Blue Coat FileThreat BLADE

SECURITY IS ABOUT WHAT YOU MAKE POSSIBLE

FileThreat BLADE

Optimized and Comprehensive Detection of Viruses, Worms and Malware Embedded in Virtually any File Type

THE CHALLENGE

Organizations are often blind to the activities of cybercriminals, hactivists and nation states due to the fact that advanced malware and zero-day attacks fly under the radar of even the most fortified enterprises. Today's persistent threats target enterprises using customized or embedded malware that evades the detection of traditional, signature-based security technologies. As a result, there is a significant increase in malicious files that successfully compromise even the most fortified enterprise networks. These new threats and attack techniques are causing significant damage, while threatening critical information assets and resources. And, once attackers are in the network, they stay in—leveraging their foothold to perform ongoing data exfiltration. 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

Performing virus and malware scans on endpoints alone is not enough to detect advanced and targeted attacks. Traditional security technologies do not have the capability to fully reconstruct and inspect the variety of potentially malicious file formats or file objects. And, despite the effectiveness of sandboxing technology to uncover the true nature and intent of malicious files, analyzing and detonating every suspicious file requires significant processing power and is highly inefficient. Enterprises need visibility, context and up-to-date threat intelligence on all the files traversing their network—allowing them to make optimized and informed decisions while minimizing the need to submit every file sample to expensive malware sandboxing systems.

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

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.

FileThreat BLADE™

KEY FEATURES

- Leverages industry's largest repository of known good files
- Dynamic scan and up-to-date knowledge-base of all known good and bad files
- Real-time extraction of virtually any file type
- Integrated file reputation and threat intelligence feeds from Blue Coat WebPulse
- Dynamic, machine-learning knowledge for optimized malware analysis
- Combines with the MalwareAnalysis BLADE for a unified analysis of malicious files
- Built on the industry-leading Solera Security Analytics Platform

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 FileThreat BLADE provides optimized, real-time protection against known malware and malicious files.

Blue Coat FileThreat BLADE

The Blue Coat FileThreat BLADE is an all-new software blade—powered by the WebPulse Collaborative Defense Cloud—that delivers real-time file reputation intelligence to guard against known viruses and malware embedded within virtually any file type. This innovative solution leverages the Solera Security Analytics Platform's real-time file extraction capability to reconstruct files based on pre-defined rules—while its machine-learning engine conducts dynamic analysis to detect advanced threats. The FileThreat BLADE benefits from the Solera Platform's intelligent algorithms that collect actionable knowledge on any known good and known bad file type, while storing file information in a local machine-learning database. The result is optimized malware analysis and a dynamic, up-to-date knowledge base leveraging both the Blue Coat MalwareAnalysis BLADE and the WebPulse Collaborative Defense Cloud. And, the Blue Coat FileThreat BLADE requires less computing power and provides faster time-to-protection—without unnecessary malware-detonation on known bad files.

The FileThreat 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, security visibility and contextual analysis on all files crossing the network. Enterprises gain unrivaled protection against known bad files through a combination of real-time threat intelligence feeds and the Solera Platform's ability to reconstruct and deliver accurate and actionable file-level evidence from raw packet data.

KEY BENEFITS

- Faster time-to-protection with locally cached file threat knowledge base
- Comprehensive coverage detects advanced malware in virtually every file type
- Machine-learning, ThreatProfiler engine for accurate, real-time detection of malicious files
- Intelligent algorithms deliver context-based malware analysis and threat intelligence
- Up-to-the-minute defense and inoculation against all known malicious files
- Unified management delivered in a single pane-of-glass
- Flexible and extensible software blade eliminates CapEx costs

Additional Blue Coat ThreatBLADES

WebThreat BLADE™

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

MalwareAnalysis BLADE™

Comprehensive, open and extensible protection against zero-day threats, targeted attacks and advanced malware

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

SPECIFICATIONS

Form Factor	Software Blade
Supported Sensors	Solera Appliances, Solera Software and Solera Virtual Appliance
Deployment Options	Single software blade or as part of the ATP Suite
Files	Detects and extracts files from dozens of file-transports
File Search	MD5/SHA1-based search
Actions	Real-time file extraction and analysis rules
Alerts	E-Mail based alerts with syslog
User Interface	Integrated into Solera Dashboard
Central Management	Solera Central Manager

REQUIREMENTS

Solera Platform	v7.0 or higher
Software	Solera FileThreat BLADE or Solera Advanced Threat Protection Suite
Sensors	Solera 2G Appliance, Solera 10G Appliance, Solera Software or Solera Virtual Appliance
Minimum CPU Cores	Four
Minimum RAM	8 GB
Minimum Storage	500 GB
Minimum Interfaces	2

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.

Solera Networks Headquarters
10713 South Jordan Gateway
Suite 100
South Jordan, Utah 84095

www.soleranetworks.com
info@soleranetworks.com
877-5SOLERA or 877-576-5372
801-545-4100

BLUE COAT | SOLERA NETWORKS™ A BLUE COAT COMPANY