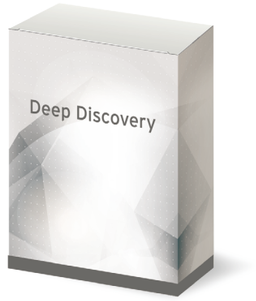
# Deep Discovery

NSS Labs의 APT 탐지 테스트 1위
APT공격 대응 솔루션

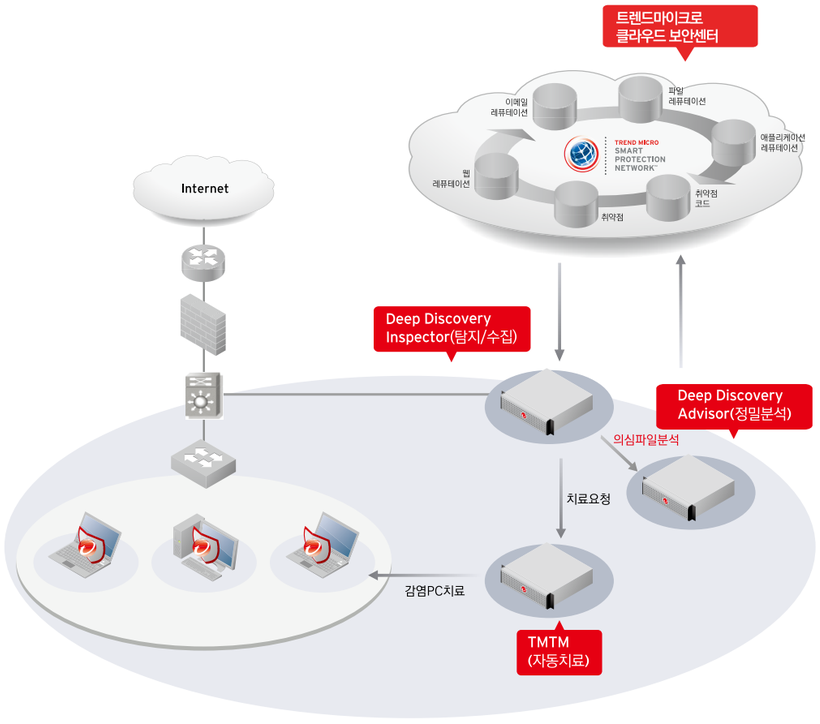
지능형지속위협(APT) 공격의 가장 핵심인 메일기반의 스피어 피싱을 포함해 실시간으로 변경되는 명령제어(C&C)서버와 악성URL에 대한 대응이 가능하며 기존의 백신이나 전통적인 보안솔루션을 우회하는 지능적인 공격에 대응하는 APT보안 솔루션

제조사 : 트렌드마이크로




Deep Discovery

## 구성도




## 제품구성

Deep Discovery는 두가지 컴포넌트. 네트웍 위협 탐지, 샌드박스, 실시간 분석 및 리포팅 기능으로 이루어지는 Deep Discovery Inspector와, 심층 침해 시뮬레이션 및 분석, 침해 연동 정보 수집, 활용 가능한 정보를 위한 보안 업데이트 서버 등 통합된 침해 정보 수집 센터 플랫폼인 Deep Discovery Advisor로 구성됩니다.

Deep discovery Advisor - 정밀 분석

Deep discovery Inspector - 탐지/수집

TMTM - 자동치료

## 주요기능

- Deep Discovery는 APT공격과 특정 타겟 위협 공격을 하는 지능화된 악성코드 또는 공격자의 활동을 모든 단계에서 악성 컨텐츠 식별, 통신 및 행위를 탐지를 하는 목적으로 설계
- 첫 탐지를 실행하고, 시뮬레이션과 분석을 진행하고, 최종적으로 오탐을 줄이고 파악이 어려운 행위를 탐지를 하기 위한 상관관계 분석을 하는 총3단계의 탐지 단계로 구성
- 탐지 엔진과 분석룰은 트렌드마이크로 클라우드 보안센터와 위협 전문가들에 의해서 이루어짐
- 높은 탐지율과 낮은 오탐율, 공격의 상관관계 분석을 위한 심층 침해 기법을 구현

**Deep Discovery의 감지 작동 방법**

- 사용자 정의 위협 탐지에 특화된 Deep Discovery는 기업을 향한 타겟 공격에 효과적인 방어와 대응을 목적
- Deep Discovery Advisor는 기업의 보안을 향상 시킬 수 있도록 지능형 악성코드 공격으로부터 보호 기능을 향상시킬 수 있는 트렌드마이크로의 다른 제품군들과 통합
- 사용자 정의 위협 탐지의 진정한 보호를 제공하기 위해서 Deep Discovery Advisor의 깊이 있는 분석 결과는 즉시 추가 공격 방어를 강화하기 위해 트렌드마이크로 클라우드 센터에 업데이트

| 구분 | 공격감지 | 감지방법 |
|---|---|---|
| 악성 컨텐츠 | • 익스플로잇이 문서 내에 포함된 이메일<br>• 반 자동 다운로드<br>• Zero-day & 알려진 악성 컨텐츠 | • 내장파일의 암호 해독 & 압축 해제<br>• 의심 파일의 제작 샌드박스 시뮬레이션<br>• 브라우저 익스플로잇 킷 감지<br>• 악성 컨텐츠 스캔(서명&휴리스틱) |
| 부정적인 커뮤니케이션 | • 봇, 다운로더, 데이터 절도, 웜, 혼합 등의 모든 악성<br>• 컨텐츠에 대한 C&C 커뮤니케이션<br>• 공격자의 백도어 활동 | • 동적 블랙리스트와 화이트 리스트를 통한 대상 분석 (URL, IP, 도메인, 이메일, IRC 채널, …)<br>• 모든 요청 및 내포된 URL의 Smart Protection Network reputation<br>• 커뮤니케이션 핑거프린팅 규칙 |
| 공격 행동 | • 악성 컨텐츠 활동: 전달, 다운로드, 스팸, …<br>• 공격자의 활동: 스캔, 브루트 포스(억지기법),<br>• 툴 다운로드, …<br>• 데이터 유출 | • 규칙 기반의 휴리스틱 분석<br>• 프로토콜과 HTTP기반의 앱을 포함하는 앱을 100여차례 이상 이용하여 확인 및 분석<br>• 행동 핑거프린팅 규칙 |

## 특장점

**트렌드마이크로의 전문적인 위협 탐지 기술과 능동적인 실시간 위협 관리 체재를 포함**

- 네트워크 전반에 관한 통찰력 및 통제권을 제공하여,APT공격과 타겟형 공격에 노출 될 위험성을 감소시킴
- 침투 위협을 실시간으로 감지하고 파악하여,심층적인 분석과 실질적인 정보를 제공함으로써 기업 데이터에 가해지는 공격을 탐지하고 파악하여 격리
- Deep Discovery의 검증된 접근 방식은 오탐이 적으며, 공격이 시작되는 시점에서 각 단계별로 악성 콘텐츠, 커뮤니케이션, 그리고 행동을 파악하여 최고의 탐지율과 방어율을 보여줌
- 진화된 악성코드와 침투 공격자의 행동에 관한 탐지와 심층 분석을 통하여 진화하는 컴퓨팅 환경에서 기업과 정부 기관에 새로운 수준의 가시성과 정보를 제공하여 APT공격과 타겟형 공격에 대한 방어를 제공.

**지능형 지속 위협(APT) 공격에 대한 완벽한 라이프사이클 제공**

탐 지

구체적인 이협 탐지 및 방어

분 석

고객환경에 맞는 가상화분석을 통한 위협에 대한 분석 정보 제공

적 용

고객환경에 맞는 블랙리스트/패턴 적용, 네트워크 보안 환경에 대비

대 응

공격에 대한 정보 및 가이드제공 빠른 위협 제거 및 치료