CYLANCE

Cylance PROTECT

CylancePROTECT Overview

기존의 시그니쳐 기반 AV(Anti-Virus) 솔루션들은 급격한 속도로 증가하고 있는 랜섬웨어 및 지능형 신종 악성코드와 무수한 변종들을 방어하기엔 한계에 이르렀으며, 이러한 한계를 극복하고자 최근 머신러닝 기술을 접목한 악성코드 탐지 솔루션의 필요성이 각광 받고 있습니다.

머신러닝 기반 악성코드 탐지 솔루션은 기존에 수집된 악성코드의 특성을 다양한 머신러닝 알고리즘을 적용하여 학습하고, 이 학습 데이터를 기반으로 전혀 새로운 형태의 악성코드도 분류해 낼 수 있는 인공지능을 탑재하고 있습니다. 이러한 인공지능은 알려지지 않은 신종, 변종 악성코드를 정확히 탐지해 낼 수 있으며, 기존의 시그니쳐 기반, 휴리스틱 기반, 샌드박스 기반, 평판조회 기반 AV 솔루션 대비 훨씬 높은 탐지율을 보장합니다.

시그니쳐기반	머신러닝기반
평균 악성코드 탐지율 ▸▸ 83.5%	평균 악성코드 탐지율 ▸▸ 98% 이상

미국 보안제품 테스트기관 Miercom 2016 보고서

CylancePROTECT는 머신러닝 기술에 기반한 차세대 엔드포인트 보안 솔루션의 선두주자라고 할 수 있으며 10페타바이트가 넘는 악성코드 데이터를 학습한 인공지능 엔진을 탑재하고 있습니다.

CylancePROTECT의 인공지능은 헤더정보, 서명, 각종 스트링, 임포트, 섹션 권한, 패커, 컴파일러 등에 이르기까지 700만개 이상의 파일 특징(feature)을 0.1초 이내에 종합하여 소위 "파일의 DNA"를 분석해 그 의도를 정확히 파악하고 악성여부를 판단합니다.

개발사인 미국 Cylance®사는 Forbes가 2015년 선정한 가장 빠르게 성장하는 보안업체로서, 2016년 1,089% 매출 성장률을 기록했으며, 기업가치 1조원 이상의 "유니콘 클럽"에 진입하였고, 머신러닝 관련 특허 10개를 보유하고 있습니다.

CylancePROTECT 주요기능

악성코드 공격으로부터 엔드포인트를 전방위적으로 보호하기 위한 다음 기능을 제공합니다.

악성코드 실행전 차단 (Malware Execution Control)

- 프로세스 신규 생성 또는 라이브러리 로딩시 해당 파일을 검사하여 악성일 경우 실행전 차단
- 기존, 신종, 변종 악성코드(랜섬웨어 포함)의 실시간 사전 차단

메모리 공격 실시간 제어 (Memory Protection)

- 익스플로잇 방지
  (스택피벗, 코드덮어쓰기, 램스크래핑, 힙스프레이 등)
- 코드 인젝션 방지 (메모리 원격할당, 매핑 등)
- 권한 상승 방지 (LASS 읽기, 제로할당 등)

스크립트/익스플로잇 실시간 제어 (Script Control)

- 악성 PowerShell 스크립트, 엑티브 스크립트 차단
- MS Office 문서내 악성 VBA 매크로 차단
- File-less 기반의 공격탐지 및 차단

앱 제어 (Application Control)

- 실행 가능한 앱 리스트 관리
- 앱 변경 제어

디바이스 제어 (Device Control)

- USB 저장장치 이용 로깅 및 통제
- 외부 저장장치를 통한 정보유출 방지

CylancePROTECT 특장점

알려지지 않은 악성코드 탐지

머신러닝 기반으로 시그니쳐없이 신종 악성코드를 탐지할 수 있습니다. 일례로 2016년 1월 버전의 CylancePROTECT 로 2017년 5월 전세계를 강타한 워너크라이(WannaCry) 랜섬웨어와 6월 유행한 페티아(Petya) 랜섬웨어를 모두 탐지하였습니다.

빠른 처리속도

파일당 평균 분석시간은 0.1초 이하로 실시간으로 악성여부 결정 및 차단이 가능합니다.

최소 리소스 소모

파일 분석시 소모되는 메모리량은 평균 30MB, CPU량은 1% 미만 수준으로 PC, 서버 등 엔드포인트 성능에 전혀 부담을 주지 않습니다. 또한 사용자가 전혀 인지하지 못하도록 사일런트 모드로 동작할 수 있습니다.

안정성

현재까지 어떠한 다른 엔드포인트 솔루션 에이전트와 충돌이 보고된 적이 없어 안정성이 매우 높습니다.

일일 업데이트 불필요

매일 업데이트를 해줘야 하는 시그니쳐기반 AV와는 달리 연간 평균 2회만 인공지능을 업데이트하면 되므로 패치서버를 운영하는 부담이 크게 줄어듭니다. 또한, 패치서버에 연결 되어 있지 않더라도 최고의 보호상태를 계속 유지하며 USB 등을 통해 유입될 수 있는 신종악성코드를 방어 할 수 있습니다.

클라우드 활용

CylancePROTECT는 클라우드 접속 없이 네트워크가 차단된 환경에서도 정상동작을 하지만 사용자가 다양한 위협정보 (Threat Intelligence)를 얻기를 원한다면 Cylance의 클라우드 서비스를 활용 할 수 있습니다. Cylance 클라우드는 REST API를 제공하며 이를 통해 글로벌 격리 목록, 정상으로 판정된 의심파일 목록 등 위협정보를 받을 수 있고 특정 파일을 전송하여 클라우드에서 분석을 진행 할 수도 있습니다.

Threat Visualization

탐지된 위협 정보는 Cylance 관리 콘솔을 통해 시각화 하여 보여 줍니다. 수집된 각종 위협 정보와 차단정보 및 사고분석 정보를 제공하여 전문적인 지식을 가진 보안 분석가가 아니더라도 위협을 직관적으로 인지하고 분석할 수 있게 도와줍니다.

엔드포인트 지원 OS

CylancePROTECT는 대부분의 주요 OS를 지원합니다.

Windows

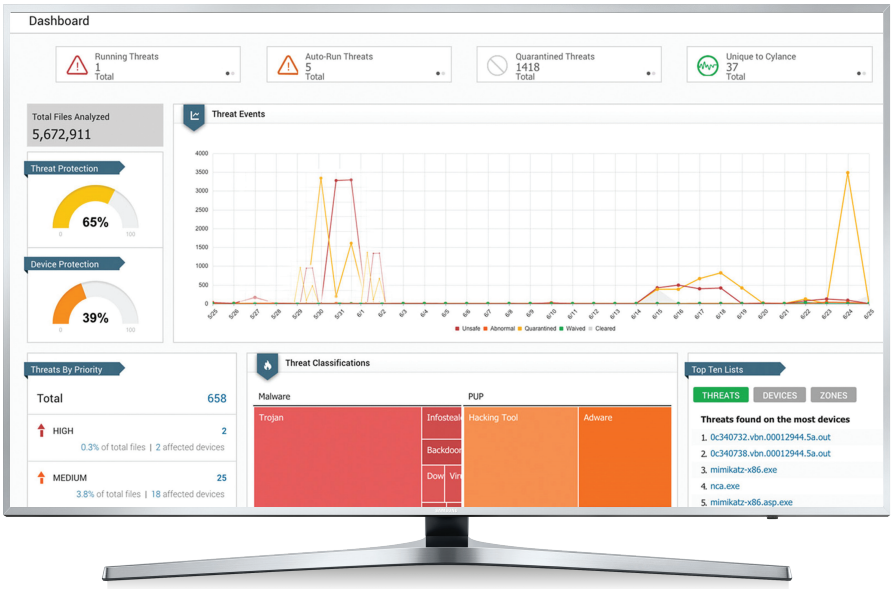
- Windows XP SP3
- Windows Vista
- Windows 7
- Windows 8 / 8.1
- Windows 10
- Windows Server 2003 SP2
- Windows Server 2008 / 2008 R2
- Windows Server 2012 / 2012 R2
- Windows 2016 Standard, Datacenter, Essential

Mac OS

- OS X 10.9 (Mavericks)
- OS X 10.10 (Yosemite)
- OS X 10.11 (El Capitan)
- OS X 10.12 (Sierra)

Linux

- RedHat Enterprise 6 ~ 7
- CentOS 6.6 ~ 7.3



제품 문의 | 사일런스 홈페이지: www.cylance.com
사일런스 한국총판: www.samsungsds.com

삼성SDS SAMSUNG