BLUE COAT®

Security Empowers Business

EMAIL-BASED THREAT PROTECTION WITH FULL VISIBILITY THAT INTEGRATES WITH MALWARE SANDBOXING

Blue Coat MailThreat BLADE

DATASHEET

Advanced persistent threats and zero-day malware use email as a common medium to breach the most secure networks. Enterprises are challenged with protecting their organizations from email-based threats, despite broad deployment of anti-spam/phishing solutions. With the changing threat landscape and ever-increasing number of attacks, organizations are struggling to protect their assets and infrastructure. More than 200,000 new malware samples are discovered every day, and exploits are evolving and diversifying quickly.

Meanwhile, today's advanced and unknown malware continue to evade even the best traditional security defenses, with email being used as an effective method of delivery. Enterprises face many challenges in gaining protection against these modern day threats, including:

- Attackers that increasingly use email and social engineering techniques to deliver targeted viruses, worms, trojans and other types of malware into even the most secure networks
- 47% of email is now opened on a mobile device ("Email Analytics", Litmus, Aug 2013)
- BYOD initiatives freely allow corporate users into the trusted network
- Cybercriminals, hacktivists and state-sponsored attackers utilizing various tactics, techniques and procedures that incorporate sophisticated email schemes
- The explosion of social media and Web 2.0 – including Facebook, LinkedIn and Twitter – and the mandate to embrace them within the enterprise
- Unintentional loss of sensitive data through employees' lack of email security awareness
- A growing security gap where even the largest, most fortified networks are still not immune to attacks and often face public shame

According to a recent Verizon Business Data Breach report, 47% of successful malware used email attachments as the threat vector. Targeted and zero-day attacks continue to dominate the headlines, whether at the hands of cybercriminals, hacktivists or nation states. Recently, state-sponsored hackers used spear phishing techniques to target and compromise global media giants, gaining access to trusted networks and sensitive data. Because traditional technologies can't defend against what they can't see, today's IT security teams need the context, content and visibility required to effectively detect and identify zero-day attacks, APTs, and next-generation malware. Although perimeter prevention-based security controls are still an important component of an effective defense-in-depth strategy, they alone are not enough in today's post-prevention world. As a result, today's advanced, stealthy and evasive malware continues to compromise even the most secure networks and devices.

The Solution

Blue Coat is revolutionizing advanced threat protection by unifying blocking and enforcement, advanced security analytics, threat intelligence and security, and SSL visibility. This Advanced Threat Protection Platform combines with the new Blue Coat ThreatBLADES, which deliver a host of extensible and fully integrated software blades on the industry-leading Security Analytics Platform. Blue Coat ThreatBLADES provide dynamic, up-to-date intelligence and analysis on today's advanced persistent threats. All of the powerful and flexible ThreatBLADES use a cloud-based threat intelligence infrastructure powered by the Blue Coat Global Intelligence Network – leveraging the collaborative 'network effect' of more than 75 million users. Blue Coat ThreatBLADES are also tightly integrated with the Blue Coat Malware Analysis Appliance, a unique, next-generation malware analysis and sandboxing solution that delivers highly accurate threat verdicts. Now, as part of the Blue Coat ThreatBLADES portfolio, the MailThreat BLADE delivers superior protection against unknown and advanced malware, malicious files and zero day attacks delivered via email.

The MailThreat BLADE is tightly integrated with the Security Analytics Platform and Security Analytics Central Manager for maximum efficiency, full security visibility and total contextual analysis across all email traffic. The MailThreat BLADE is deployed on the Security Analytics Appliance, Security Analytics Software or Security Analytics Virtual Appliance.

BLUE COAT®

Security Empowers Business

DATASHEET

Blue Coat MailThreat BLADE

The Blue Coat MailThreat BLADE – powered by integrated malware analysis and sandboxing technology from Blue Coat – detects, classifies and safely analyzes email-based threats that are missed by traditional messaging security gateway solutions. It allows enterprises to quickly and accurately identify zero-day attacks, advanced persistent threats and other malicious code embedded within email attachments – including Microsoft Office documents, PDFs, Java files, EXE files and much more. For the first time, enterprises can gain full visibility and perform the industry's most comprehensive malware analysis on all email traffic – including SMTP, POP3, IMAP and Web mail. MailThreat BLADE compares email attachment file-hashes against known good and bad file knowledgebases before forwarding them for sandbox detonation, optimizing malware analysis. And, our unique dual-method virtualization and emulation sandbox design achieves unprecedented detection accuracy of VM-evasive malware. Using the Security Analytics Platform, enterprises will be able to create policies that will trigger alerts when a known malicious email is detected in their network. The MailThreat BLADE also uses the full packet capture capabilities of the Security Analytics Platform to enable full reconstruction of emails and attachments in human-readable format to monitor and investigate sensitive data loss.

The powerful Global Intelligence Network and the network effect of 15,000 customers and 75 million users allows the MailThreat BLADE to have the latest information on all known malicious URL links embedded in emails.

KEY FEATURES

- Powered by integrated sandbox technology from Blue Coat
- Real-time extraction of email attachments for malware analysis
- Monitor all email traffic including SMTP, POP3, IMAP traffic and webmail
- Full email reconstruction, delivered in its original format
- Single-user interface combines email threat detection and security analytics
- Built on the industry-leading Security Analytics Platform

KEY BENEFITS

- Hybrid sandbox for highly accurate detection of email-based malware
- Near real-time threat detection on unknown and embedded malware
- Comprehensive malware coverage for all email attachments
- Optimized attachment analysis with extensive hash-lookups before sandboxing
- Unified management delivered in a single pane-of-glass
- Industry's only solution combining email threat protection with security analytics
- No hardware – flexible and extensible software blade eliminates CAPEX costs

SPECIFICATIONS

FORM FACTOR	Software Blade
SUPPORTED SENSORS	Security Analytics Appliances, Software and Virtual Appliance
DEPLOYMENT OPTIONS	Al-a-carte or as part of the Blue Coat Advanced Threat Protection (ATP) Suite
EMAIL PROTOCOLS	SMTP, POP3, IMAP and webmail
SANDBOX	Blue Coat Malware Analysis Appliance or 3rd-party sandboxing technology
ACTIONS & ALERTS	Real-time alerts based on IP and URL reputation or known email-based attacks
USER INTERFACE	Integrated into Security Analytics Dashboard
CENTRAL MANAGEMENT	Security Analytics Central Manager

REQUIREMENTS

SOFTWARE VERSION	v7.1 or higher
SOFTWARE	Blue Coat MailThreat BLADE or Blue Coat ATP Suite
SENSORS	Security Analytics 2G/10G Appliances, Security Analytics Software or Security Analytics Virtual Appliance
MINIMUM CPU CORES	Four
MINIMUM RAM	8 GB
MINIMUM STORAGE	500 GB
MINIMUM INTERFACES	2

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