BLUE COAT®

Security Empowers Business

DATASHEET

SEE, UNDERSTAND, RESPOND TO, AND PREVENT ADVANCED ATTACKS

Blue Coat Security Analytics Software

Advanced targeted attacks, customized malware, and zero-day attacks are infiltrating networks at record speeds. Traditional security infrastructure and tools are not keeping pace. In fact, recent reports indicate that 84% of attacks compromised their target within seconds, minutes or hours, while 78% of attacks take days, months, or even years to discover. Blue Coat has a solution. Blue Coat Security Analytics Software, an integral part of the Blue Coat Advanced Threat Protection Lifecycle Defense, delivers the full visibility, security analytics, and real-time threat intelligence you need to successfully protect your infrastructure and your workforce – and empower your business.

Sophisticated Protection from Advanced Threats

Advanced security threats require a modern, comprehensive strategy that provides the intelligence and real-time analysis needed to see, understand, respond to, and prevent advanced threats and targeted attacks. An effective solution must:

- Use security analytics to provide answers to the most difficult post-breech questions, including: Who hacked us? How did they do it? Which data/systems were affected? Is it over? How do we prepare for subsequent attacks?
- Accommodate simple, fast and scalable deployments to all corners of your organization, from the data center to remote/branch offices.
- Leverage previous technology investments and integrate with existing security tools such as next-gen firewalls, IDS/IPS, SIEM, malware analysis and other tools that focus on “known” threats.
- Easily fit within security budgets that are already stretched.

Blue Coat Security Analytics Software is the industry’s only comprehensive solution that delivers the full visibility, security analytics, and real-time threat intelligence you need to successfully protect your business.

Unlike other tools that claim to provide advanced threat protection, Blue Coat can truly deliver a cost-effective solution on your hardware of choice, allowing you to leverage the efficiencies and buying power you have established with leading hardware providers.

Security Analytics Software provides:

Application Classification – More than 1,800 applications and thousands of descriptive metadata attributes, including content types, file names, user personas, are classified for easy analysis and recall.

Real-time Threat Intelligence – Blue Coat ThreatBLADES integrate directly with Security Analytics Software and leverage the Blue Coat Global Intelligence Network to deliver instant, actionable, real-time intelligence on threats delivered via web, email or file.

Layer 2 to 7 Analytics – Security Analytics Software provides a variety of analysis tools

AT A GLANCE

Description

Security Analytics Software delivers complete network visibility and situational awareness to provide clear, actionable intelligence about security threats to enable swift and targeted incident response.

Capabilities

- Records and classifies every packet of network traffic and provides intelligence about threats to applications, files, and web content
- Automatically analyzes all network traffic and enables immediate alerting about zero-day threats and next-generation malware
- Supports large-scale, multi-location deployments, with central management for visibility across software, appliance, or virtual appliance deployments

Key Benefits

- Gain 20/20 visibility into advanced malware, targeted threats and zero-day attacks
- Respond faster with 100% situational awareness of any network activity before, during and after an attack
- See every detail of an event with Layer 2-7 traffic capture and deep packet inspection
- Optimize performance of next-generation malware analysis and sandboxing
- Quickly achieve results with fast, flexible deployment anywhere

DATASHEET

such as complete session reconstruction, data visualization, Root Cause Explorer, timeline analysis, file and object reconstruction, IP geolocation, and trend analysis.

Context-Aware Security – The software integrates with best-of-breed security technologies such as next-gen firewalls, IDS/IPS, DLP, SIEM, and malware analysis tools to pivot directly from any alert or log and obtain full-payload detail and evidence of the exact source and scope of the event – before, during and after the breach. Key integrations include Dell SonicWALL™, FireEye™, HP ArcSight™, McAfee®, Palo Alto Networks™, Sourcefire®, Splunk®, and many other security applications.

Root Cause Explorer – Uses extracted network objects to reconstruct a timeline of suspect web sessions, emails, and chat conversations.

Visibility into Encrypted Data – With the Blue Coat SSL Visibility Appliance, Security Analytics Software provides complete visibility into threats that hide within encrypted traffic.

Industry-Standard Hardware Compatibility – Security Analytics Software is easily deployed on industry-standard, server-class hardware platforms.

Benefits

- **20/20 visibility** into advanced malware, targeted threats and zero-day attacks
- **100% situational awareness** of any network activity – before, during and after an attack
- **Cost reduction** through lower capital expenditures and reduced footprint
- **Easy to deploy, use, and manage** in standalone or distributed operation
- **On-demand incident response** with remote deployment
- **Integration with existing security controls** to deliver advanced threat protection
- **Scalability** to expand as your coverage and storage needs grow

Features

- Fully featured security intelligence and analytics solution
- Complete network capture (layers 2-7), indexing, classification, deep packet inspection, storage and replay
- Integration with Blue Coat Global Intelligence Network
- Performance and scalability to support large-scale, multi-location deployments
- Central management to gain enterprise-wide visibility across software, appliance or virtual appliance deployments
- Integrates with common, existing security controls such as NGFW, IPS, SIEM and more

BLUE COAT®

Security Empowers Business

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

© 2015 Blue Coat Systems, Inc. All rights reserved. Blue Coat, the Blue Coat logos, ProxySG, PacketShaper, CacheFlow, IntelligenceCenter, CacheOS, 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. v.DS-SECURITY-ANALYTICS-SOFTWARE-EN-v3c-0415