GOSECURE INBOX DETECTION AND RESPONSE

When a successful email attack reaches an employee's inbox, the last thing you want is an employee wondering whether to open it. Or, worse yet, open it and expose your organization to unknown damage. And with internal email submissions averaging over a day to review, end-users have lost patience. Organizations need an employee-driven reporting service that analyzes suspicious emails and delivers rapid incident response.

KEY BENEFITS

- Automated email analysis
- Rapid end-user response
- Immediate email incident response
- Defend against malware and ransomware attacks
- Reduce phishing dwell time

GoSecure Inbox Detection and Response (IDR) automates email threat resolution in the user's inbox. If an attack gets through your current email security gateway, GoSecure IDR lets employees submit suspicious emails and then instantly routes those emails through machine learning filters—as well as expert human analysis—to check the email's true intent. In minutes the email is either verified or vanquished. All without help from IT, or end-user hassle.

Key Features:

Completely Automated

Submission, analysis, classification and response are fully automated – no administrator interaction required. And the time from submission to response averages less than 5 minutes.

1. Employee notices suspicious email in Outlook Inbox and clicks the GoSecure IDR button to launch review
2. Flagged email is automatically quarantined and routed through the GoSecure Active Response Center
3. GoSecure automated machine learning engines investigate suspicious email
4. Live security experts join the investigation of suspicious email with multi-faceted analysis
5. Within minutes the suspicious email is returned, either verified or removed
6. Real-time reporting gives IT clear visibility into every incident and its resolution

Advanced Threat Investigation & Analysis

Automated machine learning and human analysis deliver the highest level of accuracy in threat detection and mitigation.

Dynamic Quarantine

Suspicious emails automatically moved into administrator quarantine once submitted. Messages remain in quarantine, away from curious end-users, until analysis is complete.

Email Incident Response

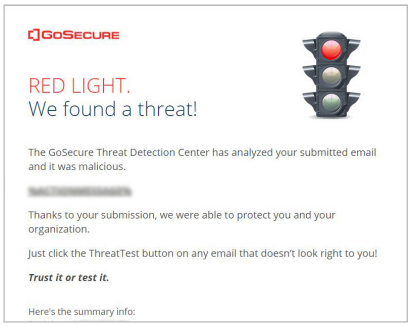
Instant removal of identified malicious message from all user inboxes.

Centralized Management

Ability for the SOC or IT administrators to configure notifications and frequency. View summary charts and set up customized reports for emails processed and categories assigned.

Real-Time Reporting & Response

Real-time, end-user driven reporting of suspicious message to the GoSecure Active Response Center. Users received closed-loop communication with the results of the investigation and automated incident response.


GoSecure

RED LIGHT.
We found a threat!

The GoSecure Threat Detection Center has analyzed your submitted email and it was malicious.

Thanks to your submission, we were able to protect you and your organization.

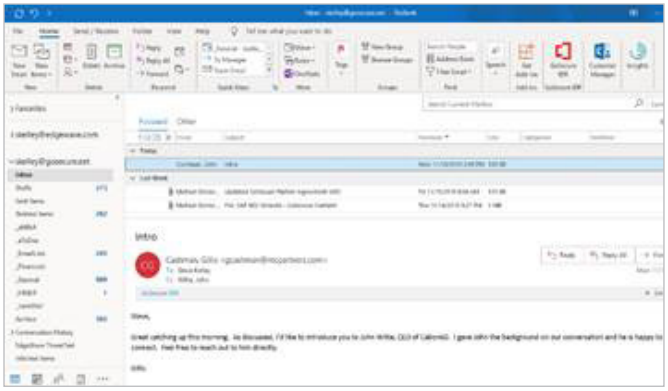
Just click the ThreatTest button on any email that doesn't look right to you!

Trust it or test it.

Here's the summary info:

Mobile Support

End-user submissions can be done from any device. Both desktop and mobile apps are supported.



GoSecure

GoSecure is recognized as a leader and innovator in cybersecurity solutions. The company is the first and only to integrate an Endpoint and Network threat detection platform, Managed Detection and Response services, and Cloud/SaaS delivery. Together, these capabilities provide the most effective response to the increased sophistication of continuously evolving malware and malicious insiders that target people, processes and systems. With focus on innovation quality, integrity and respect, GoSecure has become the trusted provider of cybersecurity products and services to organizations of all sizes, across all industries globally. To learn more, please visit: https://www.gosecure.net.