[DATE]

Carahsoft's Unsolicited Proposal to
Federal Government for

Palo Alto Networks' WildFire

CARAHSOFT TECHNOLOGY CORP.
1860 MICHAEL FARADAY DRIVE, SUITE 100
RESTON, VIRGINIA 20190

855-6NEXTGN
WWW.CARAHSOFT.COM

Solutions Provided By:

DUNS: 088365767 | CAGE: IP3C5

Proposal Overview

Government endpoints are a critical path to sensitive government data and are central to government operations. Malicious, unauthorized changes and access to these systems can have a significant impact on an agency's operations and, potentially, that of the country. Palo Alto Networks WildFire can protect against today's rapidly changing threat environment in a manner that is minimally disruptive to government operations and meets the productivity needs of the end user.

Introduction

Carahsoft Technology Corp. understands that the federal government could benefit from Palo Alto Networks' WildFire. Carahsoft and Palo Alto Networks are proposing WildFire cloud-based threat analysis service to secure your agency by replacing traditional threat analysis service with a multi-technique approach to ensure cloud protection. Some of key features include:

- Classifying all applications, on all ports, all the time
- Enforcing security policies for any user, at any location
- Preventing known and unknown threats using a unique, multi-technique approach

Palo Alto Networks has extensive experience in providing WildFire to a variety of the federal government agencies.

Objectives

Palo Alto Networks' WildFire goes beyond traditional approaches used to detect unknown threats, bringing together the benefits of independent techniques for high-fidelity and evasion-resistant discovery. By utilizing four different types of analysis, it discovers and prevents unknown malware and exploits with high efficacy and near-zero false positives. For example, WildFire provides users with a closed-loop approach to preventing cyberthreats, ensuring they are known to all and blocked across the attack lifecycle.

Key Problems Solved

This endpoint protection will help Federal Government address the following needs:

- Detects evasive zero-day exploits and malware with a unique combination of dynamic and static analysis, novel machine learning techniques, and an industry first, bare metal analysis environment
- Orchestrates automated prevention for unknown threats in as few as five minutes from any location
- Builds collective immunity for unknown malware and exploits with shared real-time intelligence from approximately 20,000 subscribers
- Provides highly relevant threat analysis and context with AutoFocus Threat Intelligence Service

WildFire Overview for Federal Government

Government initiatives provide citizens with better access to government services and place extra demands on IT and security teams. Additionally, because they provide services essential to modern life, the federal government is a high-value targets for cyber attackers. With Palo Alto Networks WildFire, your agency will meet the privacy and regulatory federal government requirements to secure all data and applications amid budget and staffing concerns.

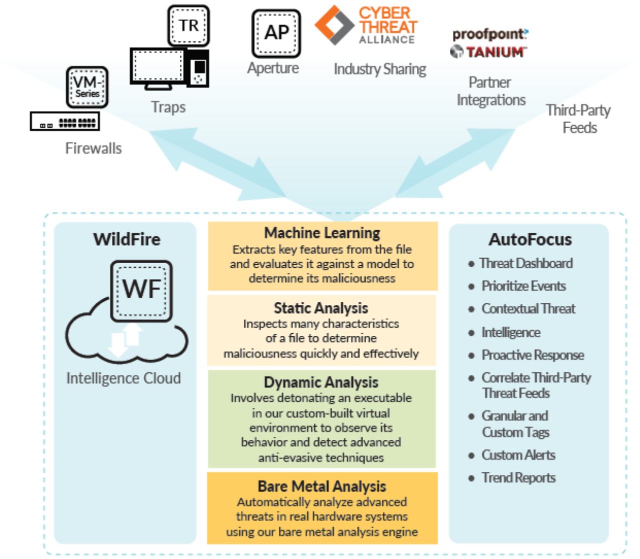
TR
AP
CYBER THREAT ALLIANCE
proofpoint
TANIUM
VM-Series
Traps
Aperture
Industry Sharing
Partner Integrations
Third-Party Feeds
Firewalls
WildFire
WF
Intelligence Cloud
Machine Learning
Extracts key features from the file and evaluates it against a model to determine its maliciousness
Static Analysis
Inspects many characteristics of a file to determine maliciousness quickly and effectively
Dynamic Analysis
Involves detonating an executable in our custom-built virtual environment to observe its behavior and detect advanced anti-evasive techniques
Bare Metal Analysis
Automatically analyze advanced threats in real hardware systems using our bare metal analysis engine
AutoFocus
Threat Dashboard
Prioritize Events
Contextual Threat
Intelligence
Proactive Response
Correlate Third-Party Threat Feeds
Granular and Custom Tags
Custom Alerts
Trend Reports

Figure 1: Evasion-resistant discovery

Within the WildFire environment, threats are detonated, intelligence is extracted, and preventions are automatically orchestrated across the Palo Alto Networks Next-Generation Security Platform within 300 seconds of first discovery anywhere in the world. WildFire goes beyond traditional approaches used to detect unknown threats, bringing together the benefits of four independent techniques for high-fidelity and evasion-resistant discovery, including:

Dynamic Analysis

Observes files as they detonate in a purpose-built, evasion-resistant virtual environment, enabling detection of zero-day malware and exploits using hundreds of behavioral characteristics.

Static Analysis

Highly effective detection of malware and exploits that attempt to evade dynamic analysis, as well as instant identification of variants of existing malware.

Machine Learning

Extracts thousands of unique features from each file, training a predictive, machine-learning model to identify new malware – which is not possible with static or dynamic analysis alone.

Bare Metal Analysis

Evasive threats are automatically sent to a real hardware environment for detonation, entirely removing an adversary's ability to deploy anti-VM analysis techniques

Your agency may start with WildFire but, as you grow your protection level, new elements to the platform can easily be added without the cost and complexity of installing and managing new network devices.

Additional Information

The Federal Government's individual goals are of the utmost importance to Carahsoft and Palo Alto Networks.

Carahsoft and Palo Alto Networks are eager to work with the Federal Government to provide a customized product solution to meet your goals and budget.

The Federal Government have several options for acquiring Palo Alto Networks' Products and Services. The Federal Government can acquire solutions from Carahsoft through GSA and SEWP.

Carahsoft and Palo Alto Networks are interested in working with the Federal Government to provide the best solution to your individual needs. To discuss product and pricing options, please contact the Palo Alto Networks Team at Carahsoft at 855-6NEXTGN / PaloAltoNetworks@Carahsoft.com.