security by providing the tools to analyze complex relationships and patterns within email data. Its applications in phishing detection, social network analysis and reputation systems demonstrate its value in defending against a wide range of email-based threats. Through continuous analysis of the evolving patterns and relationships within email networks, graph theory helps maintain a robust defense mechanism against the ever-changing landscape of cyberthreats.

1. Phishing Detection

The primary application of graph theory in email security is the detection and prevention of phishing attacks. Phishing, a prevalent method used by cybercriminals, involves sending fraudulent emails that appear to be from trusted sources to steal sensitive information or trick unsuspecting victims into performing an action that benefits the bad actor. By utilizing graph theory, an email security solution analyzes the relationships and patterns between different email senders and recipients. This analysis helps in identifying anomalous behaviors that deviate from the normal communication patterns within the network, which are indicative of impersonation and phishing attempts.

For example, a sudden increase in emails sent from a particular account to multiple recipients within a short timeframe, especially if these emails contain links or attachments, could be flagged as a potential phishing campaign. Graph theory enables the mapping of these relationships in a visual and analytical way, allowing the email security tool to spot and isolate these threats more effectively.

2. Social Network Analysis

Another application is in the analysis of social networks within email data. By constructing graphs that represent the social interactions between email users, an email security solution can identify influential nodes (i.e., key individuals within an organization) and monitor for targeted attacks against these users, known as spear-phishing.

3. Reputation Systems

Graph theory is utilized in developing reputation systems for email senders. By analyzing the sender-recipient interactions over time, an email security solution assigns reputation scores to senders based on the quality and safety of their emails. Senders consistently involved in sending safe and legitimate emails are deemed trustworthy, while those frequently linked to suspicious activities can be flagged or blocked.

What Makes Graphus so Effective?

Graphus AI analyzes 50+ different message attributes to define trusted interactions. It instantly assesses incoming emails and detects even the most subtle anomalies and red flags. AI continues learning from every user interaction, allowing Graphus to become highly precise and effective in detecting and removing threats.

When Graphus detects any malicious characteristics, it immediately quarantines these emails – even zero-day attacks it has never seen before. For instance, if a compromised payload or URL is detected, the message is auto-quarantined, an alert is generated and the Graphus admin is notified. To ensure no user interaction with malicious messages, Graphus automatically and instantly removes them from all recipient inboxes.

It also notifies the IT team about the attack and helps them analyze quarantined emails with our investigation wizard.If the investigation finds a message to be benign, Graphus automatically returns it to users' inboxes.