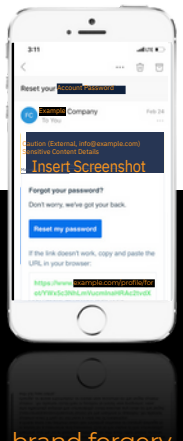
Email Protection

Supports Microsoft 365

Forum Info-Tech Managed Managed Email Protection is a cloud-based email security product that detects business email compromise, spam, and phishing-type emails and attacks. The product catches malicious emails by utilizing computer vision, AI, and machine learning. Forum's Managed Email Protection is fully managed and provides you with the option to either inform your users of suspicious or malicious emails through an HTML banner or block them with quarantine features. Driven, curious, mobile, and growing smarter by the subject line, Forum's Managed Email Protection adds an important layer of protection to your inbox.



Key Features

Detects VIP spoofing, brand forgery, and other attacks used in business email compromise and phishing

Provides user-friendly warnings in way of banners on malicious and suspicious email

Sanitizes embedded links to help protect users from potentially malicious websites

AI and Computer Vision models to catch evasion techniques

Easy “Report to SOC Button” for human analysis

Fast Deployment built into Forum Managed dashboard

Phishing, Zero-Day Phishing, 3rd Party Brand Impersonation

AI, machine learning, and computer vision identify patterns in text, image, and html to identify potential threats. The unique banner system allows for borderline threats to be flagged without compromising business functionality

VIP Impersonations

Identifies attempts to impersonate VIPs via email spoofing, typo squatting, or other malicious tactics

Malicious Files

Scans for malicious links, infected PDFs, and embedded code including scripts. Analyzes text within each email and attachment(s) to determine if sensitive words or phrases are used such as: password, invoice, payment, etc.

Malicious Links

All links in emails are sanitized using a sandboxed server. The user cannot access the link directly. They are brought to a landing page showing a screenshot

Personal Device & Home Attacks

Attacks on personal devices are mitigated by conducting analysis on the server side and injecting the results into the email, completely removing the need for remote software such as dedicated email clients

Malicious Insider

Machine learning develops behavior profiles and social graphs that identify suspicious emails that don’t match a known profile, triggering an impersonation warning