



## Joint Solution Brief

# Protect Against Targeted Attacks, APTs and Ransomware with Trend Micro Deep Discovery and GigaSECURE

### The Challenge

Today's networks are faced with superior and advanced malware and a new breed of target attacks and advanced persistent threats that can evade standard security solutions. It is not enough to simply put up a firewall or intrusion prevention system and/or deploy an anti-virus solution to protect intellectual property.

### Integrated Solution

With the combination of the Trend Micro Deep Discovery and the Gigamon GigaSECURE® Security Delivery Platform, traffic is analyzed and threats are detected immediately, allowing administrators to discover and respond to malware, command and control (C&C) communications, and attacker network activity before real damage can be done.

### Joint Solution Benefits

- Broad and deep visibility across physical, virtual, and cloud network traffic flows augments Trend Micro Deep Discovery's ability to detect and respond to advanced threats in real time
- The GigaSECURE platform's automatic traffic load distribution and aggregation functionality optimizes traffic for Trend Micro Deep Discovery
- The GigaSECURE platform de-duplicates and filters traffic gathered from multiple collection points and distributes traffic to Trend Micro Deep Discovery to accelerate breach detection and response
- With the GigaSECURE platform's real-time SSL decryption functionality, Trend Micro Deep Discovery gets increased visibility into traffic flows without performance degradation

### Introduction

Today's networks are faced with superior and advanced malware and a new breed of target attacks and advanced persistent threats that can evade standard security solutions. It is not enough to simply put up a firewall or intrusion prevention system and/or deploy an anti-virus solution to protect intellectual property. A robust solution includes comprehensive visibility into every area of the network and all traffic to protect valuable assets, keep attackers away, and ensure security tools are used to their full advantage.

The key to finding them—and finding them much faster—is pervasive visibility across physical, virtual, and cloud environments.

Together with Trend Micro Deep Discovery, the Gigamon GigaSECURE Security Delivery Platform provides the visibility necessary to detect, analyze, and respond to today's stealthy, targeted attacks.

### The Gigamon and Trend Micro Joint Solution

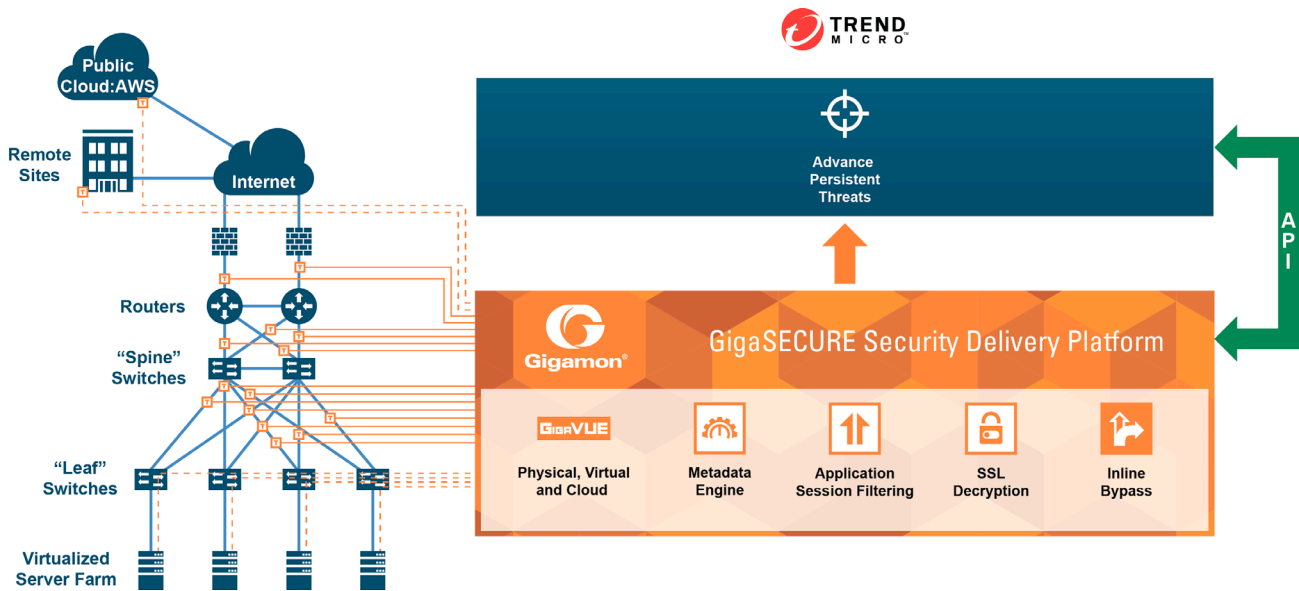
Trend Micro and Gigamon have partnered to create a complete solution that provides real-time threat protection against targeted attacks without hindering performance, reliability, or availability. With the combination of the Trend Micro Deep Discovery and the Gigamon GigaSECURE Security Delivery Platform, traffic is analyzed and threats are detected immediately, allowing administrators to discover and respond to malware, command and control (C&C) communications, and attacker network activity before real damage can be done.

Trend Micro Deep Discovery is an advanced threat protection platform that enables businesses to detect, analyze, and respond to today's stealthy, targeted attacks. Using specialized detection engines, custom sandboxing, and global threat intelligence from the Trend Micro Smart Protection Network, Deep Discovery defends against attacks that are invisible to standard security products. Deployed individually or as an integrated solution, Deep Discovery solutions for network, email, endpoint, and integrated protection provide advanced threat protection where it matters most to an organization.

### Deep Discovery Platform Key Features

**Advanced Threat Detection:** Identifies attacks anywhere on the network using specialized detection engines, correlation rules, and custom sandboxing.

**Custom Sandboxing:** Uses virtual environments that precisely match system configurations to detect the threats that target the organization.



**Smart Protection Network intelligence:** Leverages real-time, cloud-based security intelligence for threat detection and in-depth attack investigation.

**Part of a Connected Threat Defense:** Shares IOC detection intelligence with other Trend Micro and third-party security products to stop further attacks.

### Key GigaSECURE Security Delivery Platform Features that Augment the Value of Trend Micro Deep Discovery Include:

**Easy access to traffic from physical, virtual and cloud networks:**

The GigaSECURE platform manages and delivers all network traffic—in the format required—to Trend Micro Deep Discovery. To monitor east-west data center traffic, and public cloud workloads, Gigamon taps virtual traffic and accesses and incorporates it into GigaSECURE for delivery to Trend Micro Deep Discovery, so that traffic is analyzed and threats are detected immediately.

**Filtering traffic to only send relevant traffic:** The GigaSECURE platform can be configured to send only relevant traffic or sessions to Trend Micro Deep Discovery so that it only analyzes traffic that provides security value.

**Aggregation to minimize tool port use:** Where links have low traffic volumes, GigaSECURE can aggregate these together before sending them to Trend Micro Deep Discovery to minimize the number of ports needed. By tagging the traffic, the GigaSECURE platform ensures that the source of the tagged traffic can be identified.

**De-duplication:** Pervasive visibility requires tapping or copying traffic from multiple points in the network, which, in turn, means

tools may see the same packet more than once. To avoid unnecessary packet processing overhead on Trend Micro Deep Discovery, the GigaSECURE platform has a highly effective de-duplication engine that removes duplicates before they consume resources and helps balance monitoring coverage.

**SSL decryption:** Real-time SSL decryption integration increases traffic visibility for Trend Micro Deep Discovery, broadening its scope for analysis and inspection of malicious activity.

**Manage Asymmetric Routing:** Most security devices, including those from Trend Micro, require inspection of all the packets in a session to be inspected by the same device. GigaSECURE provides an intelligent and efficient way to make this happen.

**Bypass Protection:** Deploy Trend Micro devices in virtual wire mode and use the GigaSECURE functionality to provide physical bypass traffic protection in the event of power loss and logical bypass traffic protection in the event of an inline tool failure.

**Agile Deployment:** Add, remove, and/or upgrade Trend Micro devices without disrupting network traffic; convert tools from out-of-band monitoring to inline inspection on the fly without rewiring.

### Learn More

For more information on Trend Micro and Gigamon solutions, contact:

