Trellix

데이터시트

Trellix 파일 보호

파일 공유 및 콘텐츠 저장소의 악성코드 탐지 및 제거

특장점

- 기존 백신 엔진으로 탐지되지 않는 잠복 악성코드 탐지
- 실시간 격리(보호) 또는 분석 전용(모니터링) 모드 지원
- CIFS 및 NFS 호환 파일 공유에 대한 재귀, 예약, 수동(on-demand) 스캔 제공
- Microsoft OneDrive 및 SharePoint 에 대한 선제적 보호 제공
- PDF, MS Office 문서, 멀티미디어 파일 등 다양한 유형의 파일 분석
- Trellix IVX Cloud와 통합되어 파일 분석 및 위협 정보 공유 (Trellix Central Management 및 DTI Cloud 활용)

개요

Trellix File Protect는 이메일, 온라인 파일 전송 도구, 클라우드, 휴대용 저장장치 등에서 유입되는 공격으로부터 다양한 유형의 파일 자산을 보호합니다. 이러한 공격은 파일 공유 및 콘텐츠 저장소로 확산될 수 있습니다. File Protect는 네트워크 파일 공유 및 콘텐츠 관리 저장소를 분석하여, 차세대 방화벽, 침입 방지 시스템(IPS), 백신(AV) 시스템 및 게이트웨이를 우회한 악성코드를 탐지하고 격리합니다.

파일 공유 내 악성코드의 위협

오늘날의 고급 사이버 공격은 정교한 악성코드와 APT(지능형 지속 위협) 전술을 사용하여 방어 체계를 우회하고, 파일 공유 및 콘텐츠 저장소를 통해 수평적으로 확산됩니다. 이로 인해 악성코드는 네트워크 내에 장기적인 거점을 형성하고, 심지어 오프라인 상태의 시스템에도 감염을 확산시킬 수 있습니다.

많은 엔터프라이즈 데이터 센터는 이러한 고급 콘텐츠 기반 악성코드에 특히 취약합니다. 이는 기존 방어 시스템이 합법적인 경로를 통해 침입하는 위협에 효과적으로 대응하지 못하기 때문입니다. 공격자들은 이러한 취약점을 악용하여 악성코드를 네트워크 파일 공유에 확산시키고, 대규모 데이터 저장소 내에 악성 코드를 은닉해 지속적인 위협을 유지합니다.

파일 콘텐츠 보호의 중요성

콘텐츠 내에 잠복한 악성코드를 탐지할 수단이 없다면, APT 공격은 네트워크 자산을 악용해 기밀 정보를 유출하고 큰 피해를 초래할 수 있습니다. File Protect는 Trellix Intelligent Virtual Execution(IVX) 엔진을 활용하여 파일 공유 및 콘텐츠 저장소를 분석하며, PDF, MS Office, vCard, ZIP/RAR/TNEF 등의 일반 파일 형식과 MP3, JPG, PNG 등의 멀티미디어 콘텐츠 내에 숨겨진 제로데이 악성코드를 탐지합니다.

File Protect는 접근 가능한 네트워크 파일 공유 및 콘텐츠 저장소를 대상으로 재귀, 예약, 수동(on-demand) 스캔을 수행하고, 악성코드를 식별 및 격리하여 지능형 공격 수명 주기의 핵심 단계를 차단합니다.

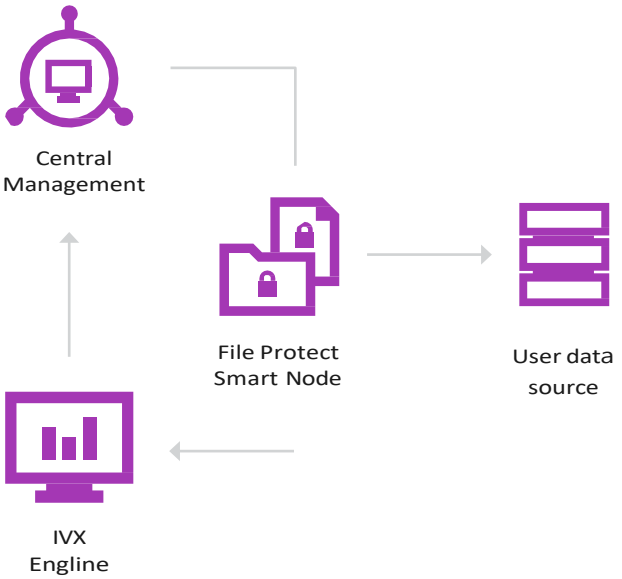

Figure 1. Trellix File Protect 구성 예시

알려지지 않은 제로데이 위협 탐지

Trellix FX는 IVX 엔진을 사용하여 각 파일을 검사하고, 제로데이 익스플로잇 또는 악성 코드 존재 여부를 확인합니다.
IVX 엔진은 제로데이, 다중 흐름 기반 위협 및 은폐형 공격을 서명 없이 동적 분석하여 가상 환경 내에서 탐지하며, 공격 체인의 감염 및 침해 단계를 사전에 차단합니다.

IVX Smart Grid 의 강점

Trellix IVX Smart Grid는 하이브리드 또는 프라이빗 클라우드를 기반으로 한 유연하고 확장 가능한 아키텍처를 통해 조직의 보안 수준을 향상시킵니다. IVX Smart Grid는 IVX 엔진을 하드웨어 및 가상 Smart Node로부터 분리하는 혁신적인 구조를 적용하여, 본사 · 지사 · 원격 사용자를 효과적으로 보호합니다.
Smart Node는 인터넷 트래픽을 분석하여 정적 분석, 보안 분석, IPS, 적용된 인텔리전스 등 다양한 기술을 활용해 위협을 탐지 및 차단하고, IVX 엔진은 핵심 동적 분석을 수행합니다.

Microsoft OneDrive 및 SharePoint 보호

File Protect는 OneDrive 및 SharePoint 저장소를 지속적으로 스캔하여 악성코드를 탐지하고 경고 및 영구 격리합니다. SharePoint 서비스와의 보안 통합은 WebDAV 프로토콜을 사용하여 이뤄지며, SharePoint 저장소 기반의 비즈니스 워크플로우를 효과적으로 보호합니다.

YARA 기반 룰로 맞춤 분석

File Protect는 사용자 정의 YARA 룰을 지원하여, 조직 특화 위협을 정밀 분석할 수 있도록 합니다.

사고 대응 우선순위 자동화

Trellix Endpoint Security와 통합하면, 각 악성 객체에 대해 기존 백신 엔진이 탐지 가능한지 추가 분석할 수 있습니다. 이를 통해 사고 대응 우선순위를 효율적으로 정하고, 알려진 악성코드에 대한 공통 명명 체계를 사용할 수 있습니다.

악성코드 인텔리전스 공유

분석 결과로 생성된 실시간 위협 인텔리전스는 Trellix Central Management와 통합되어 로컬 네트워크 전반을 보호하는 데 활용됩니다.

또한 이 인텔리전스는 Trellix Dynamic Threat Intelligence(DTI) Cloud를 통해 전 세계 Trellix 사용자에게 공유되어, 신종 위협에 대한 선제적 대응이 가능합니다.

튜닝 없이 배포, 오탐 최소화

기존 보안 솔루션과 달리 Trellix File Protect는 튜닝 없이도 바로 배포할 수 있으며, 오탐율이 거의 없습니다.

분석 전용 모니터링 모드 또는 능동적 격리 모드로 유연하게 구성할 수 있으며, 조직 내 파일 공유에 존재하는 악성코드를 파악하고, 수평 확산을 적극적으로 차단합니다.

Content Smart Node를 통한 유연한 콘텐츠 보호

Trellix Content Smart Node는 콘텐츠 및 보안 관리자가 기업 전반의 미션 크리티컬 콘텐츠를 유연하게 보호할 수 있는 가상화 솔루션을 제공합니다.
IVX Smart Grid 기반 아키텍처를 활용하여, 보호가 필요한 곳에 콘텐츠 보안을 확장성과 함께 손쉽게 배포할 수 있습니다.

Deploy via flexible form factors 유연한 배포 지원

가상 Content Smart Node 또는 전통적인 온프레미스 하드웨어 어플라이언스 중 선택하여, 환경에 적합한 배포 방식을 구성할 수 있습니다.

Table 1. Trellix File Protect Smart Node 가상 어플라이언스 사양

	FX 2500V
운영 체제 지원	Microsoft Windows, MacOS X, CentOS
성능	50,000 files per day
네트워크 인터페이스 포트	Ether 1, Ether 2
CPU 코어 수	2
메모리	8 GB
저장 용량	512 GB
하이퍼바이저 지원	KVM 1.5.3, VMWare ESXi 6.0 or later

Table 2. Trellix File Protect Smart Node 클라우드 어플라이언스 사양

	FX 2500V
운영 체제 지원	Microsoft Windows, MacOS X, CentOS
성능	50,000 files per day
네트워크 인터페이스 포트	Ether 1, Ether 2
CPU 코어 수	2
메모리	8 GB
저장 용량	512 GB (AWS), 2TB (Azure)
하이퍼바이저 지원	AWS m5.xlarge, Azure

Table 3. Trellix File Protect Smart Node 하드웨어 어플라이언스 사양

	FX 6600
성능	Up to 87,000 files per day
네트워크 인터페이스 포트	1x 1 GigE BaseT
IPMI 포트 (후면 패널)	included
USB 포트 (후면 패널)	2X USB2.0 , 2X USB3.2
시리얼 포트 (후면 패널)	115,200 bps, no parity, 8 bits, 1 stop bit
저장 용량	4x 4TB RAID 10, HDD 3.5 inch, FRU
인클로저 형식	2RU, fits 19-inch rack
섀시 크기 (가로 x 깊이 x 높이)	17.2 x 25.5 x 3.5 inches (437 x 620 x 88.4 mm)
AC 전원 공급 장치	Redundant (1+1), FRU, 920W with Input 100-240V, 11-4.4A, 50-60 Hz IEC60320-C14 inlet
최대 전력 소비량	618 watts
최대 열 방출	2108 BTU/hr
MTBF	26023
어플라이언스 단독/배송 시 무게 (lb /kg)	41 lbs/ 67 lbs
안전 인증	CAN/CSA 22.2 No. 62368 UL 62368 IEC 62368, EN 62368 BS EN 62368
EMC/EMI 인증	FCC Part 15 Class-A, CE (Class-A), CNS 13438, CISPR 32, VCCI-CISPR32, EN 55035, EN 55032, EN 61000, ICES-003, KN 32, KN 35
작동 온도	5°C - 35°C (41°F - 95°F)
작동 상대 습도	5% - 95% (non-condensing)
작동 고도	0 to 5000ft