BRIEF

/ MailMarshal Blended Threat Module

LevelBlue

Maximum security against phishing, powered by machine-learning

LevelBlue MailMarshal is the industry's most reliable and flexible email security solution. LevelBlue MailMarshal's Blended Threat Module (BTM) protects against phishing with security powered by machine-learning.

What is a Blended Threat?

A Blended Threat is an attempt to compromise information security that uses multiple vectors. Blended Threat email messages are typically crafted so that they appear to be from a trusted sender. They contain links to a website hosting malicious code or attempts to entice the user into providing personal information. Blended Threat emails are sometimes targeted to a specific individual or individuals.

What is the Blended Threat Module?

The LevelBlue MailMarshal Blended Threat Module (BTM) uses several validation methods, including real-time behavioral analysis and content inspection as well as information from several industry standard sources, to identify and block sites that serve suspicious or malicious code. Because validation is performed in real-time by a cloud service when a link is clicked, it provides superior effectiveness in catching and neutralizing new exploits for all users on any device from any location.

How does the BTM work?

The BTM functions as follows:

1. MailMarshal scans emails and rewrites links before delivering the email.
2. Clicking a link invokes the LevelBlue Link Validator cloud service.
3. The Link Validator passes the link to one or more validation services. These include various link reputation services that check whether the link has been associated with phishing or other malicious activity. Links are also subject to real-time checking of page content using LevelBlue's smart link classifier, based on machine learning technology, which is continuously trained on real-world data to recognize phishing and other threats. Real-time scanning helps detection of new threats in the window of time before links become listed in reputation lists.
4. Depending on the results of validation, the Link Validator redirects the request to the original site or blocks the requests.

Benefits

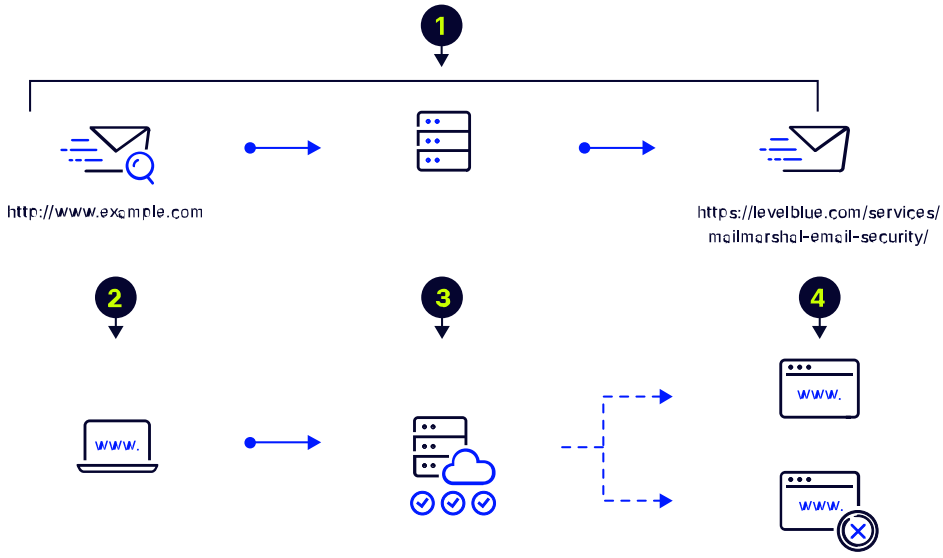
- Protects against Ransomware, Business Email Compromise (BEC), Phishing, Malware, and Zero-Day
- 0 Clients reported ransomware infection in 20+ years
- 99.99% Malware and exploit capture rate < 0.001% spam false positives
- Layered threat intelligence, powered by telemetry from 5,000+ global MSS/MDR clients and ML-powered algorithms
- Granular control of internal SMTP traffic
- Decades of leadership in email security supported by LevelBlue SpiderLabs elite threat detection security team

Ease of implementation

- Deploy on prem or hybrid cloud
- Complements Microsoft 365 and other cloud email
- Cost-effective

How it works

1. Scan emails and rewrite links before delivering email,
2. Clicking a link invokes LevelBlue Link Validator cloud service,
3. The Link Validator passes the link to one or more validation services,
4. Depending on the results of the validation service, the request is redirected or blocked



LevelBlue

Contact us www.levelblue.com