

Blue Coat Mail Threat Defense - S400

Secure Email Against Targeted Phishing Attacks

Email is one of the most common attack vectors used by hackers to get into your corporate network. Attackers will send targeted communications “phishing” for information they can use to perpetrate other attacks and establish a foothold in your organization they can use to spread. They may try to trick your users into providing sensitive data – such as usernames and passwords, financial records, etc. – or get them to click on a link or open a file that contains malicious code that automatically infects the endpoint. To protect against these types of attacks, you need a solution that is capable of identifying and preventing the varied phishing methods attackers deploy – you need Blue Coat Mail Threat Defense.

Blue Coat Mail Threat Defense protects against email-borne malware in links and attachments that are activated by unsuspecting end users. The solution can identify and extract malicious content from an email before it is delivered to the user to neutralize the attack. As a result, you can effectively enforce corporate security policies and keep your resources safe, without impacting the user’s experience.

Blue Coat Defeats Targeted Attacks

Mail Threat Defense inspects and analyzes all email messages for malicious content before they arrive in the targeted user’s in-box. If there is malware contained within embedded URL links or file attachments, Mail Threat Defense will identify it and actively block, alter, or quarantine the message, based on the severity of the threat and your corporate security policy. The solution has no impact on the user experience, beyond ensuring they only receive sanitized, safe messages in their inbox.

Eliminates Known Attacks

Mail Threat Defense scans embedded file attachments and URL links to identify known malware and takes action based on your

corporate security policy. The solution also identifies files and URLs that are known to be good and sends those safe messages on to the user. Mail Threat Defense applies a variety of sophisticated techniques to quickly identify both known bad and good files and URLs, including:

- URL Filtering
- File Hash Reputation
- Anti-Virus Detection
- Static Code Analysis

The solution leverages the Blue Coat Global Intelligence Network, which collects and analyzes over a billion previously uncategorized new web requests a day from our 15,000 enterprise customers and their millions of users accessing the Internet daily.

Uncovers New Attacks

Mail Threat Defense can identify never-before-seen, unique and zero-day malware. It extracts any unknown files and URLs it detects and sends them to Blue Coat Malware Analysis for identification and risk scoring. Malware

AT A GLANCE

Defeats Targeted Attacks

- Ability to identify attacks in embedded file attachments and URL links
- Delivers screened and sanitized email messages to end users

Eliminates Known Attacks

- Uses sophisticated techniques to quickly identify both known bad and good files and URLs
- Leverages the Global Intelligence Network to stay up-to-date on the latest threats

Uncovers New Attacks

- Uses precise detonation chambers to uncover new, zero-day attacks. Understands the risk level of new attacks with targeted malicious risk scoring

Provides Configurable Security Policies

- Supports the unique security enforcement need of the organization
- Balances message delivery speed, user autonomy desires and business needs

Analysis is an advanced, multi-stage sandbox that uses precisely tailored, gold-image detonation chambers to perform recursive analysis on any primary files or URLs, plus any subsequent “dropped” files and callback URLs. It uses:

- Static Code Analysis
- Dynamic/Behavioral Analysis
- Reputational Analysis
- YARA Rules Analysis

The solution will then provide a targeted risk score for the malware it has discovered, so you can effectively address and mitigate the risk posed by this previously unknown threat.

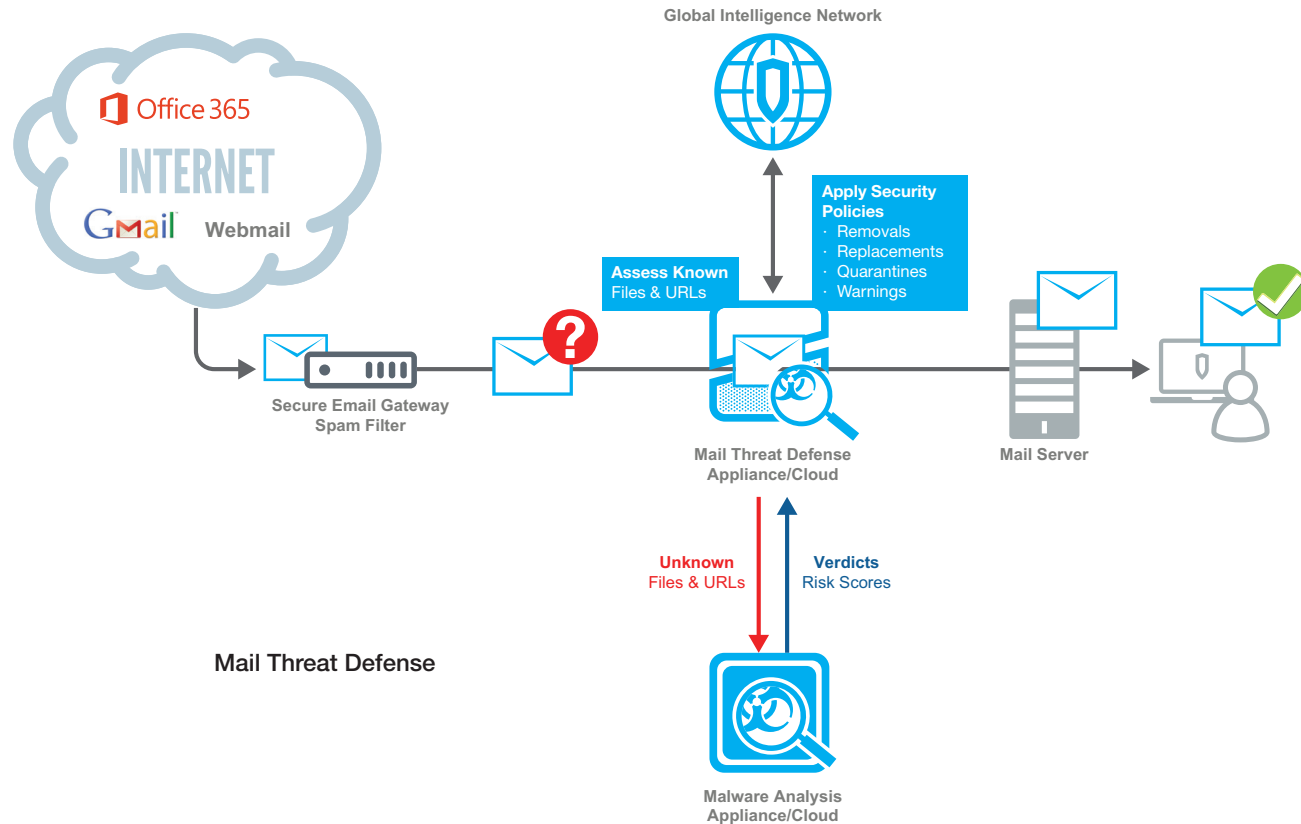
Provides Configurable Security Policies

The security policies of Mail Threat Defense enable you to balance message delivery speed, user autonomy desires and business security needs. Based on the verdicts and malicious risk scores determined by the solution, you can enact policies that block, alter, quarantine or detect / alert on the malware. As a result, you can:

- Remove malicious attachments
- Remove / Replace malicious links
- Add malicious content warnings
- Quarantine malicious messages

Deployment Modes

The solution can be deployed inline, as a cloud-based service or an on-premises appliance. It is typically positioned behind the firewall, after the SPAM filter, to ensure it can inspect all mail before it is delivered to the user. Note, the solution can also be deployed passively, alerting you as soon as email malware is detected. It seamlessly integrates with any other email security solutions you have to preserve and enhance the value of your investments.



| | APPLIANCES | | VIRTUAL APPLIANCE |
|--------------------------------------|---|---|---------------------------|
| MAIL THREAT DEFENSE MALWARE ANALYSIS | MTD S400-10 MAA S400-10 | MTD S400-20 MAA S400-10 | MTD-VA ¹ |
| PERFORMANCE | | | |
| ADVANCED MAIL ANALYSIS | Up to 300,000 emails / day | Up to 500,000 emails / day | Up to 300,000 emails /day |
| SYSTEM | MTD S400-10 ONLY | MTD S400-20 ONLY | MTD-VA |
| DISK DRIVES | 3 x 1 TB | 6 x 1 TB | 100 GB HDD |
| RAM | 24 GB | 48 GB | 8 GB |
| ONBOARD PORTS | <ul style="list-style-type: none"> (2) 1000Base-T Copper ports 1000Base-T Copper, System Management Port (1) 1000 Base-T Copper, BMC Management Port² | <ul style="list-style-type: none"> (2) 10Gb Base-T Copper ports 1000Base-T Copper, System Management Port (1) 1000Base-T Copper, BMC Management Port² | 2 virtual NICs |
| OPTIONAL NICS | <ul style="list-style-type: none"> 2x10Gb Base-T Copper | <ul style="list-style-type: none"> 2x10Gb Base-T Copper | |

¹ Virtual appliance minimum specifications using VMWare ESX 5.0 or later and 4 CPU cores. MTD-VA also utilizes Malware Analysis MAA S400-10.

² BMC ports are currently disabled

| PHYSICAL PROPERTIES | MTD S400, MAA S400 APPLIANCES |
|------------------------------|---|
| DIMENSIONS AND WEIGHT | |
| DIMENSIONS | 572mm x 432.5mm x 42.9mm (22.5in X 17.03in X 1.69in) (chassis only) 643mm x 485.4mm x 42.9mm (25.3in x 19.11in x 1.69in) (chassis with extensions) 1 RU height |
| WEIGHT (MAXIMUM) | Approx. 12.8 kg (28 lbs) +/- 5% |
| OPERATING ENVIRONMENT | |
| POWER | Dual redundant and hot swappable power supplies, AC power 100-240V, 50-60Hz, 4A (DC power available) |
| MAXIMUM POWER | 450 Watts |
| THERMAL RATING | Typical: 1086 BTU/hr, Max: 1381 BTU/hr |
| TEMPERATURE | 5°C to 40°C (41°F to 104°F) at sea level |
| HUMIDITY | 20 to 80% relative humidity, non-condensing |
| ALTITUDE | Up to 3048m (10,000ft) |

| MAIL THREAT DEFENSE APPLIANCES | | |
|--------------------------------|---|--|
| REGULATIONS | SAFETY | ELECTROMAGNETIC COMPLIANCE (EMC) |
| International | CB – IEC60950-1, Second Edition | CISPR22, Class A; CISPR24 |
| USA | NRTL – UL60950-1, Second Edition | FCC part 15, Class A |
| Canada | SCC – CSA-22.2, No.60950-1, Second Edition | ICES-003, Class A |
| European Union (CE) | CE – EN60950-1, Second Edition | EN55022, Class A; EN55024; EN61000-3-2; EN61000-3-3 |
| Japan | --- | VCCI V-3, Class A |
| Mexico | NOM-019-SCFI by NRTL Declaration | --- |
| Argentina | S Mark – IEC 60950-1 | --- |
| Taiwan | BSMI – CNS-14336-1 | BSMI – CNS13438, Class A |
| China | CCC – GB4943.1 | CCC – GB9254; GB17625 |
| Australia/New Zealand | AS/NZS 60950-1, Second Edition | AS/ZNS-CISPR22 |
| Korea | | KC – RRA, Class A |
| Russia | CU – IEC 60950-1 | GOST-R 51318.22, Class A; 51318.24; 51317.3.2; 51317.3.3 |
| ENVIRONMENTAL | RoHS-Directive 2011/65/EU, REACH-Regulation No 1907/2006 | |
| PRODUCT WARRANTY | Limited, non-transferable hardware warranty for a period of one (1) year from date of shipment. BlueTouch Support contracts available for 24/7 software support with options for hardware support. | |
| GOV'T CERTIFICATIONS | For further government certification information please contact Federal_Certifications@bluecoat.com | |
| MORE INFO | Contact regulatoryinfo@bluecoat.com for specific regulatory compliance certification questions and support | |

© 2016 Blue Coat Systems, Inc. All rights reserved. Blue Coat, the Blue Coat logo, BlueTouch, CacheFlow, CloudSOC, ContentIQ, Elastica, IntelligenceCenter, PacketShaper, Perspecsys, PolicyCenter, ProxyOne, ProxySG, StreamIQ, and WinProxy are registered trademarks or trademarks of Blue Coat Systems, Inc. or its affiliates in the U.S. and certain other countries. This list may not be complete, and the absence of a trademark from this list does not mean it is not a trademark of Blue Coat or that Blue Coat has stopped using the trademark. All other trademarks mentioned in this document owned by third parties are the property of their respective owners. This document is for informational purposes only. Blue Coat makes no warranties, express, implied, or statutory, as to the information in this document. Blue Coat products, technical services, and any other technical data referenced in this document are subject to U.S. export control and sanctions laws, regulations and requirements, and may be subject to export or import regulations in other countries. You agree to comply strictly with these laws, regulations and requirements, and acknowledge that you have the responsibility to obtain any licenses, permits or other approvals that may be required in order to export, re-export, transfer in country or import after delivery to you. v.DS-MAIL-THREAT-DEFENSE-S400-EN-v3a-0616

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