SOPHOS
Security made simple.

Sophos Intercept X

비교 할 수 없는 엔드포인트 보호

소포스 Intercept X는 머신 러닝 멀웨어 탐지, 익스플로잇 차단,
안티 랜섬웨어 등의 조합으로 가장 광범위한 공격을 차단합니다.

Highlights

- 최고의 멀웨어 탐지 엔진과 딥러닝 기술 제공
- 익스플로잇 방어는 공격자가 취약한 소프트웨어를 제어하는 기술을 차단
- 능동적인 공격자를 완화하여 호스트에 지속적인 방어를 제공 합니다.
- 근본원인분석은 멀웨어가 무엇을 했고 어디서 들어 왔는지 확인하게 합니다.
- 소포스만의 랜섬웨어 방어 기술
- Intercept X는 기존의 안티바이러스를 보완합니다. Intercept X Advanced는 최신의 기술과 기본 안티 바이러스의 방식을 조합하여 최신의 엔드포인트 보안을 제공합니다.

Sophos Intercept X는 단순히 중요한 하나의 보안 기술에 의존하는 것이 아니라, 엔드포인트 탐지를 위해 종합적은 심층방어(Defense-in-depth) 접근 방식을 적용 했습니다. 이것은 선도하는 기본 기술과 현대 기술의 조합으로 "the power of the plus" 입니다.

최신 기술은 딥러닝 멀웨어 탐지, 익스플로잇 차단, 특정 안티랜섬웨어 기능 등이 포함되어 있고, 기본 기술로는 시그니처 기반의 멀웨어 탐지, 행위 기반분석, 악의적인 트래픽 탐지, 디바이스 제어, 애플리케이션 제어, 웹 필터링, 데이터 손실 방지(DLP)등이 포함되어 있습니다.

딥 러닝 멀웨어 탐지

Intercept X에 내장된 인공 지능은 딥러닝 신경 네트워크로, 시그니처 의존 없이 알려진 멀웨어와 알려지지 않은 멀웨어 모두를 탐지하는 진화된 형태의 머신러닝 입니다.

Intercept X에 내장된 업계최고의 멀웨어 탐지 엔진으로, 제 3자 테스트 기관으로부터 검증을 받았습니다. 이로써 Intercept X는 다른 엔드포인트 보안 툴이 탐지 하지 못하는 멀웨어를 탐지 할 수 있게 되었습니다.

익스플로잇 차단과 공격 차단

소프트웨어에서 취약점은 빠르게 나타나며, 벤더가 지속적으로 패치 해야 합니다. 반면에 새로운 익스플로잇 기술의 등장은 매우 드물어 취약점을 발견한 공격자가 익스플로잇을 반복적 사용 합니다. 익스플로잇 방어는 익스플로잇 배포, 자격 증명 탈취, 탐지 우회에 사용되는 익스플로잇 툴과 기술을 차단 합니다. 이를 통해 소포스는 네트워크에서 보안을 우회 하는 해커와 제로데이 (Zero-day) 공격을 방어 할 수 있습니다.

입증된 랜섬웨어 보호

Intercept X는 이전에 본적 없는 멀웨어와 부트 레코드 공격을 행위 분석을 활용하여, 가장 진화된 안티 랜섬웨어 기술을 만들어 내고 있습니다. 신뢰할 수 있는 파일 이나 프로세스 조차도 악용되거나 도용된 경우, CryptoGuard는 차단하고 사용자가 IT 지원 담당자의 개입 없이 원래 상태로 되돌릴 수 있습니다. CryptoGuard는 파일 시스템 레벨에서 동작하여, 문서나 다른 파일을 수정하려는 원격 컴퓨터와 로컬 프로세스를 지속적으로 감시 합니다.

엔드포인트 탐지 및 대응 (EDR)

예방 차원을 넘어서 추가 위협을 탐지, 조사하고 대응 하기 위해선 엔드포인트 탐지 및 대응(EDR) 기능이 필요 합니다. Sophos Intercept X Advanced with EDR은 업계 최고수준의 엔드 포인트 보호기능과 지능형 EDR을 단일 솔루션으로 통합하여 제공하기 때문에 조직내에서 발생하는 보안사고에 민첩하게 대응 할 수 있습니다.

심플한 관리와 배포

소포스 센트럴에서 보안을 관리 할 수 있다는 것은 안전한 엔드포인트를 위해 더 이상 서버를 준비하고 설치 하지 않아도 된다는 것을 의미 합니다. 소포스 센트럴은 첫날부터 가장 효과적인 보호를 받을 수 있도록 하기 위해 기본 정책과 권고 구성을 제공 합니다.

방어를 위한 4단계

1. 평가판 사용을 하기 위해 sophos.com/intercept-x를 방문 하십시오.
2. 소포스 센트럴 관리자(Admin) 권한을 생성 하십시오.
3. Intercept X 에이전트를 다운로드 하여 설치 하십시오.
4. 소포스 센트럴을 통해 에이전트를 관리 하십시오.

기술 명세서 (Technical Specifications)

Sophos Intercept X는 Windows7 또는 그 이상 버전에서 동작하며, 32비트, 64비트 모두를 지원 합니다. 또한 타사 엔드포인트와 안티바이러스 제품과 함께 실행하여 딥러닝 멀웨어 탐지, 안티 익스플로잇, 안티 랜섬웨어, 근원원인분석, Sophos Clean기능을 추가 할 수 있습니다. Intercept X Advance는 Intercept X의 최신 기능에 소포스 센트럴 엔드포인트 보호의 기본 기술이 더해진 제품 입니다.

			엔드포인트 프로텍션				INTERCEPT X	
		SKU	ENDPOINT PROTECTION STANDARD	ENDPOINT PROTECTION ADVANCED	ENDPOINT EXPLOIT PREVENTION	CENTRAL ENDPOINT PROTECTION	CENTRAL INTERCEPT X ADVANCED	CENTRAL INTERCEPT X ADVANCED W/ EDR
보호 (PREVENT)	공격지점 감소	웹 보안 (Web Security)	✓	✓		✓	✓	✓
		다운로드 평판 확인	✓	✓		✓	✓	✓
		웹 제어/ 카테고리 기반URL 차단	✓	✓		✓	✓	✓
		매체 제어 (e.g. USB)	✓	✓		✓	✓	✓
		어플리케이션 제어	✓	✓		✓	✓	✓
		클라이언트 방화벽	✓	✓				
	실행 전 분석	딥 러닝 멀웨어 감지					✓	✓
		안티 멀웨어 파일 검사	✓	✓		✓	✓	✓
		라이브 프로텍션 (Live Protection)	✓	✓		✓	✓	✓
		실행 이전 행위 분석 (HIPS)	✓	✓		✓	✓	✓
		Potentially Unwanted Application (PUA) 차단	✓	✓		✓	✓	✓
		패치 평가 (Patch Assessment)		✓				
		데이터 유출 방지 (DLP)		✓		✓	✓	✓
		익스플로잇 방지			✓		✓	✓
탐지 (DETECT)	위협실행 차단	런타임 행위 분석 (HIPS)	✓	✓		✓	✓	✓
		악의적인 트래픽 감지 (MTD)		✓		✓	✓	✓
		Active Adversary 완화 (안티 해커)					✓	✓
		랜섬웨어 파일 보호 (CryptoGuard)			✓		✓	✓
		디스크 및 부트레코드 보호 (WipeGuard)					✓	✓
		Man-in-the-Browser Protection (Safe Browsing)			✓		✓	✓
대응 (RESPOND)	조사 및 제거	자동 멀웨어 제거	✓	✓		✓	✓	✓
		Synchronized Security Heartbeat				✓	✓	✓
		근본 원인 분석					✓	✓
		Sophos Clean			✓		✓	✓
		Endpoint Detection & Response (EDR)						✓