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

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

DETECTS ZERO-DAY ATTACKS
Graphus® analyzes messages in real time. There is no delay on emails and safe messages are never quarantined.

NO DELAY IN RECEIVING EMAILS
Graphus® integrates at the API level to detect sophisticated social engineering (i.e. phishing, BEC, spoofing) attacks.

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

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

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

ZERO-DAY ATTACKS SLIP BY
All messages are filtered through a SEG which can cause delays in receiving the message or even safe messages being quarantined.

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

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

EMPLOYEES AREN’T NOTIFIED
BLOG POST
www.graphus.ai/where-secure-email-gateways-fail-graphus-excels