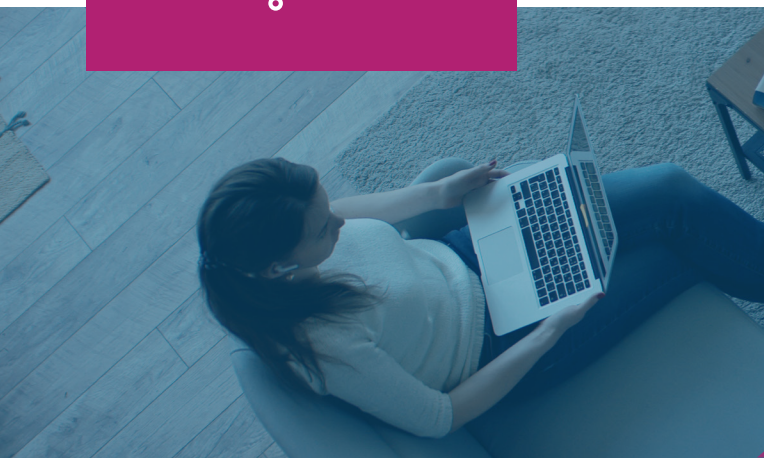
GRAPHUS
A Kaseya COMPANY

Simple, Powerful, Automated!



# Phishing and Spam Defense for Microsoft 365 and Google Workspace

Graphus is a simple, powerful and cost-effective automated phishing defense solution that helps managed service providers (MSPs) quickly protect every inbox in a customer's organization from email-borne threats — whether they originate outside or inside a client's email platform.

Adding Graphus to your security stack enables you to improve clients' security posture by defending them from email-based cyberattacks, including phishing, spear phishing, business email compromise (BEC), account takeover (ATO), identity spoofing, malware and ransomware.

## How is Graphus unique?

To uncover these attacks, Graphus employs patented AI technology that monitors communication patterns between people, devices and networks to reveal untrustworthy emails. By focusing on the credibility of each interaction, Graphus identifies and blocks social engineering attacks targeting businesses and employees to keep your customers safe from today's biggest threats.

## Why add Graphus to your MSP security stack?

**Protect clients from costly security incidents and meet their security needs:**

- Help customers comply with industry regulations that require email security
- Help clients obtain or renew cyber insurance policies
- Keep customers informed with detailed email threat reports


**Increase revenue and become more profitable with:**

- Per-user pricing with aggressive margins
- Ability to target both Microsoft 365 and Google Workspace customers
- Powered Services, our partner portal that helps you market your services to drive new customer acquisition

**Enhance your productivity:**

- Deploy across customers' cloud email in minutes, with no email rerouting or agents to install
- Effortlessly manage multiple clients with our MSP-centric multi-tenant platform
- Seamless alerting and mitigation via integrations with other security tools and IT ticketing systems commonly used by MSPs

# 3 Layers of Defense for Microsoft 365 and Google Workspace Inboxes

1. **TrustGraph** automatically detects and quarantines suspected malicious emails that slip through clients' cloud email security or existing secure email gateway (SEG), preventing the end user from interacting with harmful messages.

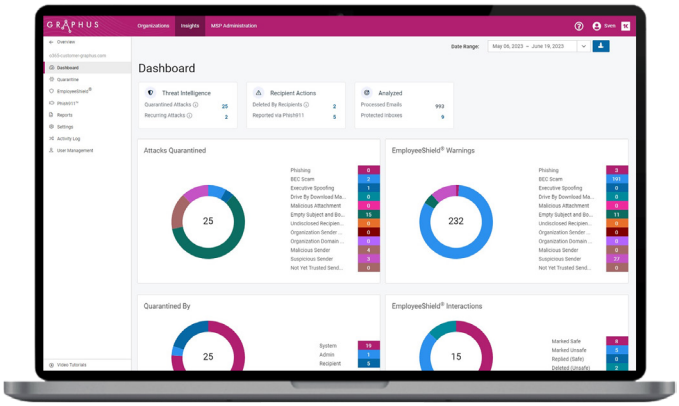
2. **EmployeeShield** places an interactive warning banner at the top of suspicious messages to alert the end users and allow them to report an email as phishing, block it as junk or mark it as safe with one click.

3. **Phish911** empowers end users to bolster email security by proactively quarantining messages they deem suspicious for IT to investigate.

**Personal Spam Filter** gives end users the ability to mark a message as spam with one click to stop receiving email from that sender – building a personal spam profile for each individual email recipient. The filter blocks the sender for that individual user only, so other end users within the organization who may want to continue receiving communications from that sender won't be affected.

The intuitive and robust **Graphus Insights Dashboard** allows MSPs to monitor their customers' real-time security posture, enabling them to quickly investigate and take action on detected threats.

The reporting feature of the dashboard generates informative security metrics reports that MSPs can share with customers, demonstrating the value of their security services.




| GRAPHUS | vs | Secure Email Gateways |
|---|---|---|
| **ACTIVATION TAKES MINUTES**<br>3-click activation in Microsoft 365. Start protecting your clients' email instantly. No email configuration required. | | **ACTIVATION TAKES WEEKS**<br>Clients are left unprotected during the weeks or even months it takes to deploy an SEG. |
| **NO DELAY IN RECEIVING EMAILS**<br>Analyzes messages in real-time with no delay in email delivery. Safe messages are never quarantined. | | **DELAYS EMAILS**<br>SEG filtering can cause delays in receiving messages or improper quarantine of safe emails. |
| **DETECTS ZERO-DAY ATTACKS**<br>Powered by patented AI technology, the TrustGraph feature detects zero-day attacks in real-time. | | **ZERO-DAY ATTACKS SLIP BY**<br>SEGs use traditional threat intelligence to detect attacks, allowing zero-day attacks to slip into inboxes. |
| **POWERFUL PHISHING DEFENSE**<br>Integrates at the API level to detect and stop sophisticated social engineering attacks. | | **LIMITED PHISHING DETECTION**<br>Built to stop spam and overtly malicious emails, not sophisticated social engineering attacks. |
| **EMPLOYEESHIELD VISUAL NOTIFICATION**<br>Provides an interactive warning banner to alert your customers' employees to suspicious emails and give them a simple way to report threats. | | **EMPLOYEES AREN'T NOTIFIED**<br>Customers' employees are not warned of suspicious messages, leaving clients extremely vulnerable to an attack. |

## Questions? Want to see a demo?

Contact us at (786) 530-5002
or visit www.graphus.ai/start-the-conversation