A Trend Micro White Paper | **June 2015**

Inside the Wire: Why Perimeter-centric Monitoring Leaves You Vulnerable

» Comprehensive, 360-degree detection is critical for stopping advanced targeted attacks

Contents

Introduction

As the news carries a steady drumbeat of revelations of significant data breaches perpetrated against major retailers, healthcare organizations, financial services, government institutions, and many others, it's clear that perimeter-centric and other traditional security defenses have been rendered ineffective by the advanced means and methods used by today's attackers.

There is nothing random or "lucky" about these breaches. When attackers come after your network (and they will—if they haven't already), they will carefully plan and execute their attacks, using techniques and attack code that is custom designed and built to evade the specific defenses that stand between them and your valuable data. And once the perpetrators succeed in bypassing your defenses, they will take up residence inside your network. If your security is focused solely on "north-south" traffic—data traveling across the network perimeter—the attack can go undetected for months.

To effectively detect these attacks you must gain visibility into attack behavior and lateral movements within your network—"east-west" activity—and not just monitor traffic into and out of the network.

Trend Micro™ Deep Discovery Inspector™ has the capabilities to deliver 360-degree detection of targeted attacks across your entire network. This capability enables the detection of lateral movement and other intra-network attack behaviors on over 100 protocols and all network ports. As a result, you gain comprehensive visibility into your network, enabling you to detect malicious activity before it can approach your valuable data.

Targeted Attacks: Why They're Different

Today's targeted attacks may be launched by a variety of actors with a variety of specific goals in mind. Your attackers might be an international criminal gang, a state or corporate spy agency, a hacktivist group, an unscrupulous competitor, or even disgruntled former employees. Their goals may be financial profit, economic advantage, competitive business advantage, making a statement, harming your organization's brand, manipulating your stock price, or attempting to harm your business financially. They may want to steal confidential customer data, valuable intellectual property, strategic business plans, partner information, and more. Or they may intend to use your network as a launch pad for an attack against a customer, supplier, or other ecosystem partner.

Despite this variety, all these attacks have two things in common:

1. They are carefully designed to penetrate your network and your perimeter defenses. Based on advanced reconnaissance and pre-attack testing, they may choose to directly exploit your employees, or first penetrate a partner's network and then "island-hop" into your network using what appear to be trusted credentials and access, or use some other tactic to outflank and evade your perimeter defenses. Attackers often devote many weeks to researching, designing, building, and testing their attack methods to ensure they can evade your security.

2. Once inside, they move east-west, or laterally within your network in search of critical data and systems using standard application protocols. These movements are invisible to perimeter-centric security—which, by definition, is focused only on north-south traffic, and is intended only to detect incoming attacks.

As attacks grow more sophisticated, ever more of their north-south communications outside the network—for example to a command-and-control (C&C) server—can be obfuscated using IP address checks, non-standard protocols, and other methods to thwart detection.

Factors ensuring continued growth of targeted attacks

- **LOW BARRIERS TO ENTRY**
  The skills, services, support, and resources needed to execute a targeted attack are inexpensive, and easily accessible through online markets and notice boards—from advanced malware to live, 24/7 tech support.

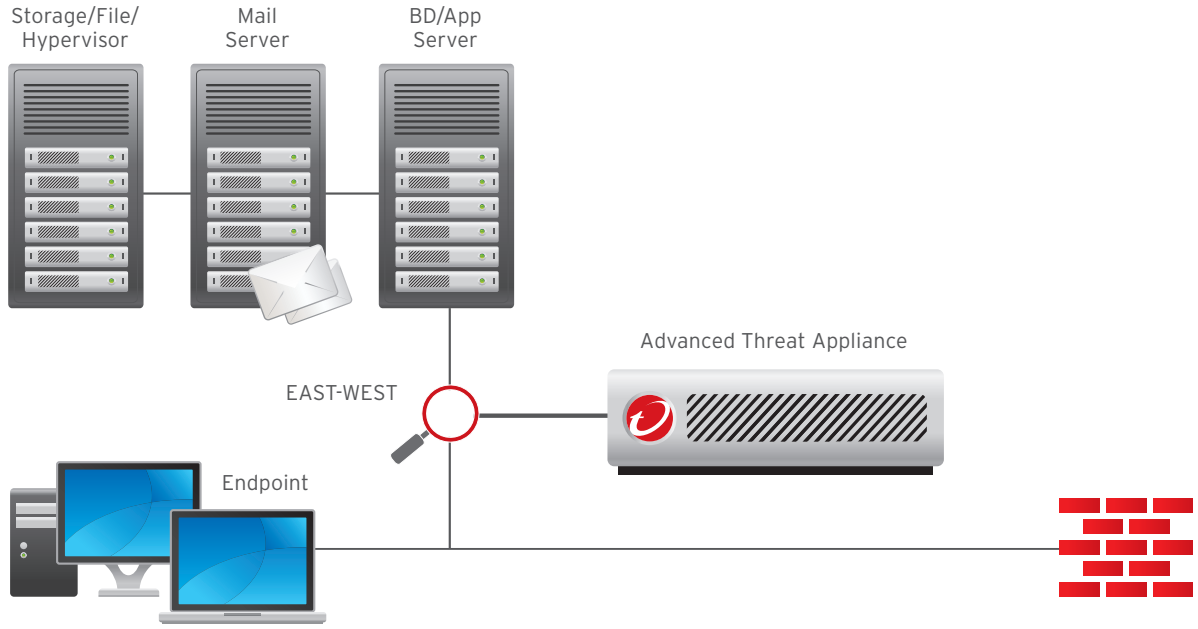
- **LOW PENALTIES FOR FAILURE**
  Arrest and prosecution is vanishingly rare. And each failure is an inexpensive lesson for attackers to apply to their next attempt, fine-tuning attack methods, payloads, and tactics to obtain what they seek. Further, the attack chain is often widely distributed, with third parties providing services, products, and support for attack research, hardware, pre-packaged code, testing, C&C infrastructure, and attack execution. The loosely coupled structure of these attacks reduces the risk of detection for all parties.

- HIGHLY INTERCONNECTED NETWORKS
  By connecting networks around the globe in multiple ways, the modern Internet has delivered vast improvements in efficiency—but it has also created a world of opportunities for cyber-miscreants to hop from one system to another with relative ease.

Detecting Attackers' Lateral Movement Within the Network

The growing number of successful data breaches provides clear evidence that perimeter defenses can be evaded by today's targeted attacks.

However, the initial penetration of the network almost never gives attackers direct access to the assets they are seeking. Instead, having established a beachhead within a particular system—a single desktop PC, mobile device, or other network-connected system—the attackers must move east-west within the network, expanding the scope of compromise in order to harvest credentials, escalate privilege levels, and find valuable data.



The attacker's need for lateral movement within the network presents an opportunity for detection of a targeted attack. Once the attacker has infiltrated your network, the attack will begin to move laterally within the network. This traffic uses server, application, and access protocols to find and communicate with critical assets and data servers. As the attack progresses, this traffic can be a form of breadcrumb and clue for those who know what to look for. And these traces of lateral movement can be the Achilles' heel of a targeted attack, providing a way to detect and respond before serious damage can be done. Two important caveats apply:

- Any targeted attack solution must be looking for attackers' lateral movement in order to detect it; and that is something that perimeter-centric defenses can't do, since lateral traffic doesn't cross the perimeter.
- This lateral traffic often uses techniques to avoid detection. In some cases it may mimic normal, legitimate traffic. In others, it may use unusual ports and protocols, taking advantage of the fact that many scanning engines monitor only common protocols such as http or smtp.

All of this points to several critical requirements for a solution that provides the necessary visibility to detect and respond to targeted attacks within your network:

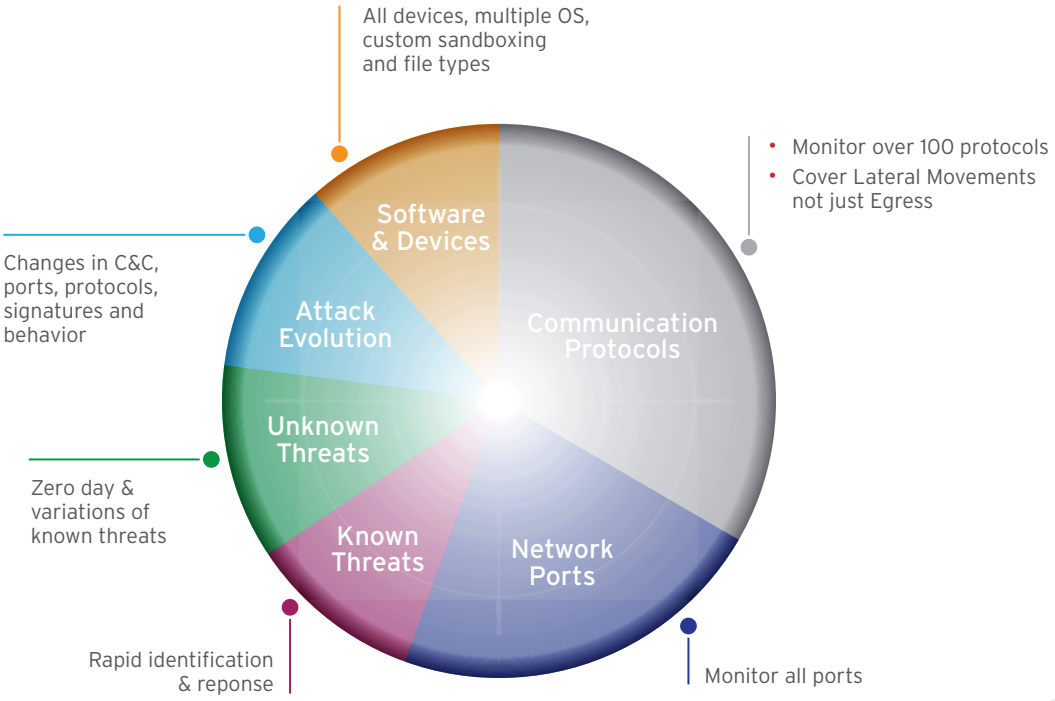
1. It must be capable of monitoring not only traffic into and out of your network, but also all internal network traffic between endpoints, servers, and any other devices that are inside your network perimeter.
2. It must be agnostic regarding ports and protocols; that is, it must examine all traffic within your network or crossing its perimeter—not just the traffic that uses common web, email, and file protocols. Your attackers do not limit themselves to http and smtp traffic, or use only ports 80 or 110. Your security must not be limited either.
3. It must employ sophisticated analytic and heuristic techniques to identify attacker behavior.
4. All of the above must be readily correlated across the entire attack sequence in order to provide clear visibility into all phases of a targeted attack.

Only a solution capable of meeting all of these requirements—capable, that is, of 360-degree detection across your entire network—can effectively detect advanced threats and targeted attacks before a breach can occur. And only a solution that provides 360-degree detection can effectively prevent the strategic, financial, and career consequences that typically result from a successful data breach.

Security vendors who suggest that a myopic, perimeter-centric defense alone can protect organizations from targeted attacks may be doing a disservice to their customers—giving them a false sense of security that actually makes them more vulnerable.

Trend Micro 360-Degree Detection

Trend Micro Deep Discovery Inspector uses comprehensive, 360-degree detection to identify targeted attacks at all stages of an attack and across your entire network, including intra-network traffic. This approach sets Deep Discovery Inspector clearly apart from other solutions on the market that have a myopic and/or perimeter-centric approach to detecting attacks.



DEEP DISCOVERY MONITORS TRAFFIC INTO, OUT OF, AND WITHIN YOUR NETWORK

Other solutions focus exclusively on defending your network perimeter. This means that when a targeted attack evades that perimeter defense—as it is carefully designed to do—often there are limited means to detect malicious behavior within the network. Attackers have the freedom to move laterally from one system to another with no fear of detection. Because no alert is raised by the perimeter defense, your IT personnel may have no clue that anything is amiss until after significant damage is done.

DEEP DISCOVERY MONITORS NETWORK TRAFFIC ACROSS ALL NETWORK PORTS, AND MORE THAN 100 DIFFERENT PROTOCOLS AND APPLICATIONS

Other solutions typically limit themselves to scanning only http and smtp traffic—which is why many attackers use unmonitored or uncommon communication methods for their lateral movements within target networks. Critically, other solutions do not scan traffic into and out of data centers and servers, which uses specialized protocols exclusive to intra-network traffic such as SQL or SMB. But this is precisely where most of your confidential data, intellectual property, financial data, and other valuable information is stored—the very information that attackers want to steal and profit from. Deep Discovery analyzes this traffic in order to detect attempts to identify, access, copy, and exfiltrate these valuable assets.

DEEP DISCOVERY USES MULTI-LAYERED ANALYSIS TO OPTIMIZE DETECTION

Other solutions rely exclusively on sandboxing, or signature matching, or limited heuristic analysis for detection. Deep Discovery combines multiple, specialized detection engines; unique correlation rules and heuristics; and custom sandbox analysis that matches your specific system profiles to detect all aspects of a targeted attack. In addition, like all Trend Micro products, Deep Discovery correlates its findings with the Smart Protection Network, Trend Micro's global, real-time threat intelligence system. Smart Protection Network not only optimizes detection rates—it also uses big-data analysis to provide critical context and insight to an attack. This can be invaluable in helping to you to respond rapidly and effectively.

THE BOTTOM LINE

Where other solutions leave significant gaps in detection of targeted attacks, Deep Discovery delivers truly comprehensive detection efficacy across the entire network. That's the whole idea behind 360-degree detection, and it's part of the reason that NSS Labs gave Deep Discovery Inspector the highest security effectiveness score in its 2014 Breach Detection Tests.

Detect Targeted Attacks Within Your Network

Targeted attacks will continue to increase in frequency and sophistication, and organizations of all types and sizes face the prospect of damaging data breaches. A truly effective security posture must fulfill the requirements outlined above—and the sooner you adopt a solution that meets those requirements, the sooner you will be able to assert with confidence that your critical and confidential data is secured against today's most dangerous attacks.

Once these requirements are integrated into your risk management strategy for targeted attacks, you will be able to provide security and business leaders with the visibility they need to make optimal decisions about how to allocate resources effectively to minimize the risk of strategic impacts, unexpected costs, and career consequences.

To learn first-hand how Deep Discovery Inspector and 360-degree detection performs in your environment, please contact Trend Micro today to discuss how we can help you detect, analyze, and respond to targeted attacks.

Further Reading and Resources

Learn more about Deep Discovery Inspector:
Deep Discovery: Advanced Network Security

Keep up with the latest information about targeted attacks and how to thwart them:
Security Intelligence—Targeted Attack News and Updates

Discover live and on-demand webinars to deepen your understanding of the threat landscape:
Trend Micro Enterprise Webinar Series

Learn how Deep Discovery Inspector came out on top in recent testing by NSS Labs:
NSS Labs 2014 Breach Detection Test Comparison Report

Trend Micro Incorporated is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our Web site at www.trendmicro.com.

TREND MICRO INC.
U.S. toll free: +1 800.228.5651
phone: +1 408.257.1500
fax: +1 408.257.2003