



Phishing and Spam Defense for Microsoft 365 and Google Workspace

Graphus is a simple, powerful and cost-effective automated phishing defense solution for companies of all sizes that protects every employee from email-borne threats – whether they originate outside or inside of your organization.

Graphus enhances your security posture by enabling you to defend employees 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 employees to keep your organization safe from today's biggest threats.

Why add Graphus to your organization's security stack?

Make your organization more secure:

- Get comprehensive email security with 3 layers of defense
- Prevent costly security incidents and improve your cyber resilience
- Keep your business compliant with regulatory and cyber insurance requirements

Make your IT team more efficient:

- Graphus is API-based with no email re-routing or agents to install
- Deploy across the enterprise within minutes
- Streamline security operations through workflow automation

Make your IT operations more cost-effective:

- Pay only for what you need (per-inbox pricing)
- Avoid financial and reputation damage from security incidents
- Integrate real-time intel into your existing threat intelligence programs



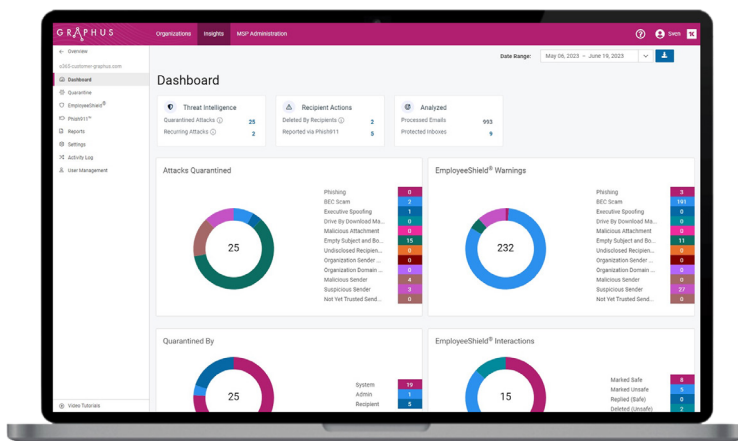
3 Layers of Defense for Microsoft 365 and Google Workspace Inboxes

- TrustGraph** automatically detects and quarantines malicious emails that slip through your organization's cloud email security or existing secure email gateway (SEG), preventing employees from interacting with harmful messages.
- EmployeeShield** places an interactive warning banner at the top of suspicious messages to alert the email recipients and allow them to report a message as phishing, block it as junk or mark it as safe with one click.
- Phish911** empowers employees to bolster email security by proactively quarantining messages they deem suspicious for IT to investigate.

Personal Spam Filter gives employees 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 employees who may want to continue receiving email from that sender won't be affected.

The intuitive and robust **Graphus Insights Dashboard** allows your IT team to monitor your real-time security posture, enabling you to quickly investigate and take action on detected threats.

The reporting feature of the dashboard generates informative **security metrics reports** you can use in security briefings with the leadership.



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

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