

Trend Micro

REAL-TIME DEFENSE AGAINST MODERN CYBER THREATS:

Federal Agencies, Trend Micro, and Continuous Monitoring

INTRODUCTION

Today's cyber threats are highly sophisticated, and in many cases are crafted with very specific targets in mind. Designed to bypass specific defenses, and to penetrate specific networks, these targeted attacks (also known as Advanced Persistent Threats, or APTs) cannot be detected by traditional perimeter network defenses.

When private-sector networks come under assault by these new threats, the results can be costly and disruptive. But when federal government networks are the targets—along with the confidential or secret data they contain—the potential damage to US national interests is incalculable.

A NEW APPROACH: CONTINUOUS DIAGNOSTICS AND MONITORING

To counter these threats, the Department of Homeland Security (DHS) has launched the Continuous Diagnostics and Monitoring (CDM) initiative, providing funds to support federal agencies in implementing Continuous Monitoring as a Service (CMaaS).

CMaaS solutions can provide real-time defense in depth against advanced targeted attacks through the continuous gathering, monitoring, analysis, and correlation of enterprise security metrics. Success depends on meeting four key requirements:

- **Correlated Threat Intelligence.** To identify and respond to "zero hour" attacks, it is crucial to be able to instantly correlate data against real-time, global threat information.
- **Deep Packet Inspection and Host Intrusion Prevention System.** Analyzing all network traffic in real time without impacting performance is especially challenging in virtualized environments.
- **File Integrity Monitoring.** Instantly identifying unauthorized changes to system and application files—again, without performance impacts—is crucial to minimizing damage from targeted attacks.
- **Log Inspection.** The sheer volume of logs generated by a tidal wave of threats is a key challenge for IT admins. CMaaS solutions must streamline and automate this process effectively.

TREND MICRO SOLUTIONS FOR CMAAS SUCCESS

Trend Micro Cloud and Data Center Security solutions deliver capabilities that make them uniquely valuable in deploying CMaaS successfully.

- **Smart Protection Network.** Trend Micro gathers and analyzes more than 7TB of global threat data daily, to quickly correlate attack profiles and components and immediately protect customers against zero-hour attacks.
- **Agentless Architecture and Virtual Patching.** Agentless security inspects all traffic in virtual environments without impacting performance. Virtual patching shields vulnerabilities instantly, to keep critical systems safe and operable while awaiting patches.
- **Hypervisor-Level File Integrity Monitoring.** Automatically monitors all critical operating-system and application files. In virtual environments, it does this at the hypervisor level, to prevent the performance impacts that VM-level monitoring can create.
- **Unified Log Inspection.** Automatically unifies the collection and inspection of logs, protection against discovered threats, and remediation in a single, streamlined process, making it easy for administrators to get real-time visibility and actionable intelligence.

CHOOSING THE RIGHT CMAAS PROVIDER

In partnership with the General Services Administration, DHS has awarded a Blanket Purchase Agreement (BPA) to seventeen Systems Integrators (SIs). Federal agencies wishing to make use of DHS funds must purchase CMaaS solutions from one of the selected SIs.

Any one of the SIs named in the BPA will be able to provision customers with Trend Micro products as part of a complete CMaaS solution, either through an existing relationship with Trend Micro or through our distributors. Thanks to Trend Micro's commitment to open and scalable architecture, transparent APIs, and web services framework, agencies and integrators alike will find it uniquely easy to build highly effective CMaaS solutions on the core security platform provided by Trend Micro.

Take the Next Step

- To learn more about CDM, CMaaS, and Trend Micro solutions for federal agencies, visit www.trendmicro.com/CMaaS
- To speak with a Trend Micro Federal Sales Specialist, please call 1-855-66-TREND



Securing Your Journey to the Cloud

©2013 by Trend Micro Incorporated. All rights reserved. Trend Micro, and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice. [SB01_CMaaS_CyberThreats_131202US]