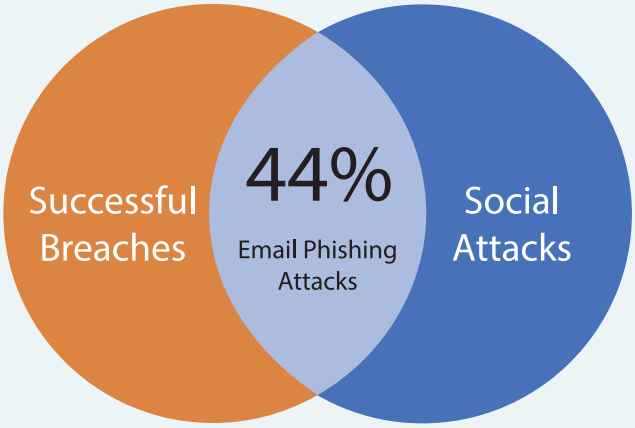
ThreatTest

Automated Phishing Email Incident Response Service

Email phishing attacks are the most prevalent variety of social attacks, which comprise nearly 44% of successful breaches.[1] When a successful email attack reaches an employee's inbox, the last thing you want is an employee wondering whether to open it—or ignoring it while the attacker moves on to the next employee target.

And if your helpdesk receives an end user request to research a suspicious email, it's difficult to find the time or threat intelligence to quickly and accurately analyze the message. In fact, 46% of surveyed IT pros say it takes a day or longer to remove a phishing email.[2]

Organizations need an employee-driven reporting service that analyzes suspicious emails and delivers rapid incident response.



Key Benefits

- Delivers automated, accurate phishing investigation and remediation
- Eliminates employee uncertainty and phishing dwell time
- Relieves resource burden and complexity of managing incident response
- Defends a company's network against malware attacks
- Increases employees' security awareness

EdgeWave ThreatTest removes the guesswork and provides an automated process for employees to report suspicious emails and receive research support—alleviating helpdesk resource constraints. When an employee receives an email impersonation or other suspicious email, with a click of a button, ThreatTest provides rapid and accurate investigation and incident response.

Key Features

Real-Time Reporting & Response

Real-time, end-user driven reporting of suspicious message to the EdgeWave Hybrid Threat Detection Center. Users received closed-loop communication with the results of the investigation and automated incident response. (*Figures 1 & 2*)

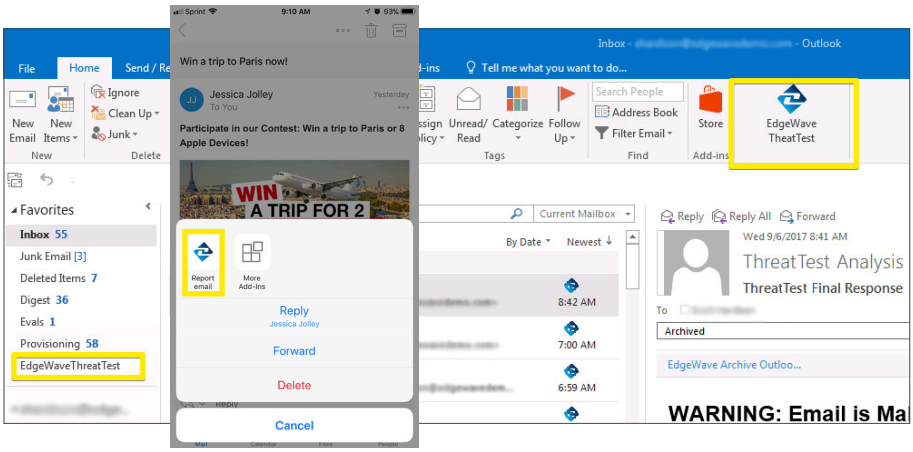


Figure 1 - From desktop to mobile, EdgeWave ThreatTest provides easy reporting for your end users and instant email quarantine.

ThreatTest

Automated Phishing Email Incident Response Service

Key Features

Advanced Threat Investigation & Analysis

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

Dynamic Quarantine

Quarantine mechanism to evaluate untrusted content within the submitted messages, such as URLs. Suspicious emails automatically moved into a custom folder once submitted.

Global Policy & Content Removal

Instant removal of a malicious message from the inbox; rules automatically applied to the global policy for all users.

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. (*Figure 3*)

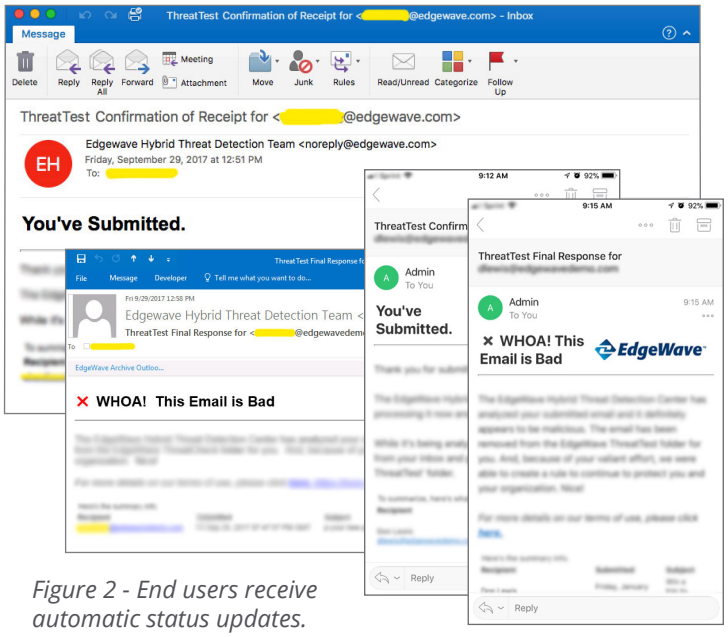


Figure 2 - End users receive automatic status updates.

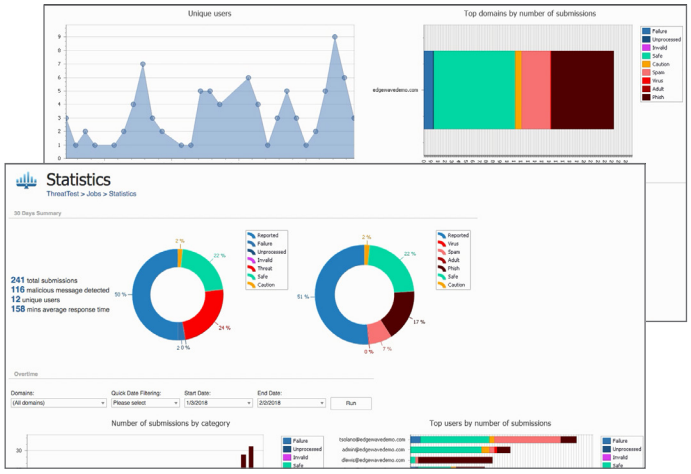


Figure 3 - Centralized reporting provides IT administrators a global status view.

System Requirements

Email Platforms Supported

Microsoft Exchange 2013 and newer; Microsoft Office 365; Outlook Web Access (OWA)

Email Clients Supported

Microsoft Outlook and Microsoft Outlook App (for Android and iOS)

With more than 20 years of security experience, EdgeWave delivers the most accurate threat intelligence with our unique hybrid approach that combines automated machine learning and human analysis to investigate and respond to phishing attacks in real-time. ThreatTest provides powerful detection and prevention of phishing, ransomware and other malicious email-borne and blended threats—closing the inbox security gap to improve end user and enterprise security effectiveness.

1 - Verizon. "2017 Data Breach Investigation Report." *2 - 2017 Ransomware Report, Cybersecurity Insiders*

4225 Executive Sq., Ste. 1600
La Jolla, CA 92037-1487

Give us a call:
1-800-782-3762

Send us an email:
info@edgewave.com

For more info, visit us at:
www.edgewave.com