JULY 9, 2018

Palo Alto Networks' Endpoint Protection Toolkit

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

855-6NEXTGN
WWW.CARAHSOFT.COM

Solutions Provided By:

carahsoft

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 Traps Advanced Endpoint Protection can protect against today's swiftly 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 federal agencies could benefit from Palo Alto Networks' Traps Advanced Endpoint Protection. Carahsoft and Palo Alto Networks are proposing Traps Advanced Endpoint Protection to secure your agency by replacing traditional antivirus with a multi-method approach to prevention. 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, including exploits, malware, and spyware

Palo Alto Networks has extensive experience in providing Traps Advanced Endpoint Protection to a variety of federal agencies.

OBJECTIVES

Palo Alto Networks' Traps Advanced Endpoint Protection is designed to detect known and unknown threats, including in encrypted traffic, using intelligence generated across many thousands of customer deployments. That means they reduce risks and prevent a broad range of attacks. For example, Traps enables users to automatically block increasingly sophisticated threats, while minimizing security management overhead to keep sensitive data protected.

KEY PROBLEMS SOLVED

This endpoint protection will help agencies address the following needs:

- Keeping up with the rapid growth of ransomware and other cyberthreats in a resource- and budget-constrained environment
- Protecting critical infrastructure and maintain 24/7 availability
- Efficiently manage network and endpoint security for different agencies with diverse security needs
- Preventing data breaches and the loss of sensitive information, such as financial transactions and personal data

Endpoint Protection Overview for Federal Government

Cyberattacks are attacks performed on networks or endpoints in order to inflict damage, steal information, or achieve other goals that involve taking control of computer systems that belong to others. Cyberattacks are perpetrated either by causing a user to unintentionally run a malicious executable, or by exploiting a weakness in a legitimate executable in order to run malicious code "behind the scenes" without the knowledge of the user.

Despite a plethora of endpoint security products on the market purporting to solve this problem, nevertheless, cyber breaches continue to increase in frequency, variety and sophistication. Faced with the rapidly changing threat landscape, current endpoint security solutions and antivirus can no longer prevent security breaches on the endpoint. Palo Alto Networks® Traps™ advanced endpoint protection replaces traditional antivirus with a unique combination of the most effective, purpose-built, malware and exploit prevention methods that pre-emptively block known and unknown threats from compromising a system.

EFFECTIVELY SECURING ENDPOINTS USING TRAPS

Signature-based legacy AV doesn't work well enough anymore making it more prone to advanced malware attacks. Palo Alto Networks helps government organizations deploy Traps into environments of all sizes, and completely stop advanced malware like ransomware. Both known and unknown threats are blocked by utilizing a proprietary combination of malware and exploit prevention methods providing longer runway for windows patching cycles.

PROVIDING SPECIALIZED DEVICE PROTECTION

The biggest challenge with protecting specialized devices (which are highly vulnerable to cyberattacks) is that you usually can't install anything onto them without approval from the vendor. So the most effective way to protect them is to isolate them from the rest of the network in a zone behind a NGFW, and use the built-in threat prevention capabilities for added protection against cyber attacks.

Figure 1: Government attack showing each stage of the cyberattack lifecycle used by the attacker

These elements that Traps provide work together at network speed to automatically prevent quickly changing cyber risks from impacting people, endpoints, or data. This approach eliminates silos of information and reduces manual intervention from overburdened IT teams. Unified policy control, visibility and reporting across security functions greatly simplifies management and compliance and reduces the potential for misconfigurations, outdated policies or overlooked threats.

Cost and Additional Information

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

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

There are several options for acquiring Palo Alto Networks' Products and Services. Agencies can acquire solutions from Carahsoft through GSA or SEWP.

Carahsoft and Palo Alto Networks are interested in working with your agency 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.