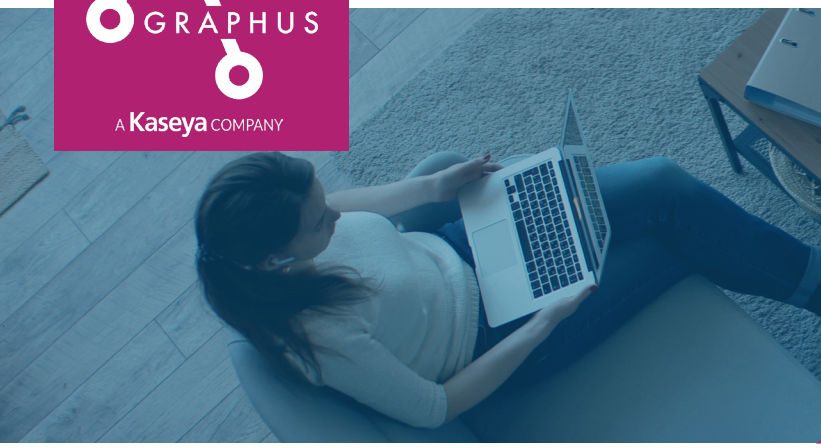
GRAPHUS

A Kaseya COMPANY

Simple, Powerful, Automated



Phishing 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 customers' organization from outside threats.

Adding Graphus to your security stack enables you to immediately defend customers 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?

Increase revenues 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:

- Graphus is entirely cloud-based with no email re-routing or agents to install
- Deploy across a customer's email platform in a matter of minutes
- Seamless alerting and mitigation via integrations with helpdesk ticketing systems commonly used by MSPs

Protect your customers' reputation:

- Reduce costly security incidents and help customers with compliance
- Keep customers informed with security metrics reports
- Enhance customer confidence

3 Layers of Defense for Microsoft 365 and Google Workspace Inboxes

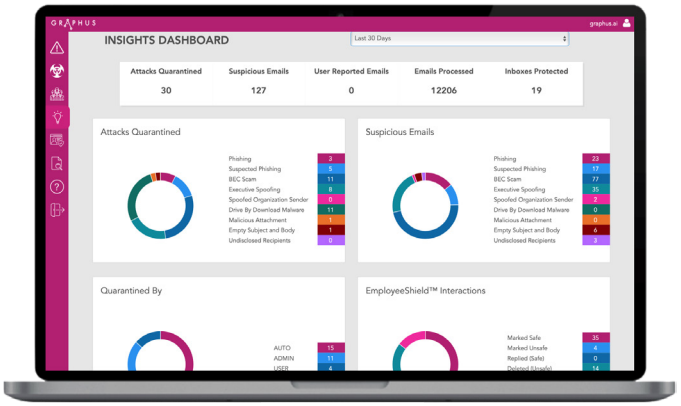
1. **TrustGraph** automatically detects and quarantines suspected malicious emails that make their way through an organization's email platform security or existing Secure Email Gateway (SEG), preventing the end user from interacting with potentially harmful messages.

2. **EmployeeShield** places an interactive warning banner at the top of suspicious messages to alert intended email recipients and allow them to quarantine a message or mark it as safe with one click.

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

Plus, 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 Start protecting your customer's organizations instantly. No email configuration required.		**ACTIVATION TAKES WEEKS** An organization is left unprotected during the weeks or even months it takes to install an SEG.
NO DELAY IN RECEIVING EMAILS Analyzes messages in real time with no delay in email delivery. Safe messages are never quarantined.		**DELAYS EMAILS** SEG filtering can cause delays in receiving messages or improperly quarantining safe messages.
DETECTS ZERO-DAY ATTACKS Powered by patented AI technology, the TrustGraph algorithm detects zero-day attacks in real time.		**ZERO-DAY ATTACKS SLIP BY** SEGs use traditional threat intelligence to detect attacks, allowing zero-day attacks to slip into inboxes.
AUTOMATED PHISHING DEFENSE Integrates at the API level to detect sophisticated social engineering attacks.		**LIMITED PHISHING DETECTION** Built to stop spam and malicious emails, not sophisticated social engineering attacks.
EMPLOYEESHIELD VISUAL NOTIFICATION Provides an interactive warning banner to notify your customers' employees of suspicious attacks and how to remediate threats.		**EMPLOYEES AREN'T NOTIFIED** Customers' employees are not warned of suspicious messages, leaving organizations extremely vulnerable to an attack.

Questions? Want to see a demo?
Contact us at (786) 530-5002
or visit www.graphus.ai/demo-request