

Secure Email Gateways

AUTOMATED PHISHING DEFENSE

GRAPHUS



ACTIVATION IN MINUTES

Graphus® can be activated in minutes and start protecting your organization, instantly. No email configuration required.



NO DELAY IN RECEIVING EMAILS

Graphus® analyzes messages in real time. There is no delay on emails and safe messages are never quarantined.



DETECTS ZERO-DAY ATTACKS

Graphus®, powered by our patented AI technology, the TrustGraph®, detects zero-day attacks in real time.



AUTOMATED PHISHING DEFENSE

Graphus® integrates at the API level to detect sophisticated social engineering (i.e. phishing, BEC, spoofing) attacks.



EMPLOYEE SHIELD™

Graphus® provides an interactive warning banner to notify employees of suspicious attacks and to remediate threats.

Secure Email Gateways



ACTIVATION IN WEEKS

It can take weeks or even months to get a SEG installed. This is time your organization is left unprotected.



DELAYS YOUR EMAILS

All messages are filtered through a SEG which can cause delays in receiving the message or even safe messages being quarantined.



ZERO-DAY ATTACKS SLIP BY

SEGs require traditional threat intelligence to detect attacks. This allows zero-day attacks to slip by and into the inbox of your employees.



LIMITED PHISHING DETECTION

SEGs were built to stop spam and malicious emails, not sophisticated social engineering attacks. They are now trying to playing catch-up.



EMPLOYEES AREN'T NOTIFIED

Employees are not warned of any suspicious messages leaving the organization extremely vulnerable to an attack.