BLUE COAT®

Network
+ Security
+ Cloud

Blue Coat Mail Threat Defense

Secures Email Against Targeted Phishing Attacks

SOLUTION BRIEF

Email is an extremely effective attack vector; according to Verizon[1], general and targeted spear phishing attacks account for nearly 80% of cyber espionage attacks. These attacks hide their intent in an email that appears to come from a legitimate source, tricking the recipient into clicking on a malicious link or opening an attachment infected with malware; once infected, the attacker can go on to do almost anything. 23% of recipients open phishing messages and 11% click on attachments – nearly half open emails and click within the first hour. Even senior executives and technically savvy users are not immune. It only takes one wrong click and your organization is breached!

Blue Coat Mail Threat Defense protects against email-borne malware in links and attachments that are activated by unsuspecting end users. The solution extracts malicious content prior to delivery, without disrupting the existing message flow, to enforce an enterprise's security policies.

Strengthens Defenses Against Email Attacks

Mail Threat Defense detects and blocks advanced email-based threats, delivering only sanitized messages to end users. It looks at each attached file and embedded URL and makes a determination, based on security policy risk ratings. It sits in the network, behind the Secure Email Gateway (SEG) and the SPAM filter, but before the email server, this ensures messages identified as spam will not be subjected to unnecessary analysis.

Mail Threat Defense is designed to augment and enhance existing emails security solutions, while preserving current message delivery workflows. It integrates seamlessly with the Blue Coat Advanced Threat Protection ecosystem, combining comprehensive pre-delivery detection and filtering capabilities into a single solution for:

- File Reputation (including whitelists and blacklists)
- Anti-Virus Detection
- Web Reputation with URL Filtering and Categorization
- Advanced Multi-Analysis Sandboxing

The diagram below illustrates the Mail Threat Defense workflow and how its various functions work together to scan email for malicious content prior to delivery to the mail server.

[1] Source: Verizon Data Breach Investigations Report

AT-A-GLANCE

BLUE COAT MAIL THREAT DEFENSE

- Pre-delivery analysis of email messages for malicious content in embedded URL links and file attachments
- Policy-based active message blocking, alteration, and quarantines, or passive malware detection and alerting
- Supports on-site mail servers and cloud email services
- Supplements and enhances existing email security solutions, without altering existing message workflows

CORE CAPABILITIES

- Pre-delivery inspection of URLs and file attachments
- Precise gold image malware detonation chambers
- Multi-stage recursive analysis of all attack vehicles
- Customized detection criteria and targeted risk scoring
- Configurable security policies based on risk scores
- Leverages Blue Coat's vast Global Intelligence Network

KEY BENEFITS

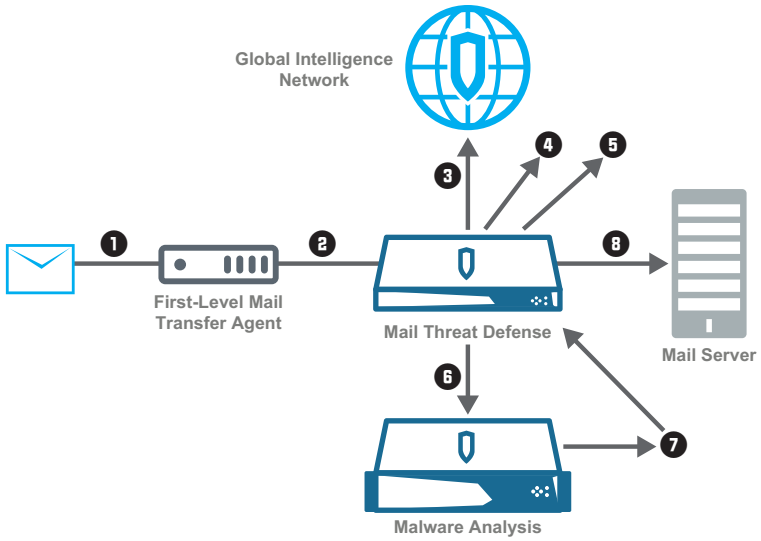
- Provides universal mail protection, regardless of mail client, device, or access method (including the cloud)
- Detects targeted malware and zero-day threats
- Eliminates threats before they can ever reach the user's inbox

BLUE COAT

Network
+ Security
+ Cloud

SOLUTION BRIEF

1. Email goes through Mail Transfer Agent for spam filtering.
2. Mail Transfer Agent sends emails that pass policy to Mail Threat Defense for further analysis.
3. Mail Threat Defense communicates with Global Intelligence Network to check the reputation of email senders and file attachments. The results determine if email should be blocked or sanitized prior to delivery.
4. **URL Category Filters** – Mail Threat Defense checks URLs within email body to assess threat level and Acceptable Use Policy; if violations occur, Mail Threat Defense enacts policy.
5. **Anti-Virus** – Mail Threat Defense looks at anti-virus pattern signatures to see if attachments contain known viruses. If viruses are found, Mail Threat Defense enacts policy.
6. **Sandboxing** – Mail Threat Defense sends unknown, suspicious attachments and URLs to sandbox for behavioral analysis.
7. If the file or URL is malicious, Mail Threat Defense enacts policy. Malware Analysis returns a risk score, categorization information, and additional threat intelligence to Mail Threat Defense, which then updates Global Intelligence Network.
8. Mail Threat Defense delivers safe emails to mail server.



Offers Flexible Deployment Options

Mail Threat Defense is designed with the scalability to meet today's high-volume enterprise email requirements and tomorrow's future growth needs. It can be deployed inline, as a cloud-based service or an on-premises appliance, to protect against advanced malware and targeted phishing attacks in emails, without blocking or delaying legitimate emails.

Delivers Universal Mail Protection – Regardless of Email Clients or Access Methods

Mail Threat Defense provides superior email threat detection combined with highly relevant alerting to defeat targeted phishing attacks. Because incoming messages are thoroughly sanitized before they ever reach the email server, Mail Threat Defense protects end users, regardless of their choice of email clients, mobile devices, or network access methods.

Secures Office 365 and Enterprise Cloud-based Email

Mail Threat Defense protects against targeted attacks and phishing for enterprises migrating to Office 365 and other enterprise cloud-based email services. It deeply scans embedded URLs and file attachments in email messages prior to delivery at the cloud mail server, then takes policy-based actions to sanitize the messages based on customized risk scores. Enterprises can confidently move email to the cloud with enhanced security controls and a vastly reduced vulnerability to malware breaches that are introduced inadvertently by errant clicks of an email user.

Removes Threats Sooner

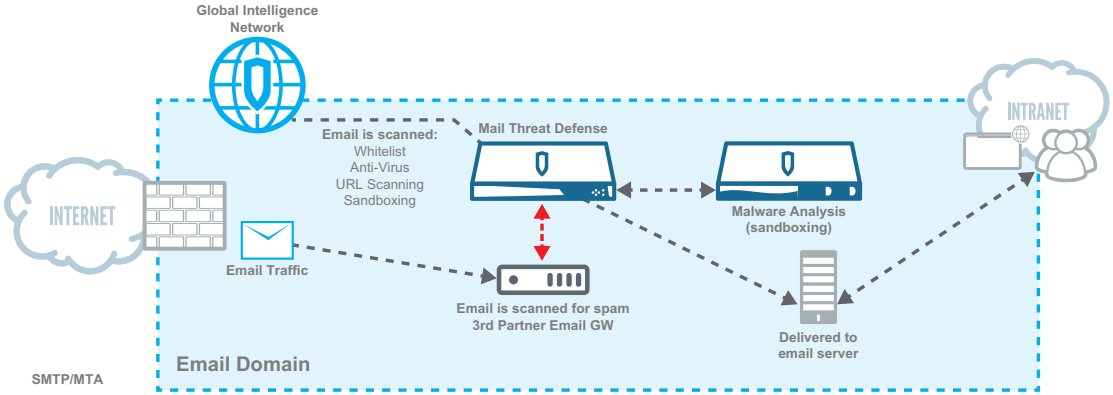
Customers with Blue Coat's industry leading ProxySG secure web gateway are already protected when users click on malicious web links, but Mail Threat Defense removes these threats sooner, before they ever reach the mail server or are delivered to the user's email inbox. It also adds protection against malicious email attachments and shares the global intelligence and malware analysis with Blue Coat's web and network security solutions to improve overall threat detection and prevention capabilities.

BLUE COAT

Network
+ Security
+ Cloud

SOLUTION BRIEF

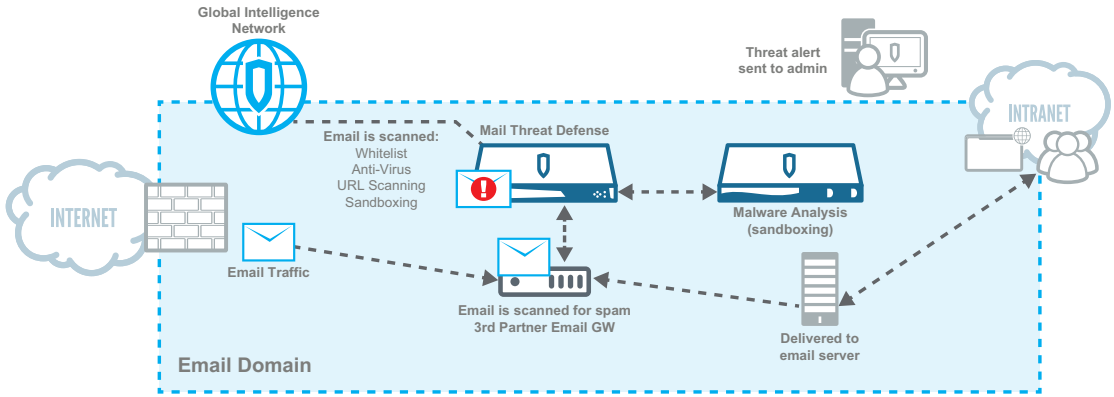
In-Line Mail Transfer Agent Mode (Active Blocking)



Blue Coat Mail Threat Defense Deployment:

- Email is first delivered to 3rd party Secure Email Gateway
- Then Blue Coat Mail Threat Defense is configured as the next Mail Transfer Agent in the chain
- Blue Coat Mail Threat Defense scans the email (Whitelist, URL, Anti-Virus and Sandboxing)
- Blue Coat Mail Threat Defense either blocks & quarantines the email or delivers to the email server

Monitor-Only Span/TAP Mode (Passive Monitoring and Alerting)



Blue Coat Mail Threat Defense Deployment:

- Email is first delivered to 3rd party Secure Email Gateway
- The 3rd party Mail Transfer Agent mirrors a copy of the email traffic to Mail Threat Defense (out-of-band)
- Blue Coat Mail Threat Defense scans the email (Whitelist, URL, Anti-Virus and Sandboxing)
- Blue Coat Mail Threat Defense alerts if malicious traffic is found (no blocking, alert only)
- Great for POC deployments

SOLUTION BRIEF

Identifies Both Known and Unknown Content

Mail Threat Defense achieves unprecedented speed and accuracy by combining advanced URL filtering, file reputation (whitelists and blacklists), and dual antivirus detection to rapidly identify both known and unknown content attached to, and embedded in, email messages. As a result, Mail Threat Defense can neutralize email-borne malware contained within both primary and secondary attack vehicles (files and URLs).

Detects Targeted Malware and Zero-Day Threats

Unknown files and URLs are extracted and sent to the Blue Coat Malware Analysis Appliance, an advanced multi-stage sandbox, for identification and risk scoring in precisely tailored gold-image detonation chambers. It performs recursive analysis on the primary file or URL plus any subsequent "dropped" files and callback URLs using static code analysis, dynamic behavioral analysis, reputational analysis, and YARA rules analysis techniques.

Enforces Configurable Security Policies

Security policies allow enterprises to balance message delivery speed, user autonomy desires, and business security needs. Based on the verdicts and malicious risk scores received, enterprises can set policies to block, alter or quarantine messages prior to delivery, or simply detect and alert.

Advanced Threat Protection: Simplifying Sophisticated Security Challenges

Mail Threat Defense is an integral part of the Blue Coat Security Platform, a comprehensive, multi-vector Advanced Threat Protection environment that empowers your organization to:

- Proactively prevent and detect against sophisticated threats
- Integrate advanced security technologies from across the industry
- Manage a unified security policy across the enterprise as well as the cloud
- Incorporate advanced incident response and forensic intelligence functions

Visit bluecoat.com to learn more.

BLUE COAT®

Network
+ Security
+ Cloud

Blue Coat Systems Inc.
www.bluecoat.com

Corporate Headquarters
Sunnyvale, CA
+1.408.220.2200

EMEA Headquarters
Hampshire, UK
+44.1252.554600

APAC Headquarters
Singapore
+65.6826.7000