

APT Guard 제품소개 자료



[주] 가디언넷



1. APTGuard 필요성

- 악성 트래픽(C&C Callback) 발생 및 악성 사이트 접속에 대한 차단 필요
- PMS에 의한 수동적인 치료 Agent 배포 시 설치 실패 및 오프라인 등 미설치 PC에 대한 관리가 어려워 능동적인 배포 방안 필요
- 모든 PC에 Agent 설치 시 관리가 어렵지만 관리가 필요한 PC를 위주로 집중적으로 관리하여 치료율 향상

2. APTGuard 동작 방식

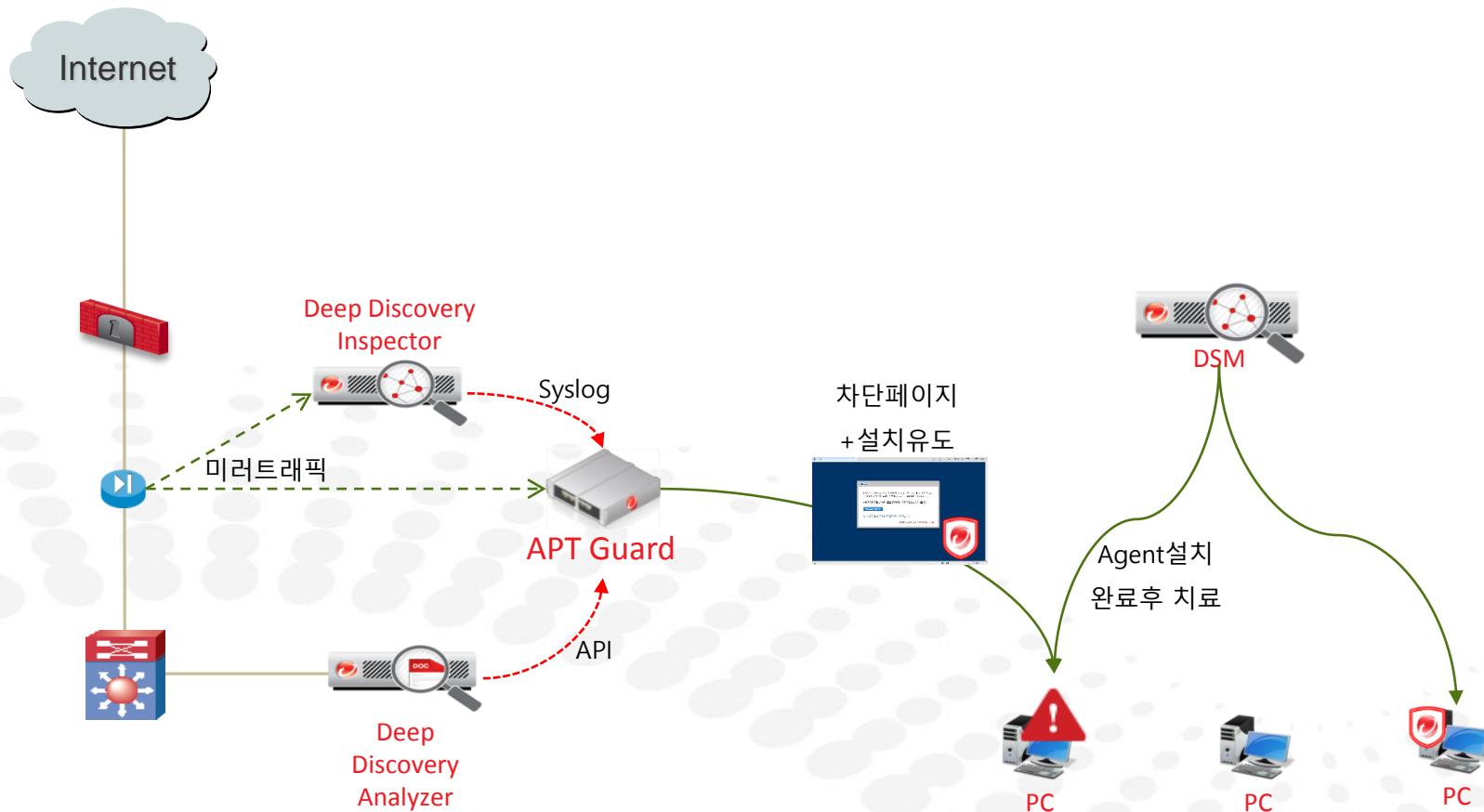
- 감염 의심 PC만을 선별하여 치료 에이전트(DSA / OCSE 에이전트)의 선택적 배포 가능
- Target PC의 악성 트래픽에 대한 Session Kill 제공
- Target PC의 인터넷(웹브라우저) 차단 및 경고 페이지를 통한 설치 유도 제공
- DDI syslog 및 DDAN의 분석결과를 기반으로 한 Target PC 선정

3. 제품 스펙

◆ 기본 HW Spec.

구 분	세 부 내 용
CPU	Intel 4core
메모리	4GB
DISK	500GB
Size	1U Rack size
LAN CARD	<ul style="list-style-type: none">- On board 10/100/1000 UTP * 2EA- Optional : 1G UTP or 1G Fiber * 4EA
O / S	Linux

4. APTGuard 동작 방식



5. APTGuard 주요 기능

메인

서버	파일 명	비고	삭제
1	Agent-Core-Windows-9.6.2-50 29.x86_64.msi	DSA	삭제
2			
3			
4			

서버: *** server 목록 ▼** 설치파일: **[파일 선택]** 선택된 파일 없음 비고: **등록**

모니터링 네트워크

No.	StartIP	EndIP	서버/Agent	비고	수정
1	192.168.1.0	192.168.9.255	1	인터넷 PC 대역	수정 삭제
1	172.17.10.0	172.17.20.255	1	외부 사용자	수정 삭제

IP대역: ~ 서버/Agent: *** server 목록 ▼** 비고: **등록**

예외 네트워크

No.	StartIP	EndIP	비고	수정
-----	---------	-------	----	----

IP대역: ~ 비고: **등록**

Agent 미지원 OS

No.	OS	비고	삭제
1	windows 10		삭제

미지원 OS: 비고: **등록**

설치대상 에이전트 등록

설치대상 네트워크 등록

예외 네트워크

예외 OS 설정