Trend Micro™ Deep Discovery 针对性攻击检测、深度分析及快速响应

非官方中文译本 · 安天技术公益翻译组 译注

文档信息			
原文名称	Trend Micro™ Deep Discovery Targeted Attack Detection, in-depth Analysis, and Rapid Response		
原文作者	趋势科技	**原文发布日期**	
作者简介	趋势科技是一家安全软件公司，其安全产品包括 Trend Micro Internet Security, Trend Micro Worry-Free Business Security, OfficeScan 等。http://en.wikipedia.org/wiki/Trend_Micro		
原文发布单位	趋势科技		
原文出处			
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者		

	和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。

Trend Micro™

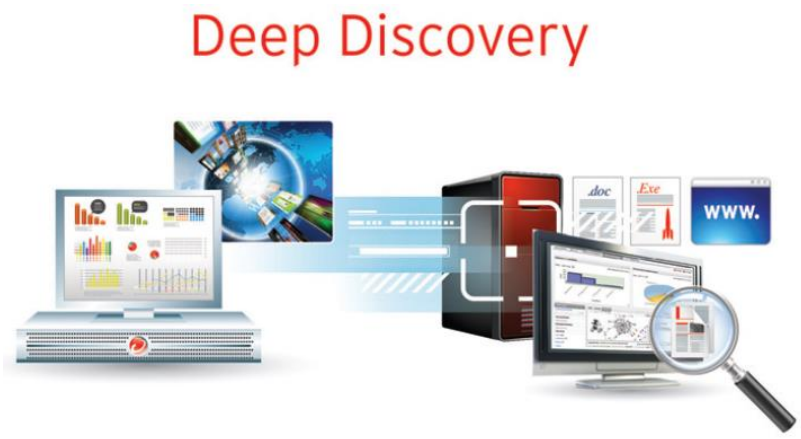
Deep Discovery

针对性攻击检测、深度分析以及快速响应

高级持续威胁（APT）和针对性攻击已经明晰的表明，他们能够逃避传统的安全防御，长时间隐蔽而不被发觉，窃取企业数据和研究成果。分析师和专家认识到了这些问题，并建议企业将安全重新定义为尽职的使用专用威胁检测技术和一个主动的实时威胁管理过程。

Trend Micro™ Deep Discovery 3.2 为您提供抗击 APT 和针对性攻击所需的全网可见性、洞察力和可控性。Deep Discovery 独一无二的实时检测和辨识隐藏的威胁，提供深度分析和相关行为情报，这些能够协助您评估、补救和抵御发生在您的企业中的针对性攻击。

Deep Discovery 是 Trend Micro Custom Defense 的核心。它是一个完整的解决方案，使您能够对贵企业遭受的针对性攻击进行检测、分析、调整和响应。Deep Discovery 拥有专用的检测引擎和自定义沙箱仿真环境，能够辨识零日恶意软件，恶意通信和对标准安全防御来说不可意见的攻击行为。基于相关威胁情报和全网安全事件的可见性，进行深度分析，遏制和修复，进而通过安全更新输出使其能够抵御更进一步的攻击。



Deep Discovery 解决方案由两个组件组成。Deep Discovery Inspector 提供网络威胁检测、自定沙箱、实时分析和报告生成。可选组件，Deep Discovery Advisor 组件提供开放的、可扩展的沙箱分析，全网范围内安全事件的可视性和安全更新输出。所有功能位于一个统一的智能平台。

检测和防御

- APTs 和针对性攻击
- 零日恶意软件和文件漏洞
- 攻击者网络行为
- Web 威胁（漏洞,自动下载）
- Email 威胁（钓鱼，鱼叉式网络钓鱼）
- 数据泄露
- 僵尸、木马、蠕虫、键盘记录器
- 破坏性应用

主要优势

APT & 针对性攻击检测
减少 APTs 导致的破坏和数据丢失的风险

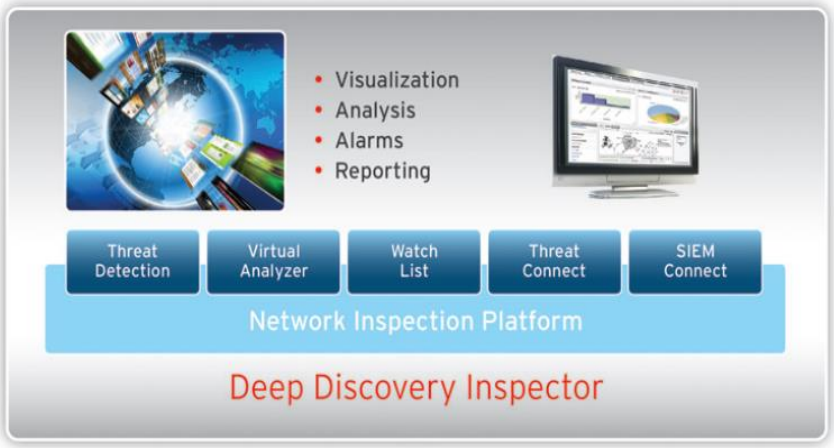
全网可视
揭示和追踪你真正的安全状态

深度场景分析和洞察
充分表征威胁和风险因素

快速遏制和响应
利用可操作性情报和安全更新输出快速修复

自定义防御的基石
通过自定义沙箱仿真、情报和更新来抗击那些对您来说很重要的威胁。

Deep Discovery Inspector



Deep Discovery Inspector 提供网络流量检测，高级威胁检测，实时分析和报告生成—专为检测 APT 攻击和针对形攻击。它采用一个三层的检测架构来实施初始的检测，然后进行沙箱模拟仿真和相关分析，最终形成交叉关联，进而揭示那些通过长时间观察才能辨识的“低调和缓慢“的行为和其它隐蔽的攻击者行为 。

在 Trend Micro™ Smart Protection Network™的全球威胁情报系统以及专有的威胁研究人员的协助下，专用的检测和相关性引擎为用户提供最精确和最新的保护。它拥有较高的捡出率和较低的误报率，并提供深度事故分析报告以加快遏制攻击的速度。

主要特点

高级威胁检测

Deep Discovery Inspector 使用非入侵的，listen-only 的方式检查所有类型的网络流量，重点识别恶意内容、通信和贯穿攻击序列每个阶段的高级恶意软件或攻击者的行为。

- 专用威胁检测引擎和多层次关联规则提供最好的检测和最低的误报。
- 虚拟分析器使用自定义沙箱仿真环境来提供额外的检测和对可疑内容的完整的取证分析.
- Smart Protection Network 情报系统和专有威胁研究人员提供不断更新的检测情报和相关规则，用以辨识攻击。

威胁追踪、分析和处置

Deep Discovery Inspector 控制台提供实时的威胁可视化展示和直观的深度分析，使安全从业人员能够专注于真正的风险，进行取证分析和快速的解决问题。

实时威胁控制台

使威胁的可视性和深度分析触手可及。

- 快速访问工具使关键信息一部了然。
- 攻击特征、行为和通信的深度分析。
- GeoTrack 辨识恶意通信源头。

关注项列表

针对严重的威胁和高沽值的资产提供基于风险的监控

- 重点追踪特定主机上的可疑行为和事件。
- 通过威胁检测和自定意选项选定被追踪主机
- 通过详细的事件时间表追踪所有涉及目标主机的攻击活动。

威胁相关情报

为您提供了解和补救一个攻击所需的威胁情报

- 直接访问 Trend Micro 情报门户获取特定攻击或恶意软件信息 。
- 详尽的威胁特征，遏制和补救建议。
- 针对这一威胁的病毒 (或其他) 检测特征的更新的方法。

SIEM 管理

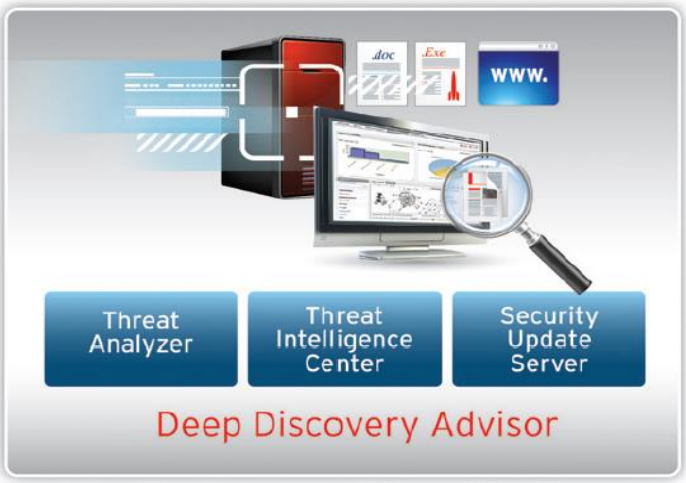
与先进的 SIEM 平台整合，通过单一的 SIEM 控制台提供增强的企业级威胁管理。

- 将网络检测结果，已辨识出的事件和相关数据提交给 SIEM。
- 深度网络可视化增强了 SIEM 的相关性和多维攻击剖析。
- SIEM 提供的企业级威胁管理作为中心控制台。

灵活，高容量部署

Deep Discovery Inspector 拥有高性能架构，可以满足各种规模用户的要求和多样化的容量需求。产品可用于全系列的硬件、软件和那些支持千兆骨干企业网下远程办公的虚拟应用。

Deep Discovery Advisor



Deep Discovery Advisor 提供开放的、可扩展的定制化沙箱分析，全网安全事件可视化展示，安全更新输出—所有功能位于一个统一智能平台

Advisor 增强了 Deep Discovery Inspector 的分析能力，使其具有自定义防御的自适应防护和快速响应的能力。

主要特点

威胁分析器

威胁分析器是可选组件，提供对潜在恶意样本文件（包括可执行文件的和常用办公文档）的深度拟和分析。它能增强和集中 Deep Discovery Inspector 的模拟仿真，通过 Web 服务接口为专业人士和其他安全产品或服务提供高级检测和安全分析。

- 深度威胁模拟和分析。使用沙箱模拟环境和其他高级检测引擎来对提交的文件进行分类和深入分析。
- 自定义沙箱执行环境允许用户创建和分析多个完全自定义的，能够精确匹配他们的主机环境的标靶。
- 可扩展架构，支持高达 50，000 样本/天的产能增量。
- 开放提交、自动提交和手动提交。支持支持安全分析师的输入，以及 Trend Micro 的产品和第三方定制的产品的自动提交和结果回传。
- 与 Deep Discovery Inspector 和其他 Trend Micro 产品整合，为用户提供扩展检测和分析选项。

威胁情报中心

威胁情报中心是一个完整的分析环境，用于来自威胁分析器的事件数据，以及来自 Deep Discovery Inspector、其他 Trend Micro 产品和第三方解决方案采集的安全事件和日志。通过这些资源和整合的威胁相关的情报，Threat Intelligence Center 提供深入的见解，以推动基于风险的事故评估、遏制和修复。

- 使用自动化分析工具、可视化工具、高级搜索和调查工具，深入分析事故和事件。
- 面向风险的监控和调查。
- 对 Trend Micro 和第三方产品的事件和日志的全网安全事件收集，确保了一个全面的风险评估，以及有效的遏制和补救措施。
- 威胁相关情报被自动整合进分析结果，为遏制和补救提供详细的威胁特征和背景相关情报。
- Deep Discovery Inspector 将来自多个 Deep Discovery Inspector 单元的检测结果集中整合上报至一个单一的显示面板，并形成可定制化的报告。
- SIEM 与先进的平台相关联，通过单一的 SIEM 控制台提供更高级的企业级威胁管理。

安全更新服务器

安全更新服务器提供了导出手段，可以导出那些从威胁分析器的模拟仿真中获取的，有用的安全拦截信息。这些信息包括新发现的恶意 IP/URL 地址和能够被各种安全产品使用的文件哈希。Deep Discovery Inspector 和其他若干 Trend Micro 产品自动接收这些信息。这些信息也能通过 CSF 文件手动导出。

Deep Discovery 工作原理

Deep Discovery 专为检测 APT 和针对性攻击而设计，识别那些可能代表高级恶意软件或贯穿攻击序列每个阶段的攻击者行为的恶意内容、恶意通信和恶意行为。

Deep Discovery 采用三层检测架构实施初始检测，进行定制化模拟仿真和相关性分析，最终通过交叉关联减少误报和揭示藏匿的行为。Trend Micro™ Smart Protection Network™的全球威胁情报系统和专有的威胁研究人员为检测引擎和相关性规则提供支撑。这导致了高的检出率，低的误报率，并提供深度事故分析报告以加快对攻击的遏制速度。

	攻击检测	检测方式
恶意内容	• 包含嵌入式文件漏洞的 Email • 自动下载 • 零日和已知恶意软件	• 解码和解压缩嵌入的文件 • 可疑文件的沙箱模拟 • Browser exploit kit 检测 • 恶意软件扫描(特征和启发式)
可疑通信	• 所有恶意代码（僵尸，下载器，数据窃取，蠕虫和混合威胁）的 Command-and-control 通信 • 攻击者的后门行为	• 基于动态黑名单,白名单的目的地分析 (URL,IP,domain,email,IRC channel 等) • Smart Protection Network™URL 信誉 • 通信指纹规则
攻击行为	• 恶意软件活动:传播,下载,垃圾邮件等 • 攻击者行为:扫描,暴力破解,服务攻击 • 数据泄露，	• 基于规则的启发式分析 • 识别和分析 100 的协议和应用，包括 HTTP 的应用。

风险管理服务

Trend Micro 服务专家通过安装，监控和咨询增加您的安全响应能力和专业知识，以进一步降低您的风险和安全管理成本。

规格

Deep Discovery Inspector

- 型号 1000：1Gbps 硬件设备
- 型号 500: 500 Mbps 硬件设备
- 型号 VM：VMware 软件应用

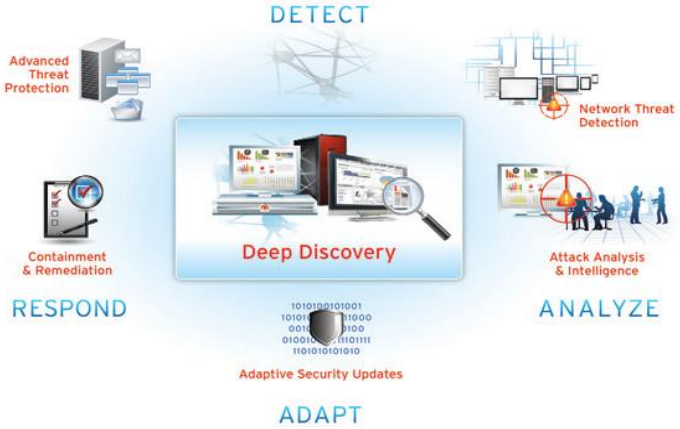
Deep Discovery Advisor 硬件设备

- 集群最高至 5 个单元

通过自定义防御对抗攻击者

Deep Discovery 专有的自定义威胁监测是抵挡针对您企业的攻击的有效防线的核心。Trend Micro 还将 Deep Discovery Advisor 的高级恶意软件检测与其他选定的 Trend Micro 产品整合，以提高对一个攻击的所有的重要初始阶段的防御能力。此外，为了给一个自定义防御提供真正的自适应防护，Deep Discovery Advisor 的深度分析结果可被用于更新 Trend Micro 产品，从而立即增强您抗击进一步攻击的能力。

- 网络级攻击检测和自定义分析
- 拥有定制化恶意软件检测功能的防护解决方案
- 针对自适应防护的定制化安全更新
- 基于全语境分析速度响应的，可操作的情报



TREND MICRO™

Securing Your Journey to the Cloud

[DS01_DD3.2_121002]