

Trend Micro

THE CUSTOM DEFENSE

Detect, Analyze, and Respond to Targeted Attacks

The targeted attacks and advanced threats that are increasingly used to breach enterprise networks are purpose-built to evade traditional defenses. Enterprises require an advanced approach to protection that identifies these attacks and enables organizations to prevent breaches and their costly consequences.

The **Trend Micro™ Custom Defense™** is a series of solutions that are designed to help organizations prevent the collateral damage associated with targeted attacks and advanced threats. These consequences frequently include:

- **Unexpected Costs**—While few data breaches reach the estimated US\$1B total cost of 2013's most damaging targeted attack, the US\$5.9M average cost per attack (Ponemon Institute LLC, May 2014) is not an acceptable "cost of doing business"—it's a major, unplanned liability
- **Strategic Impacts**—When organizations suffer data losses, they must turn their focus away from growth and expansion to control damage, repair reputations, and reclaim competitive position
- **Unexpected Risk**—From potential fines for non-compliance to litigation launched by damaged customers, partners, and others, the risks associated with a successful attack can be significant
- **Career Impacts**—Following the disclosure of a major breach, enterprises sometimes find that the first step in rebuilding trust is to accept the resignations of high-level executives—up to and including the CEO

To prevent these potential consequences, Custom Defense solutions enable organizations to **detect, analyze, and respond** to targeted attacks and advanced threats, before high-value data and intellectual property is stolen.



KEY BENEFITS

Proven Threat Detection—Detects suspicious activity, command-and-control communications, and lateral movement on inbound, outbound, and internal network communication

Advanced Malware Analysis—Executes suspicious files in virtual sandbox environments that are customized to precisely match your desktop images

A Unified Defense—The ability to share threat insight across your security infrastructure to prevent malicious communication, websites, applications, malware, and other targeted attack behavior from compromising the network further

Prompt Response—Correlation of local and global threat insight to enable rapid remediation of compromised network assets and devices

FLEXIBILITY TO ADDRESS THE CHALLENGES THAT MATTER TO YOUR ORGANIZATION

Detect and Respond to Targeted Attacks

For organizations that need to protect data, intellectual property, and communications by identifying suspicious inbound, outbound, and internal network activity and advanced malware associated with targeted attacks, the Trend Micro Deep Discovery Inspector is a single-appliance solution that monitors more than eighty applications and protocols and every network port for attacker and other suspect activity on your network.

Stop Targeted Email Attacks

Because targeted attacks are most commonly initiated using a targeted “spear-phishing” email attack, organizations can now deploy a purpose-built solution that addresses the critical need to detect and block these emails. Working with your existing secure email gateway, the Trend Micro Deep Discovery Email Inspector uses advanced heuristics, reputation, and custom sandboxing to analyze suspicious attachments and embedded URLs, providing single-appliance protection that blocks attacks before they can begin.

Enhance Protection Against Targeted Attacks

Enterprise organizations with an existing investment in Trend Micro security solutions can increase the value of these products with the addition of custom sandbox analysis to detect advanced malware. The Trend Micro Deep Discovery Analyzer is a single appliance that integrates seamlessly with a wide range of email and web security solutions, to extend advanced-threat detection capabilities across your entire security infrastructure.

Contact Trend Micro or your preferred reseller to learn more about the Trend Micro Custom Defense and how to enhance your security with capabilities to detect, analyze, and respond to advanced threats and targeted attacks.

Trend Micro Deep Discovery

The Deep Discovery threat protection platform is at the heart of the Custom Defense, providing advanced, integrated capabilities in a variety of configurations to address each organization's specific needs.

Deep Discovery Inspector

360-degree monitoring of network traffic, with advanced threat detection

Deep Discovery Email Inspector

Detects and blocks spear-phishing emails by analyzing email contents, attachments, and embedded URLs

Deep Discovery Endpoint Sensor

Validates compromised endpoint devices and enables swift remediation

Deep Discovery Analyzer

Extends the value of existing security infrastructure by integrating detection of advanced threats



Securing Your Journey to the Cloud

©2014 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_CustomDefense_140714US]