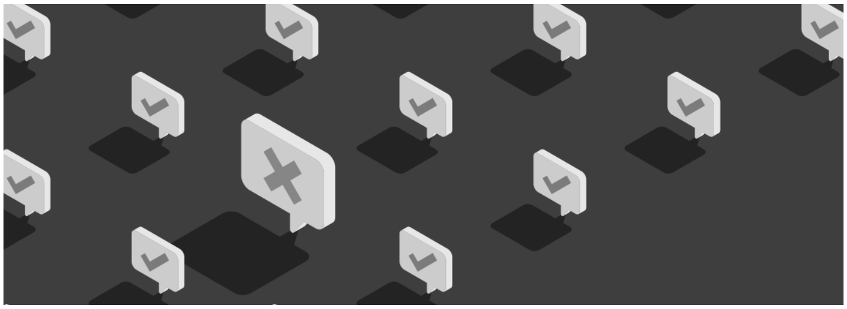
FORTRA®

DATASHEET

# Suspicious Email Analysis



## Detect, Analyze, and Mitigate Advanced Email Threats

Enterprises struggle to stop email threats from routinely reaching user inboxes, leading to Business Email Compromise (BEC) and ransomware attacks. While users become more adept at identifying suspicious emails and enterprises invest in increasingly sophisticated email security stacks, threat actors continue to deploy emails designed to trick employees. Security teams with limited expertise, time, and budget have difficulty stopping every threat and lack the time to properly close the feedback loop with reporters, placing enterprises at risk.

Suspicious Email Analysis helps enterprises by providing expert triage and automated responses to user-reported emails, ensuring real threats are quickly identified while users receive timely feedback to reinforce security awareness training programs.

## Expert-Verified Threat Intel from Millions of Users

Advanced email threats use social engineering techniques that supplemental frontline security stacks fail to detect. To complicate matters, security analysts struggle to manage the high volume of suspicious emails reported, which leads to malicious emails landing in employee inboxes.

Fortra helps enterprises efficiently source and analyze intelligence from suspicious emails reported by users. We gather threat intelligence from users across a wide variety of enterprises and promptly follow up with each reporter and the SOC team to close the communication gap, while proactively monitoring for look-alike domains and socially engineered emails designed to slip past email security stacks and prey on users.

## SERVICE SUMMARY

### COMMON THREATS

- Business Email Compromise (BEC)
- Ransomware
- Credential theft
- Office 365 lures
- Malicious attachments

### COLLECTION METHODS

Gathers threat indicators from multiple sources, including:

- Reported emails from staff
- Threat Indicators globally sourced from other Fortra customers
- Other Fortra intelligence sources

### ANALYSIS AND INTELLIGENCE

Gathers threat indicators from multiple sources, including:

- Expert-vetted human analysis
- Automated analysis and feeds

### THREAT MITIGATION

- Mitigates advanced threats that get past frontline security defenses
- Works with Fortra CDR to quarantine threats from multiple inboxes
- Provides timely status feedback to reporters and SOC team

> *"Good quality in the instant email analysis. Quick responses and good support on questions!"*
>
> ***-Global Auto Manufacturer***

## Separate Real Threats from the Noise

A vast majority of suspicious emails reported by users are either non-malicious spam or related to other non-issues, hindering the separation of real threats from noise. Because of this, many potential email threats need expert analysis to be accurately dispositioned, resulting in significant alert fatigue for busy security teams.

Through a combination of automation and expert analysis, Fortra efficiently processes user-reported emails without burdening security teams. Automation expedites the review of massive quantities of reported emails, and human analysts provide the valuable context necessary to ensure accurate classification of email threats, while maintaining updated communication with reporters and the SOC team along the way.

## Mitigate Threats Across the Entire Organization

Hunting and removing known threats across user inboxes requires multiple, time-consuming steps. Threats, such as BEC and ransomware, require swift action that, without advanced automation tools, require inefficient and unscalable manual intervention.

Fortra mitigates email attacks by identifying and suspending advanced threats, such as look-alike domains designed to target your employees before emails are sent, as well as referencing threat indicators to block emails from registered look-alike domains. To stop multi-pronged attacks, Suspicious Email Analysis works with Continuous Detection and Response to automatically find and remove threats attacking multiple inboxes.

## Protect Against Costly Inbox Attacks

Cybercriminals threaten enterprise security by using advanced social engineering techniques to target user inboxes. Security teams must be able to quickly distinguish real threats from a large volume of suspicious activity, yet are often ill-equipped to effectively identify and mitigate attacks due to time-consuming and inefficient manual processes.

Suspicious Email Analysis provides expert triage and automated response to user-reported emails, ensuring real threats are quickly identified while users receive timely feedback that reinforces security awareness programs. This proactively disrupts costly attacks while strengthening your security architecture to defend against future threats.

*Suspicious Email Analysis includes:*

**Suspicious Email Analysis** provides users the ability to report suspicious emails that make it past security and into corporate inboxes. Users report emails through a “Report Phish” button, a third-party plugin, or an internal abuse box monitored by Fortra experts. Experts examine reported emails through system automation and human analysis and then respond to the individual reporter to close the feedback loop and encourage future reporting. When a malicious email is confirmed, an alert is sent to the Incident Response Group. Extracted threat indicators are then made available via API to be added to internal tools to strengthen security and remove similar threats from other inboxes.

**Email Threat Indicators** include suspicious URLs, file hashes, IP Addresses, and malicious email addresses from threat activity reported by your users, other Fortra customers, and malicious indicators encountered other Fortra services, including our Credential Threat and Domain Monitoring services. This dataset can be fed into existing security architectures, such as firewalls, IPS, proxies, mail gateways and endpoint agents via API, to extend and strengthen security postures and identify other threats that may exist in your system.

To eliminate threats that have evaded initial detection and were previously delivered to inboxes, Suspicious Email Analysis can work with Cloud Email Protection's Continuous Detection and Response, or your SOAR, to continuously scan employee inboxes for the latest threat indicators and eradicate multi-pronged attacks. These indicators are identified by multiple Fortra intelligence sources to neutralize attacks in multiple inboxes.

FORTRA®

Fortra.com

**About Fortra**

Fortra provides advanced offensive and defensive security solutions that deliver comprehensive protection across the cyber kill chain. With complete visibility across the attack chain, access to threat intelligence spanning the globe, and flexible solution delivery, Fortra customers can anticipate criminal behavior and strengthen their defenses in real time. Break the chain at fortra.com.