BLUE COAT

Network
+ Security
+ Cloud

Blue Coat Content Analysis System with Cylance INFINITY ENGINE

Adding Predictive File Analysis to Your Cybersecurity Arsenal

SOLUTION BRIEF

There are some things you know you want to allow in your network and others you know you don't; to ensure you are not wasting precious time and resources worrying about the files you know to be 'good' or 'bad' you need a way to quickly and accurately identify and filter them. File whitelisting is commonly used to quickly identify and deliver 'good' files to their recipient, while signature-based anti-malware can detect files that are known to be 'bad' and block them. Adding predictive file analysis provides even more granular filtering, allowing you to block files, in real-time, that exhibit malicious characteristics to further reduce the noise and impact of attacks in your network. The Blue Coat Content Analysis System with the Cylance INFINITY ENGINE is designed to deliver all of these capabilities and more to fortify your network against known attacks and advanced malware.

The Addition of Predictive File Analysis

The Cylance INFINITY ENGINE adds predictive file analysis to the already robust capabilities of the Blue Coat Content Analysis System to deliver unparalleled filtering and attack identification. The Content Analysis System uses Cylance's predictive model to classify files as good, unsafe or abnormal; it correlates a file's characteristics with the features found in millions of good and bad samples to detect known, as well as unknown and zero-day attacks.

The Cylance INFINITY ENGINE provides a confidence score for every sample as part of its classification process. For instance, a good file with a Cylance score of 0.80 means the model is 80% confident the file is good; abnormal samples will have low scores. These scores become part of the Content Analysis System's Threat Indicator Reports, which explain the classifications. For example, a Report could call out an executable's capabilities, such as the logging of keystrokes, the ability to inject code or terminate other processes, the ability to tamper with a Windows® firewall policy, etc. This data can help accelerate the ongoing analysis and response to threats that have been detected.

Delivering Comprehensive Security

The Content Analysis System with the Cylance INFINITY ENGINE works in tandem with the Blue Coat Malware Analysis Appliance and ProxySG to enable you to automate advanced threat protection at the gateway and protect your files against known, unknown and advanced malware. When files are classified as unsafe or abnormal, they can be sent to sandbox devices from Blue Coat or third parties for further behavioral-based analysis that can help you understand the nature of attacks targeting the custom applications and specific files and folders of your organization's gold images. This information can be shared

AT-A-GLANCE

PROBLEM

Need a quick, accurate way to identify and block malicious files.

SOLUTION

Blue Coat Content Analysis System with Cylance INFINITY ENGINE

BENEFITS

- **Game-Changing Malware Detection** – capable of identifying known, unknown and zero-day attacks in files.
- **Higher Barrier for Attackers** – vast analysis and broad spectrum classification makes it harder for attackers to hide their attacks.
- **Improved Operations** – ability to quickly deploy to reduce the time it takes to detect advanced malware.

SOLUTION BRIEF

BLUE COAT®

Network
+ Security
+ Cloud

with the Blue Coat ProxySG appliances, at both a local and worldwide level, to automate the blocking of newly identified threats at the gateway, as well as the Blue Coat Security Analytics Platform to support advanced threat profiling and the remediation of the full scope of an attack.

How It Works

The Blue Coat Content Analysis System with the Cylance INFINITY ENGINE collects file information, extracts specific file characteristics, analyzes what these characteristics mean, from a threat perspective, and then classifies the files to ensure they are appropriately handled by your security infrastructure.

Collection

Much like DNA analysis, file analysis starts with the collection of a massive amount of data – in this case the collection of specific file types (executables, dlls, .pdf, .doc, .xls, etc.). Hundreds of millions of these files are collected via 'feeds' from industry sources, proprietary organizational repositories and live inputs from active computers using a Cylance agent.

Extraction

The next phase in the machine learning process is attribute extraction. This process is substantively different from the process of behavior identification or malware analysis. Rather than looking for things which people believe are suggestive of something that is malicious, Cylance leverages the compute capacity of machines and data mining techniques to identify and extract the broadest possible set of file characteristics to remove any bias that could be introduced by manual classification. These characteristics are based on the file type and can be as basic as the PE file size or the compiler used or as complex as a review of the first logic leap in the binary. By using thousands of attributes, the Cylance INFINITY ENGINE substantially increases the cost for an attacker to create a piece of malware that cannot be characterized by the Content Analysis System.

Learning and Adaptation

Once the attributes are collected, the attribute output is normalized and converted to numerical values that can be used to build statistical models. Leveraging the millions of file attributes identified during the extraction, Cylance mathematicians develop statistical models that accurately predict whether a file is valid or malicious. It is important to remember that for each and every file, thousands of attributes are analyzed to differentiate between legitimate files and malware. The solution can divide a single file into an enormous number of characteristics and analyze each one against hundreds of millions of other files to make decisions about the normalcy of the characteristics.

Classification

Cylance INFINITY ENGINE embeds the statistical models and enables the classification of samples, either locally or through a cloud lookup, which can be used to quickly allow or block files at the gateway. This classification takes milliseconds and is very precise as a result of the breadth of the file characteristics analyzed.

Benefits

The Blue Coat Content Analysis System with the Cylance INFINITY ENGINE delivers the intelligent, defense-in-depth capabilities you need:

- **Game-Changing Malware Detection** – The Content Analysis System with the Cylance INFINITY ENGINE identifies threats in Windows Portable Executables, PDFs, and Microsoft Office documents, using predictive models that can accurate classify files and identify advanced attacks. Cylance does not rely on traditional signatures or hash cloud lookups, making it the industry's leading solution to detect and classify zero-day and unknown malware.
- **Higher Barrier for Attackers** – The predictive learning technology inspects thousands of individual features in each file to classify it as good or bad. This approach is superior to traditional signature-based detection because attackers and malware authors require exponentially greater effort and resources to bypass detection.
- **Improved Operations** – The Content Analysis System with the Cylance INFINITY ENGINE runs locally, so it does not require any behavioral analysis or cloud lookups; the score and threat indicators enable you to significantly reduce the time it takes to detect malware and advanced threats.

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

Copyright © 2016 Symantec Corp. All rights reserved. Symantec, the Symantec Logo, the Checkmark Logo, Blue Coat, and the Blue Coat logo are trademarks or registered trademarks of Symantec Corp. or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners. This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice. v.SB-CAS-WITH-CYLANCE-INFINITY-ENGINE-EN-v1g-0916