

Blue Coat MalwareAnalysis BLADE



MalwareAnalysis BLADE

Comprehensive, Open and Extensible Protection Against Zero-Day Threats, Targeted Attacks and Advanced Malware

THE CHALLENGE

For years, organizations have built strong perimeters and complex firewall rules to keep the enemy out—deploying more and more security point-products along the way in an effort to stay ahead of the threat. Unfortunately, today’s persistent threats and threat actors target enterprises with customized malware and targeted attacks that fly under the radar of traditional, signature-based security technologies. As a result, today’s advanced, stealthy and evasive malware continues to compromise even the most secure networks and devices. According to the 2013 Verizon Data Breach Investigations Report:

- 84% of advanced target attacks compromise their target in seconds, minutes or hours
- 78% of advanced target attacks take weeks, months or years to discover

Successful targeted and zero-day attacks continue to dominate the headlines – whether at the hands of cybercriminals, hactivists or nation states. Recently, several media giants joined the ranks of big banks, defense contractors, government agencies, leading Internet providers and energy companies all penetrated by hackers using advanced threats and targeted attacks. 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 advanced and unknown malware.

THE SOLUTION

Blue Coat and Solera Networks are revolutionizing advanced threat protection by unifying big data security analytics, threat intelligence and security 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 Solera Security Analytics Platform (formerly Solera DeepSee). Blue Coat ThreatBLADES provide dynamic, up-to-date threat intelligence 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 WebPulse Collaborative Defense Cloud—leveraging the collaborative ‘network effect’ of more than 75 million users. Now, as part of the Blue Coat ThreatBLADES portfolio, the MalwareAnalysis BLADE delivers superior protection against unknown and advanced malware, malicious files and zero-day attacks.

SECURITY IS ABOUT WHAT YOU MAKE POSSIBLE



Blue Coat ThreatBLADES™

Blue Coat ThreatBLADES deliver a comprehensive solution that integrates with the award-winning Solera Security Analytics Platform to unify big data security analytics, threat intelligence and security visibility.



MalwareAnalysis BLADE™

KEY FEATURES

- Integrated sandboxing on the Solera Security Analytics Platform
- VM Sandbox provides Intelligent virtualized malware detonation
- Emulator Sandbox simulates bare metal environments to detect evasive malware
- On-premises, cloud-based or ecosystem-integrated deployment options
- Malware analysis covering dozens of file-transport
- Optimized and smart detonation only on unknown malware
- Integrated with Blue Coat WebPulse Collaborative Defense Cloud

Blue Coat MalwareAnalysis BLADE

The Blue Coat MalwareAnalysis BLADE—powered by integrated sandbox technology from Blue Coat—detects, identifies and safely analyzes suspected malware-infected files. This allows enterprises to quickly and accurately identify zero-day attacks, advanced persistent threats and other malicious code embedded within



dozens of file types—including Microsoft Office documents, PDFs, Java files, EXE files and more. For the first time, enterprises can gain full visibility and perform the most comprehensive malware analysis across the entire network—including advanced malware capable of rapidly spreading to multiple network locations and devices. The MalwareAnalysis BLADE leverages the Solera Platform's dynamic, machine-learning ThreatProfiler engine—which automatically and efficiently extract dozens of file types

and objects in real-time for proactive malware analysis. And, our unique hybrid virtualization and emulation sandbox design achieves unprecedented detection accuracy of evasive malware for faster time-to-protection and greater ability to minimize impact.

The MalwareAnalysis BLADE works together with other Blue Coat ThreatBLADES, and is tightly integrated with the Solera Security Analytics Platform and Solera Central Manager for maximum efficiency and total contextual analysis across the enterprise. What's more, the MalwareAnalysis BLADE allows the freedom to choose between a locally controlled on-premises deployment, a highly scalable cloud-based solution, or an integrated deployment with other best-of-breed analysis platforms through Solera's flexible file-broker architecture.

KEY BENEFITS

- Unique hybrid sandboxing design delivers unrivaled malware and threat detection
- Multiple deployment options provide freedom of choice
- Automated, real-time alerting on malware and zero-day threats
- Optimized and contextual malware analysis for faster time-to-resolution
- Machine-learning architecture minimizes submitted malware samples
- Unified management delivered in a single pane-of-glass
- Flexible and extensible software blade eliminates CapEx costs

Blue Coat MalwareAnalysis BLADE detects and analyzes suspected malware-infected files (with integrated Blue Coat malware-detonation sandbox technology), identifies zero-day attacks and advanced persistent threats (APTs), and provides actionable intelligence for eradicating infections

Additional Blue Coat ThreatBLADES



**WebThreat
BLADE™**

Dynamic, real-time and comprehensive protection against web- and email-based threats



**FileThreat
BLADE™**

Optimized and comprehensive detection of viruses, worms and all kinds of malware for virtually any file type





Combining Blue Coat ThreatBLADES into an easy-to-deploy, integrated suite

SOFTWARE SPECIFICATIONS

| | |
|--------------------|---|
| Software Version | Solera Platform v7.0 or higher |
| Form Factor | Software Blade |
| Supported Sensors | Solera Appliances, Solera Software and Solera Virtual Appliance |
| Deployment Options | On-premises or cloud-based |
| File Transport | Extracts files from dozens of file-transports |
| File Search | MD5/SHA1-based search |
| Actions & Alerts | Real-time file extraction and e-mail alerts |
| User Interface | Integrated into Solera Dashboard – Single Pane of Glass |
| Central Management | Solera Central Manager |

ON-PREMISES MALWARE ANALYSIS APPLIANCE SPECIFICATIONS

| | Management Ports | Performance | Rack Height | Rack Depth | Power Supplies |
|---|------------------------|------------------------------|---------------|----------------|-------------------------|
|  <p>Blue Coat MalwareAnalysis 1U Appliance</p> | 2 -- 10/100/1000 BaseT | Up to 10,000 samples per day | 1 – Rack Unit | 710 mm / 28" | Dual, Hot-plug – 750 W |
|  <p>Blue Coat MalwareAnalysis 2U Appliance</p> | 2 -- 10/100/1000 BaseT | Up to 50,000 samples per day | 2 – Rack Unit | 723 mm / 28.5" | Dual, Hot-plug – 1100 W |

ABOUT SOLERA NETWORKS, A BLUE COAT COMPANY

Solera Networks, a Blue Coat Company, is the industry's leading provider of big data security analytics for advanced threat protection. Its award-winning Solera Platform levels the battlefield against advanced targeted attacks and malware, and gives security professionals clear and concise answers to the toughest security questions. The Solera Platform is powered by next-generation deep-packet inspection and indexing technologies, full-packet capture, malware analysis and real-time security intelligence and analytics capabilities. Global 2000 enterprises, cloud service providers and government agencies rely on Solera for real-time situational awareness, continuous monitoring, security incident response, advanced malware detection, data loss monitoring and analysis, organization policy compliance and security assurance—allowing them to respond quickly and intelligently to advanced threats and attacks, while protecting critical information assets, minimizing exposure and loss, and reducing business liabilities.

© 2013 Blue Coat Systems, Inc. All rights reserved. Blue Coat, the Blue Coat logos, ProxySG, PacketShaper, CacheFlow, IntelligenceCenter, CacheEOS, CachePulse, Crossbeam, K9, the K9 logo, DRTR, Mach5, Packetwise, Policycenter, ProxyAV, ProxyClient, SGOs, WebPulse, Solera Networks, the Solera Networks logos, DeepSee, "See everything. Know everything.", "Security Empowers Business", and BlueTouch 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.