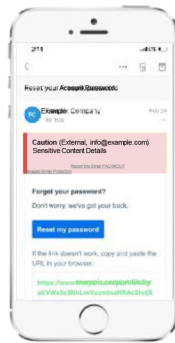


# Email Management & Managed Security

Real Time | Full Time | Security Operations Team  
Supports Microsoft 365



Pocket Protector by TetherView offers Fully Managed Email & Managed Email Protection that detects business email compromise, spam, and phishing-type emails and attacks. The product catches malicious emails by utilizing computer vision, AI, 24 x 7 experts, and machine learning. Pocket Protector 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. Pocket Protector adds an important layer of protection to your inbox. Pocket Protector fully manages your O365 email to adhere with any regulatory requirements.



## Key Features

Fully Managed and Staffed Security.  
User management and administration.

Enable Compliance and Data Loss Controls, aligned with regulatory requirements.

Sanitizes embedded links to help protect users from potentially malicious websites

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

24 x 7 Monitoring with easy "Report to SOC Button" for human analysis

Fast Deployment

### 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

External (sender@example.com)

External (sender@example.com)  
Blacklisted SenderIP Details

External (sender@example.com)  
Brand Impersonation Details