SOPHOS

Cybersecurity made simple.

CLOUD READY

Intercept X for Server

사내에 있던 클라우드에 있던, 관리자는 서버상에 존재하는 기업의 핵심 데이터와 중요 어플리케이션을 보호해야 합니다. 서버용 인터셉트 X는 딥러닝 멀웨어 탐지, 익스플로잇 방지, 안티 랜섬웨어 기술, 어플리케이션 화이트리스팅, 고급 익스플로잇 완화, 그리고 심도 있는 근본원인분석을 사용해 포괄적인 심층 방어 (Defense-in-depth) 접근법을 제공합니다.

Highlights

- 마이크로소프트 애저(Azure)와 아마존웹서비스(AWS) 상의 워크로드 디스커버리 및 보호
- 감염된 엔드포인트로부터의 원격 공격을 포함하여 서버를 랜섬웨어로부터 보호
- 서버 락다운(Lockdown) – 어플리케이션 화이트리스팅
- 지능형 해킹 기법 및 익스플로잇 차단
- 공격의 원인 및 감염 경로에 대한 상세 정보를 제공하는 근본원인분석
- 여러 소포스 제품들간의 위협, 상태, 보안 정보를 공유하는 소포스 동기화 보안 (Synchronized Security)
- 소포스 센트럴 (Sophos Central)을 통한 간편한 관리
- 윈도우 및 리눅스 시스템에 대한 위협 방어

서버에 특화된 강력한 보호 기능

서버용 인터셉트 X 는 제로데이 공격, 익스플로잇 및 해커의 공격을 방어하기 위해 광범위한 보호 기능을 활용합니다. 이러한 보호 기능들은 먼저 공격이 서버에 도달하는 것을 방지하고, 실행되기 전에 공격을 탐지하거나, 실행을 차단하며 보호 기능을 간신히 우회한 경우라도 철저한 클린업(cleanup)을 제공합니다. 지속적으로 업데이트 되는 인공지능(Artificial Intelligence) 모델은 서버에서 잠재적으로 악의적인 코드에 대한 의심스러운 속성을 찾도록 잘 훈련되었습니다.

또한, 서버 락다운(Lockdown) 및 클라우드 워크로드 디스커버리(Cloud Workload Discovery)와 같은 서버 특화 기능을 사용하면 서버 구성이 더욱 안전합니다.

서버용 인터셉트 X 는 마이크로소프트 애저(Azure)와 아마존웹서비스(AWS)를 포함한 클라우드 상의 워크로드를 찾고 보호합니다. 소포스 센트럴(Sophos Central)과 AWS 및 애저를 연결함으로써, 서버용 인터셉트 X는 서버가 보호되고 있는 상황을 시각적으로 확인할 수 있으며, 소포스 센트럴 상에 관련 정보를 표시하여 관리가 쉬워집니다.

서버 기반의 랜섬웨어 방어

크립토가드(CryptoGuard)는 의도치 않은 파일 암호화를 감지하고 차단하기 위해 파일 시스템 레벨에서 동작하며, 서버 상의 혹은 서버와 연결된 원격지 엔드포인트로부터의 랜섬웨어 공격을 방어합니다. 와이프가드(WipeGuard)는 마스터부트레코드(MBR)를 악의적인 암호화로부터 보호합니다.

서버용 인터셉트 X는 한 번의 클릭으로 서버를 잠글 수 있습니다. 서버를 안전한 상태로 보호하기 위해 어플리케이션 화이트리스팅을 수행하며, 인가되지 않은 어플리케이션의 실행을 차단합니다. 시스템을 검사하여 수동 규칙 생성이 필요 없이 자동으로 승인된 어플리케이션의 인벤토리(목록)를 설정합니다. 어플리케이션과 그와 연관된 DLLs, 데이터 파일, 스크립트와 같은 파일을 완벽하게 연결합니다.

Disrupt attacks: 해커의 서버 접근 차단

취약점(Vulnerabilities)은 놀라운 속도로 생겨나며, 사용자의 불편 없이 서버를 패치 하는 것은 쉽지 않은 일입니다. 서버 환경에서 익스플로잇(Exploit) 공격은 치명적일 수 있으며 전형적인 안티바이러스 기술로는 탐지할 수 없는 경우가 많습니다. 서버용 인터셉트 X는 가장 완고한 해커조차도 자격증명을 수집하기 위해 익스플로잇 기법을 사용하지 못하도록 설계되었습니다. 해커가 숨겨진 상태로 유지를 시도하든 지속적인 접근을 시도하든, 혹은 같은 네트워크 상에서 이동을 시도하든 인터셉트 X 는 이런 시도를 차단하도록 설계 되어 있습니다.

서버용 인터셉트 X

근본 원인 분석

서버용 인터셉트 X 에는 완벽한 가시성을 제공하기 위한 탐지(Detection) 및 대응(Response) 기술이 포함되어 있으므로 관리자는 공격의 진입 지점, 진행 방향, 영향 받은 파일들과 향후 취해야 할 조치에 대해 알 수 있습니다. 서버용 인터셉트 X는 추가적인 에이전트나 관리 콘솔 없이 이 기능을 제공합니다.

소포스 동기화 보안(Synchronized Security)

소포스 동기화 보안은 공격에 대응하는 방어 시스템들을 연계하는 최상의 보안 시스템입니다. 수상 경력에 빛나는 제품들과 직관적인 보안 플랫폼을 결합하여 적극적으로 협력하며 고급 위협을 차단하기 위한 독보적인 보호 기능을 제공합니다.

소포스 센트럴을 통한 손쉬운 관리

소포스 센트럴(Sophos Central)을 통해 보안을 관리하면 더 이상 시스템을 보호하기 위한 관리서버를 배치할 필요가 없습니다. 소포스가 제공하는 소포스 센트럴은 설치할 콘솔 서버 없이 즉각적인 엑세스를 제공합니다.

소포스 센트럴은 서버에 대해 격이 다른 정책들을 제공하는 동시에 소포스 인터셉트 X, 모바일, 와이파이, 이메일 및 웹 등의 모든 소포스 제품을 하나의 창으로 관리할 수 있습니다.

서버용 인터셉트 X 주요 기능

보호		윈도우 서버	✓
		리눅스[1]	✓
		퍼블릭 클라우드 (MS애저, 아마존 AWS)	✓
	공격지점 감소	어플리케이션 화이트리스팅 (서버 락다운)	✓
		웹 보안	✓
		윈도우 방화벽 제어	✓
		다운로드 평판 확인	✓
		웹 제어 (URL 차단)	✓
		매체제어 (e.g USB 등)	✓
		어플리케이션 제어	✓
	적극적 행동	딥 러닝 멀웨어 탐지	✓
		익스플로잇 방어	✓
		안티 멀웨어 파일 검사	✓
		라이브 프로텍션 (Live Protection)	✓
		실행 이전 행위 분석 (HIPS)	✓
		가상 머신 검사 (ESXi and Hyper-V)[2]	✓
		PUA (Potentially Unwanted Application) 탐지	✓
		데이터 유출 방지 (DLP)	✓
감지	실행차단	안티 해커/능동형 공격자 완화	✓
		랜섬웨어 파일 보호 [CryptoGuard] 원격지 엔드포인트로부터의 공격을 감지하는 것을 포함.	✓
		디스크 및 부트레코드 보호 [WipeGuard]	✓
		악의적인 트래픽 감지 (MDT)	✓
대응	조사	Sophos Clean - 자동 멀웨어 제거	✓
		근본 원인 분석	✓
관리	제어	서버 특화된 정책 관리	✓
		업데이트 캐시 및 메시지 릴레이	✓
		자동 검사 예외 처리	✓
		Synchronized Application Control[4]	✓
	가시성	애저 워크로드 디스커버리/보호	✓
		AWS 워크로드 디스커버리/보호	✓
		AWS 맵, 멀티 리전 시각화	✓
		시큐리티 하트비트™ (향상된 위협보호, 소스식별, 자동격리) 기술을 사용한 소포스 동기화 보안[4]	✓
		윈도우 리모트 데스크탑 서비스 (사용자 가시성)	✓
	소포스 센트럴	별도의 물리적 서버 설치가 필요 없는 클라우드 기반의 관리 플랫폼. 엔드포인트, 모바일, 이메일, 무선 솔루션과 함께 하나의 창에서 서버를 관리	✓
		멀티 팩터 인증	✓
		역할 기반 관리	✓

1 모든 기능은 윈도우에서 사용할 수 있습니다; 리눅스에서는 일부 기능만 사용할 수 있습니다.
2 에이전트 배포를 위해서 Sophos for Virtual Environments 라이선스 가이드를 참고하세요.
3 Sophos Enterprise Console에서 관리되는 윈도우 서버의 경우, 크립토가드 기능 사용을 위해서는 Endpoint Exploit Prevention(EXP)의 추가 라이선스가 필요합니다.
4 Sophos XG Firewall과 함께 사용 필요

Azure

aws partner network
Advanced Technology Partner
Security Competency
Public Sector Partner
Marketplace Seller