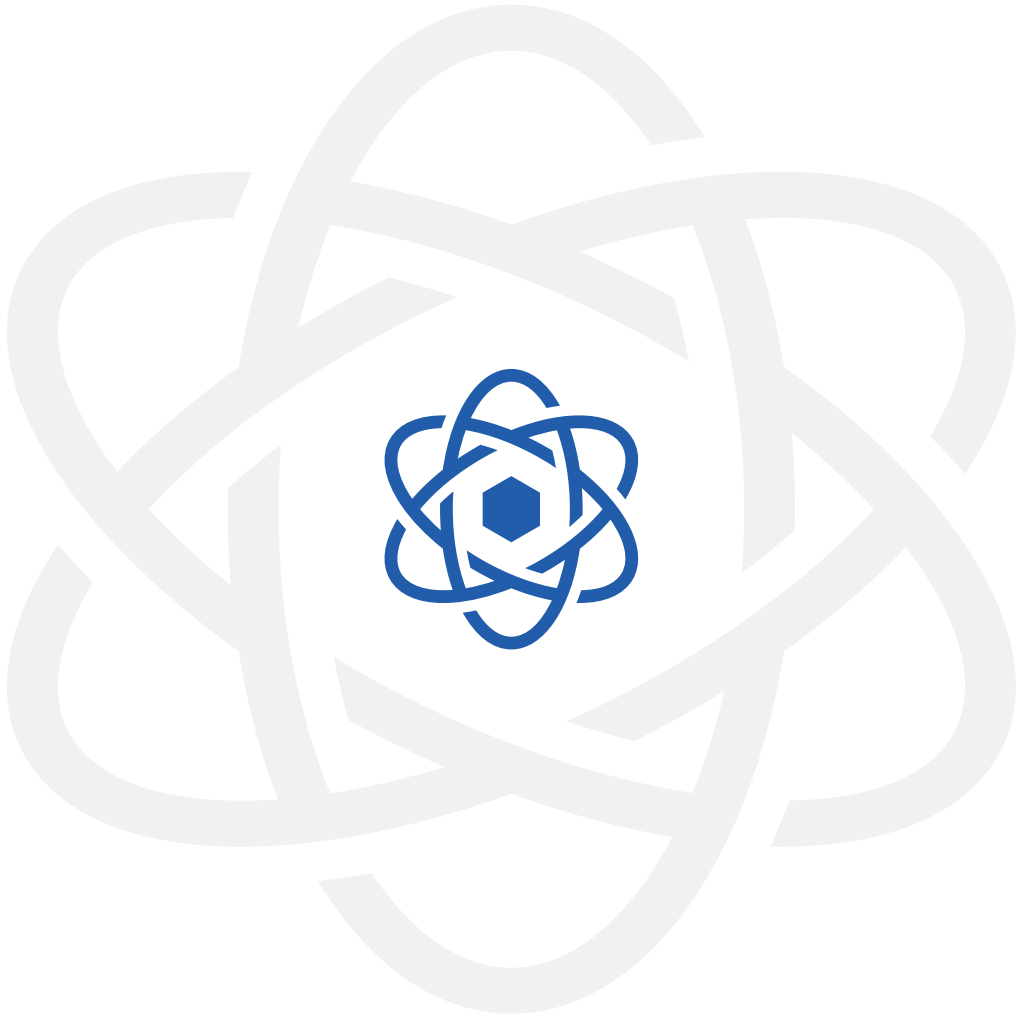
2022 Sophos
제품 안내서



Ep Fw Svr MTR Em Ph Mb ZT Sw RR Enc

SOPHOS

SOPHOS

Cybersecurity Evolved

Sophos 제품을 사용하면 노트북에서 가상 데스크탑, 서버, 웹, 이메일 트래픽 및 모바일 장치에 이르기까지 네트워크의 모든 엔드포인트를 보호할 수 있습니다. 또한, 이러한 장치의 보안은 사용자의 섬세한 요구 사항에 맞는 제품을 통해 가능합니다. Sophos는 다른 누구도 제공할 수 없는 단 한 가지 기능인 "Simplicity (간편성)"을 제공하여 네트워크의 보안을 보장합니다.

Sophos Endpoint
Intercept X
(차세대 엔드포인트)

Sophos Firewall
XGS Firewall
(차세대 방화벽)

Sophos MTR
Managed Threat Response
(매니지드 위협 대응)

Endpoint Protection

PC에서 서버, 스마트폰, 태블릿에 이르기까지 랜섬웨어 방어와 Deep Learning, XDR을 포함한 차세대 보호기능은 사용자를 안전하게 보호합니다.

Sophos Endpoint
Intercept X

Sophos Server
Intercept X for Server

Sophos Mobile
Central Mobile, Intercept X for Mobile

Network

Sophos의 Network 보안 제품은 차세대 방화벽, 스위치, 와이파이, 제로 트러스트 및 클라우드 제품을 포함합니다.

Sophos Firewall
XGS Firewall

Sophos ZTNA
Zero Trust Network Access

Sophos Switch

Security Operations

소포스의 전문 분석팀이 직접 고객사의 위협을 탐지하고 적절한 대응을 제공합니다.

Sophos MTR
Managed Threat Response

Sophos RR
Rapid Response

Messaging

소포스랩에서 사용하는 샌드박싱 기능이 포함된 이메일 보호와 사용자 피싱 교육을 위한 캠페인 및 교육 솔루션입니다.

Sophos Email
Central Email

Sophos Phish Threat
Central Phish Threat

Cybersecurity Evolved

SOPHOS HIGHLIGHTS

500,000 BUSINESSES
100M USERS
150 COUNTRIES
1985 FOUNDED
4,000 EMPLOYEES WORLDWIDE
90%+ RENEWAL RATE
70,000+ CHANNEL PARTNERS

Sophos

- 1985년 영국에서 설립된 최초의 시그니쳐 기반 백신 개발 회사
- 150개국 500,000 이상의 고객사, 1억명 이상의 사용자 보유
- 약 70,000개 이상의 채널 파트너
- Endpoint 보안 및 Network 보안 분야의 업계 리더
- 세계에서 가장 크고 빠르게 성장중인 MDR 서비스 업체

Gartner peerinsights customers' choice 2021

4.8/5 Customer Rating
Endpoint Protection Platforms

업계 분석기관에서 보는 Sophos

- 2021 Gartner Peer Insights '엔드포인트 보호' 고객사 평가 1위 선정
- 2021 Gartner Magic Quadrant '엔드포인트 보호' 13년 연속 리더 선정
- 2021 SE Labs SMB, Enterprise 대상 백신 정확도 1위
- 2021 Forrester 9년 연속 리더 선정
- MRG Effitas 위협 탐지 및 익스플로잇 차단 1위
- AV Comparatives 멀웨어 보호 1위

2021 Magic Quadrant for Endpoint Protection Platforms

SE Labs AAA Enterprise Endpoint Protection Jan-Mar 2019
AAA Rated
Enterprise Protection

MRG Effitas Efficacy Assessment & Assurance
100% Block
Real World Threats

Gartner
Leader
11 reports In a row

AV comparatives
#1
Malware Protection

SE Labs Intelligence-led Testing BEST Small Business Endpoint WINNER 2019
Best Solution
Small Business Endpoint

MRG Effitas Efficacy Assessment & Assurance
#1
Exploit Protection

FORRESTER®
LEADER
Since 2013

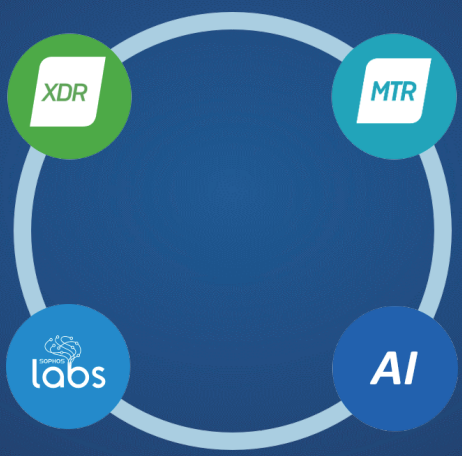
PC PCMAG.COM
Editor's Choice
Best Ransomware Protection

Sophos의 앞선 선순환 보호 구조

인적 분석과 자동화된 탐지가 이끌어내는 지속적인 현상

Practical Security

MTR, AI 및 Labs에서 생성되는 위협정보로부터 제품간의 예방, 탐지, 대응을 제공하는 지속적인 보정 및 예측



MTR SecOps

보안 대응팀과 분석가들이 발견하는 새로운 IOC와 위협 헌팅

Sophos Labs

독점적 위협 인텔리전스, 파일, 이메일, 행위, URL 및 DPI에 대한 전문적인 분석

Sophos AI

데이터에 대한 전문가 라벨링과 실시간 데이터에 대해 지속적으로 훈련 및 보정된 35개 이상의 모델

SOPHOS

Sophos Central

The world's most trusted cybersecurity platform

Sophos Central은 귀사의 모든 차세대 기술을 위한 단일 클라우드 관리 솔루션입니다. 통합 관리 콘솔로 제품 간 실시간 위협 정보 공유 및 자동화된 사고 대응, 사이버 보안을 보다 쉽고 효과적이게 합니다.

Highlights

- 단일 플랫폼 통합으로 시간, 노력 및 비용 절감
- 통합 제품 및 업계 최고의 A.I. 자동 위협 대응
- 강력한 리포팅, SophosLabs 위협 인텔리전스 및 교차 제품 조사
- 관리 역할에 따른 권한, 통합 및 API, 셀프 서비스 포털을 통해 모든 규모의 비즈니스를 위한 유연한 관리

시간, 노력 및 비용 절약

모든 보호 기능을 단일 클라우드 플랫폼으로 통합하면 리소스를 확장하지 않고도 보안을 확장할 수 있습니다. 모든 것을 한곳에서 볼 수 있으므로 시간, 노력 및 비용을 절약할 수 있습니다. 보호가 필요할 경우, 엔드포인트, 서버, 모바일, 퍼블릭 클라우드, 방화벽, 이메일, 무선, WAF, ZTNA 등에 대한 보안을 제공합니다.

고객은 IT 보안 관리에 소요되는 시간과 노력을 50% 절감하고, 보안 사고율을 85% 줄이며, 문제를 파악하는데 소요되는 시간을 90% 단축하는 등의 효과를 보고 있습니다.

자동화된 보안 제공

업계 최고의 A.I가 탑재된 Sophos Central 제품들은 위협 정보를 서로 공유하여 보안 이슈에 자동으로 대응합니다. 다른 어떤 보안 공급업체도 이처럼 긴밀하게 통합된 제품을 제공하지 않습니다. Sophos 제품은 정보와 원격 측정 정보를 실시간으로 공유함으로써 보안 이슈에 자동으로 대응할 수 있습니다. 네트워크 공격 확산 차단을 위하여 감염된 엔드포인트를 분리하며 호환되지 않는 모바일 장치의 Wi-Fi를 제한합니다. 손상된 메일함이 탐지되면 엔드포인트를 검사합니다. 사용자가 액세스하는 모든 앱을 식별하는 것은 사이버 보안 분야에서 가장 큰 판도를 바꾼 것 중 하나입니다.

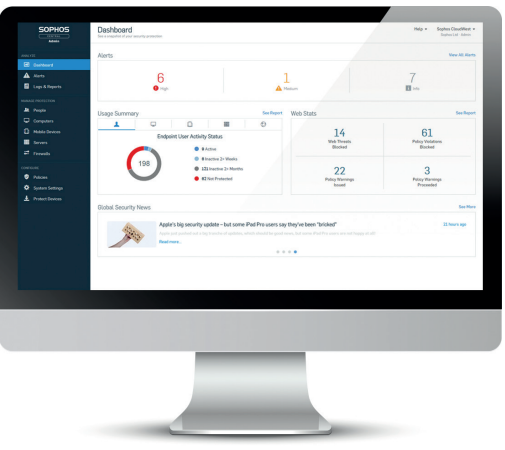
손쉬운 정보 접근

클라우드, 엔드포인트 및 네트워크 전반에 걸친 통합된 관리 콘솔, 강력한 리포팅 기능 및 실시간 데이터를 통해 그 어느 때보다 빠르고 정확하게 대응할 수 있는 실용적인 통찰력을 제공합니다. Sophos Labs Intelix 위협 인텔리전스 및 제품 간 조사는 최고의 보안 결정을 내리는데 필요한 컨텍스트를 제공합니다.

유연한 관리를 통해 비즈니스에 맞게 구축

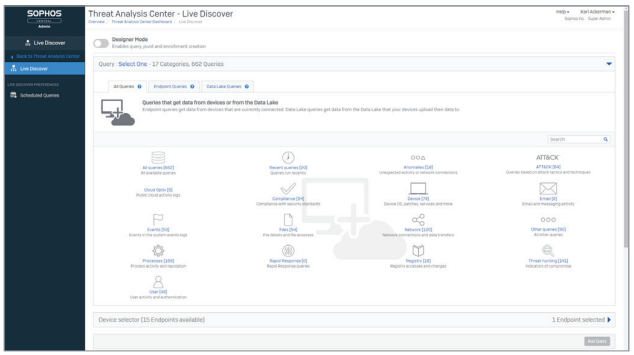
Sophos Central은 소규모 사무실, 대기업 또는 Sophos 파트너에 관계없이 간편한 클라이언트 설정 및 Zero-Touch 방화벽 구축, 사전 정의된 관리, 헬프 데스크 및 리포팅 역할, 네트워크 방화벽에 대한 중앙 백업 관리 및 펌웨어 업데이트 등 모든 것을 한 곳에서 관리하는 데 필요한 모든 기능을 갖추고 있습니다.

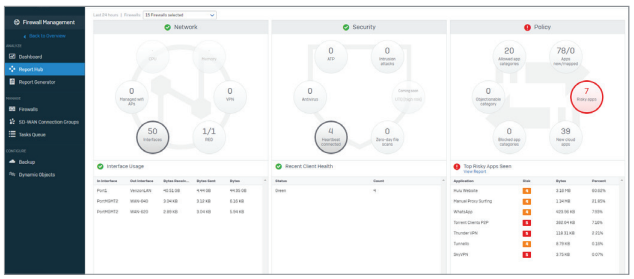
Sophos 파트너는 Sophos Central을 사용하여 비즈니스를 관리하고 동일한 콘솔에서 고객의 보안을 관리할 수 있습니다. Kaseya와의 통합이 준비돼 있어 타사 SIEM, RMM, PSA 및 기타 관리 툴과의 통합을 위한 보안 API를 포함하여 ConnectWise, AutoTask 등을 지원합니다. 또한 Sophos Email, Device Encryption 및 Mobile 사용자는 셀프 서비스 포털을 통해 스팸 이메일을 관리하고 암호화 키를 요청하며 스마트폰을 원격으로 관리할 수 있음으로써 사용자는 자유롭게 다른 작업에 집중할 수 있습니다.



Sophos Cental은 무료인거, 알고 계셨나요?

대부분의 IT 보안 공급업체는 고객들이 클라우드 관리에 추가 비용을 지불하기를 원하지만 우리는 그럴 필요는 없다고 생각합니다. Sophos의 제품은 클라우드용으로 설계되었으며 하이브리드 또는 온프레미스 솔루션에서는 찾아볼 수 없는 최신 기능을 활용합니다. 지금 바로 Sophos Central 제품 체험을 통해 직접 확인해보세요!





Technical Specifications

웹 브라우저와 인터넷 연결만 필요합니다.

- Google Chrome
- Apple Safari
- Microsoft Edge
- Microsoft Internet Explorer 11
- Mozilla Firefox

How to buy

파트너로부터 하나 이상의 Sophos Central 관리 제품을 구입하시기만 하면 됩니다.

Sophos Central Managed Products

Sophos Endpoint
Intercept X

Sophos Firewall
Next-gen Protection

Sophos MTR
Managed Threat Response

Sophos Email

Sophos Web

Sophos CSPM

Sophos Mobile

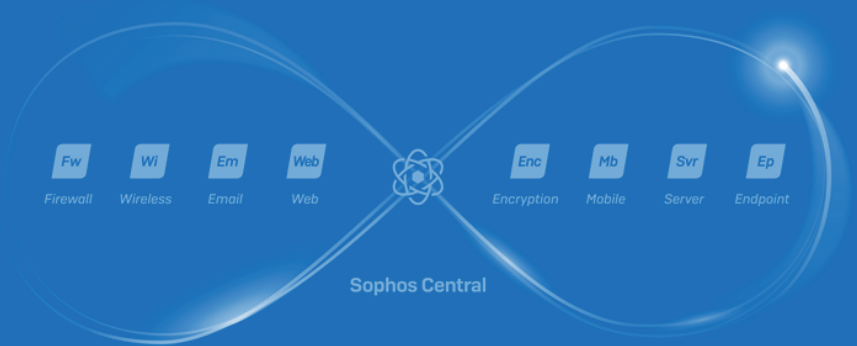
Sophos Wireless

Sophos Phish Threat

Sophos Encryption

Synchronized Security

모든 소포스의 보안 솔루션들이 Security Heartbeat™의 위협 인텔리전스 공유를 통해, 제품 간 탐지된 위협 정보를 커뮤니케이션하며 능동적인 보안 대응을 제공합니다.



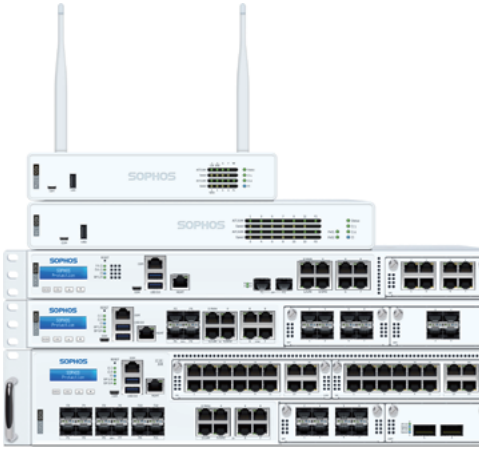
Sophos Firewall

강력한 보호 및 퍼포먼스

Sophos Firewall, 그리고 전용 Xstream Flow Processor를 탑재한 XGS 시리즈 어플라이언스는 궁극의 SaaS, SD-WAN 및 클라우드 애플리케이션 가속, 고성능 TLS Inspection, 그리고 가장 까다로운 네트워크에 대한 강력한 위협 보호를 제공합니다.

Highlights

- 세계 최고 수준의 가시성, 보호 및 대응
- 유연한 배포: 하드웨어, 클라우드, 가상, 소프트웨어
- Sophos의 전체 사이버 보안 솔루션 생태계와 통합
- Security Heartbeat™를 통한 고유의 Synchronized Security
- 추가 비용이 없는 Sophos Central 클라우드 관리
- 풍부한 on-box 및 클라우드 기반 Reporting 포함
- 모듈형 연결성 및 SD-WAN 옵션



Xstream Protection

Sophos Firewall의 Xstream 아키텍처는 최신 위협으로부터 네트워크를 보호하고 중요한 SaaS와 SD-WAN 및 클라우드 애플리케이션 트래픽을 가속합니다.

TLS 1.3 Inspection

빠르고 효과적인 지능형 TLS Inspection으로 방대한 사각지대를 제거합니다. 이 TLS Inspection은 광범위한 예외 사항이 포함된 최신 표준과 마우스 클릭으로 손쉽게 사용 가능한 정책 툴을 지원하여 성능과 프라이버시 및 보호 간 완벽한 밸런스를 제공합니다.

Deep Packet Inspection

차세대 IPS, 웹 보호, 앱 제어를 포함한 고성능 스트리밍 딥 패킷 검사와 딥 러닝 및 SophosLabs Intelix 기반의 샌드박싱으로 최신 해킹과 공격을 즉시 저지합니다.

Application Acceleration

신뢰할 수 있는 SaaS, SD-WAN 트래픽과 VoIP, 비디오 및 기타 미션 크리티컬 애플리케이션과 같은 클라우드 트래픽을 자동으로 또는 사용자 정책을 통해 가속화할 수 있습니다. Xstream Flow Processor를 통해 이러한 트래픽을 FastPath에 배치하여 성능을 최적화하고 심층 검사가 필요한 트래픽에 대한 여유 자원을 늘립니다.

Synchronized Security

Sophos Firewall은 Sophos Intercept X와 긴밀히 통합되어 정보를 공유하고 Security Heartbeat™를 통해 자동으로 대응하는 업계 고유의 제품입니다. 모든 엔드포인트의 상태를 한눈에 확인할 수 있고 위협이 활성화되어 있으면 Sophos Firewall이 이를 격리하기 위한 자동 대응을 수행하여 위협의 확산을 방지합니다. Security Heartbeat™는 또한 사용자와 애플리케이션의 ID를 방화벽과 공유하여 애플리케이션 검색, 정책 컴플라이언스, 성능 및 라우팅을 개선합니다.

Sophos Central Management 및 Reporting

Sophos Central은 최고의 사이버 보안 클라우드 관리 플랫폼으로서, 무료로 손쉽게 이용할 수 있습니다. 그룹 정책 툴을 사용하여 모든 방화벽을 관리하고 클라우드에서 백업 관리, 펌웨어 업데이트 스케줄링 및 Zero-Touch 배포를 수행합니다. 또한 강력한 클라우드 기반 Reporting 툴을 활용하여 네트워크 활동에 대한 깊이 있는 통찰력을 얻을 수 있습니다.

Sophos Firewall XGS Series Appliances

모든 XGS 시리즈 어플라이언스는 TLS 암호화와 딥 패킷 검사를 지원하는 고성능 멀티코어 CPU, 그리고 VoIP, 동영상 및 기타 신뢰할 수 있는 애플리케이션과 같은 실시간 트래픽의 지능형 가속을 위한 전용 Xstream Flow Processor의 이점을 모두 제공합니다.
그 결과, 모든 가격대에서 Xstream 성능을 발휘하여 오늘날의 분산되고 암호화된 다양한 네트워크에 필요한 보호를 제공합니다.

Model		Tech. 스펙			Throughput			
Model	유형	Ports/Slots (Max Ports)	w-model*	Swappable Components	Firewall (Mbps)	IPsec VPN (Mbps)	Threat Protection (Mbps)	Xstream SSL/ TLS (Mbps)
XGS 87(w)	Desktop	5/- (5)	Wi-Fi 5	n/a	3,700	750	240	375
XGS 107(w)	Desktop	9/- (9)	Wi-Fi 5	Second power supply	7,000	900	330	420
XGS 116(w)	Desktop	9/1 (9)	Wi-Fi 5	Second power supply, 3G/4G, Wi-Fi**	7,700	1,100	685	650
XGS 126(w)	Desktop	14/1 (14)	Wi-Fi 5	Second power supply, 3G/4G, Wi-Fi**	10,500	1,800	900	800
XGS 136(w)	Desktop	14/1 (14)	Wi-Fi 5	Second power supply, 3G/4G, Wi-Fi**	11,500	2,500	1,000	950
XGS 2100	1U	10/1 (18)	n/a	Option)외부 전원	30,000	3,000	1,250	1,100
XGS 2300	1U	10/1 (18)	n/a	Option)외부 전원	35,000	3,500	1,400	1,450
XGS 3100	1U	12/1 (20)	n/a	Option)외부 전원	38,000	5,200	2,000	2,470
XGS 3300	1U	12/1 (20)	n/a	Option)외부 전원	40,000	6,500	2,770	3,130
XGS 4300	1U	12/2 (28)	n/a	Option)외부 전원	75,000	9,800	4,800	8,000
XGS 4500	1U	12/2 (28)	n/a	Option)외부 전원	80,000	16,000	8,390	10,600
XGS 5500	2U	16/3 (48)	n/a	Power, SSD, Fan	100,000	21,600	12,390	13,500
XGS 6500	2U	20/4 (68)	n/a	Power, SSD, Fan	115,000	26,000	17,050	16,000

* 802.11ac
** XGS 116w, 126w 및 136w 전용 2차 Wi-Fi 모듈 옵션

Xstream Protection Bundle 라이센스

Sophos Firewall의 Xstream Protection Bundle은 매우 높은 보안 수준을 요구하는 네트워크를 운영하는 데 필요한 모든 차세대 보호 기능과 성능 및 가치를 제공합니다.

Xstream Protection Bundle 라이센스

BASE LICENSE	네트워킹, 무선, Xstream 아키텍처, 무제한 원격 액세스 VPN, site-to-site VPN, 상세 리포팅
NETWORK PROTECTION	Xstream TLS 및 DPI 엔진, IPS, ATP, Security Heartbeat™, SD-RED VPN, 상세 리포팅
WEB PROTECTION	Xstream TLS 및 DPI 엔진, 웹 보안 및 제어, 애플리케이션 제어, 상세 리포팅
ZERO-DAY PROTECTION	머신러닝 및 샌드박싱 파일 분석, 상세 리포팅
CENTRAL ORCHESTRATION	SD-WAN VPN 오케스트레이션, Central Firewall Reporting Advanced(30일), MTR/XDR-ready
ENHANCED SUPPORT	연중무휴 지원, 기능 업데이트, 해당 기간 하드웨어 교체 보증

성능 시험 방법은 sophos.com/compare-xgs를 참조하세요.

Sophos MTR

Managed Threat Response (전문가 주도의 위협 대응)

Sophos MTR(Managed Threat Response)은 완전한 매니지드 서비스로 보안 전문가팀이 제공하는 연중무휴 위협 헌팅, 탐지 및 대응 기능을 제공합니다.

Highlights

- 완전한 매니지드 서비스로 제공되는 지능형 위협 탐지 및 대응 기능
- 연중무휴 대응 팀이 위협을 원격으로 억제하고 무력화를 위해 조치와 협력
- MTR 팀이 직접 조치를 취하고 보안 사고를 관리하는 방법을 결정 및 제어 가능
- 고도로 훈련된 전문가 팀과 최고 수준의 머신러닝 기술
- 사내 보안 단계에 따라 2가지 서비스 계층 (Standard 및 Advanced)의 포괄적인 서비스 기능 선택 가능

위협 알림은 해결책이 아닙니다. - 보안의 시작입니다.

새로운 위협으로부터 사전 예방 및 24시간 보안 프로그램을 통한 방어를 효과적으로 관리할 수 있는 적절한 도구, 인력 및 프로세스를 사내에 보유한 조직은 거의 없습니다. Sophos MTR 팀은 단순히 공격이나 의심스러운 행동을 알리는 것 이상으로 가장 정교하고 복잡한 위협을 무력화하기 위해 사용자를 대신하여 표적 조치를 취합니다.

보호가 필요한 사내 조직은 Sophos MTR을 통해 아래와 같은 보안 행위를 수행할 위협 대응 보안 전문가로 구성된 연중무휴 24시간 팀으로 무장합니다.

- 잠재적인 위협 및 사고를 사전에 추적하고 검증합니다.
- 사용 가능한 모든 정보를 사용하여 위협의 범위 및 심각도를 결정합니다.
- 유효한 위협에 적합한 비즈니스 컨텍스트를 적용합니다.
- 위협을 원격으로 중단, 억제 및 무력화하는 작업을 시작합니다.
- 반복적인 위협과 근본 원인을 해결하기 위한 조치 및 조언을 제공합니다.

전문가 대응을 통한 보안 기능 향상

Intercept X Advanced with XDR 기술을 기반으로 구축된 Sophos MTR은 머신러닝 기술과 전문가 분석을 결합하여 위협 헌팅 및 탐지 개선, 경보에 대한 심층 조사, 표적 조치를 통해 빠르고 정확하게 위협을 제거합니다. 계속해서 최고 등급으로 평가되는 Sophos의 엔드포인트 보호 및 지능형 XDR과 세계적 수준의 보안 전문가팀이 결합하여 "전문가 대응을 통한 보안 기능 향상"이 이루어집니다.

투명하고 완벽한 통제

Sophos MTR을 사용하면 의사결정을 직접 내릴 수 있으며 잠재적인 사건이 확대되는 방법과 시기, 당사가 취할 대응 조치 (있는 경우) 및 커뮤니케이션에 포함할 사용자를 지정할 수 있습니다. Sophos MTR은 세 가지 대응 모드를 갖추고 있으며, MTR 팀이 사고 발생 시 함께 작업할 수 있는 최선의 방법을 선택할 수 있습니다.

알림[Notify]: 탐지에 대해 알리고 우선순위 지정 및 대응에 도움이 되는 세부 정보를 제공합니다.

협업[Collaborate]: 탐지에 대응하기 위해 내부 팀 또는 외부 담당자와 협력합니다.

권한 부여[Authorize]: 격리 및 무력화 처리 후 취해진 조치를 리포팅합니다.

Sophos MTR 서비스 레벨

Sophos MTR은 두 가지 서비스 계층 (Standard 및 Advanced)을 제공하며 모든 규모와 조직의 보안 수준에 따라 포괄적인 기능 세트를 제공합니다. 선택한 서비스 계층과 관계없이 요구 사항에 따라 세 가지 응답 모드 (알림, 협업 또는 권한 부여) 중 하나를 활용할 수 있습니다.

Sophos MTR : Standard

24/7 Lead-Driven (리드 기반) 위협 헌팅

확인된 악성 아티팩트 및 활동 (강력한 신호)은 자동으로 차단되거나 종료되어 보안 전문가가 직접 위협 헌팅을 수행할 수 있도록 합니다. 이러한 유형의 위협 헌팅은 이전에는 탐지할 수 없었던 새로운 공격 지표 (IoA) 및 타협 지표 (IoC)를 발견하기 위해 인과 관계 이벤트 (취약 신호)에 따라 집계 및 조사가 진행됩니다.

Activity Reporting

CASE 활동 요약을 통해 사내 탐지된 위협과 각 보고 기간 내에 수행된 대응 조치를 파악할 수 있습니다.

Security Health Check

Intercept X Advanced with XDR을 기반으로 Sophos Central을 통한 통합 관리 및 각 제품의 작동 상태를 사전에 검사하고 권장되는 구성 개선 사항을 통해 최고 성능으로 작동하도록 할 수 있습니다.

Adversarial Detections

대부분의 성공적인 공격은 탐지 도구에 합법적으로 보일 수 있는 프로세스의 실행에 의존합니다. MTR 팀은 독자적인 조사 기술을 사용하여 합법적인 행동과 공격자가 사용하는 TTP (전술, 기술 및 절차) 간의 차이점을 확인합니다.

Sophos MTR : Advanced 모든 Standard 기능과 다음 기능을 포함합니다.

24/7 Leadless (무단서) 위협 헌팅

데이터 과학, 위협 인텔리전스 및 최고의 전문 위협 전문가의 직관으로 회사 프로필, 고가치 자산 및 고위험 사용자를 선별 및 결합하여 공격자 행동을 예측하고 새로운 공격 지표 (IoA)를 식별합니다.

Dedicated Threat Response Lead

장애가 확인되면 활성 위협이 무력화될 때까지 사내 리소스 (내부 팀 또는 외부 파트너)와 직접 협업할 수 있는 전용 위협 대응 리드가 제공됩니다.

Enhanced Telemetry

위협 조사는 엔드포인트 기본 기능 외에도 확장된 다른 Sophos Central 내 관리되는 제품을 통한 원격 분석으로 공 격자 활동에 대한 전체적인 그림을 제공하고 보완합니다.

Direct Call-In Support

귀하의 팀은 SOC (Security Operations Center)에 직접 문의할 수 있습니다. MTR 운영팀은 24시간 이용할 수 있으며, 전 세계 26개 지역에 걸친 지원팀의 지원을 받고 있습니다.

Proactive Posture Improvement

전체 보안 기능을 저하하는 구성 및 아키텍처 약점을 해결하기 위한 규범적인 지침을 통해 보안 상태를 능동적으로 개선하고 방어를 강화할 수 있습니다.

Asset Discovery

OS 버전, 애플리케이션, 취약성을 다루는 자산 정보에서 관리되는 자산과 관리되지 않는 자산 식별에 이르기까지 영향 평가, 위협 추적 및 사전 예방적 상태 개선 권장 사항을 통해 귀중한 통찰력을 제공합니다.

Intercept X

Intercept X Advanced, Intercept X Advanced with XDR, Intercept X Advanced with MTR

Sophos Intercept X는 세계 최고의 엔드포인트 보호를 제공합니다. 딥 러닝 AI, 안티 랜섬웨어 기능, 익스플로잇 차단 등의 조합으로 최신 사이버 보안 위협을 차단합니다.

Sophos Intercept X는 단순히 하나의 기본 보안 기술에 의존하는 것이 아닌, 포괄적이고 심층적으로 엔드포인트 보호에 접근하는 방식을 사용합니다. 이러한 계층화된 접근 방식은 최신 기술과 기존 기술을 결합하여 가장 광범위한 위협을 차단합니다.

Highlights

- 딥 러닝 AI로 이전에 본 적이 없는 위협 차단
- 랜섬웨어를 차단하고 영향을 받는 파일을 안전한 상태로 복원
- 공격 체인 전체에서 사용되는 취약점 악용 기술 차단
- EDR을 사용하여 중요한 IT 운영 및 위협 추적 관련 질문에 대한 답변 제공
- 완전 관리형 서비스로 연중무휴 24시간 보안 제공
- XDR을 사용해 방화벽, 이메일 및 기타 데이터 소스 확인 및 활용
- 원격 작업 환경에서도 쉽게 배포, 구성 및 유지 관리

알려지지 않은 위협 차단

Intercept X의 딥 러닝 AI는 이전에 본 적이 없는 멀웨어를 감지하고 차단하는데 탁월합니다. 시그니처 없이 위협을 식별하기 위해 수억 개의 샘플에서 파일 속성을 조사하여 이를 수행합니다.

랜섬웨어 차단

차세대 IPS, 웹 보호, 앱 제어를 포함한 고성능 스트리밍 딥 패킷 검사와 딥 러닝 SophosLabs Intelix 기반의 샌드박싱으로 최신 해킹과 공격을 즉시 저지합니다.

취약점 악용 차단

취약점 악용 방지 기술은 공격자가 기기를 손상하고, 자격 증명을 도용하고, 멀웨어를 배포하는 데 사용하는 취약점 악용 기술을 차단합니다. Intercept X는 공격 체인 전체에서 사용되는 기술을 차단함으로써 파일리스 공격과 제로데이 취약점 악용으로부터 조직을 안전하게 보호합니다.

계층화된 방어

Intercept X는 강력한 차세대 기능 외에, 입증된 기존의 보안 기술도 활용합니다. 예를 들어, 애플리케이션 Lockdown, 웹 제어, 데이터 손실 방지 및 시그니쳐 기반 멀웨어 탐지 기능이 있습니다. 이렇게 차세대 기술과 기존 보안 기술을 조합하여, 공격 지점을 줄이고 최고의 심층 방어를 가능하게 합니다.

Synchronized Security

다른 Sophos 솔루션을 함께 사용하면 더 효과적입니다. 예를 들어, Intercept X 및 Sophos 차세대 방화벽은 서로 보안 인텔리전스를 공유하여, 멀웨어 차단을 진행하는 동안 손상된 디바이스를 자동으로 격리하고, 이후 해당 위협이 제거되면 네트워크 접속을 다시 허용합니다. 관리자 개입 없이 모든 것이 이루어집니다.

엔드포인트 탐지 및 대응

IT 관리자와 사이버 보안 전문가를 위해 설계된 Sophos EDR은 중요한 IT 운영 및 위협 추적 관련 질문에 대한 답변을 제공합니다. 예를 들어, 성능 문제가 있거나 비표준 포트에서 연결을 시도하는 의심스러운 프로세스가 있는 기기를 식별한 다음, 기기에 원격으로 액세스하여 수정 조치를 취합니다.

관리형 위협 대응 (MTR)

Sophos 전문가 팀이 연중무휴 24시간 위협 추적 감지 및 대응 서비스를 제공합니다. Sophos 분석가는 잠재적 위협에 대응하고, 침해 지표를 찾고, 무슨 일이 어디서, 언제, 어떻게, 왜 일어났는지를 포함하여 이벤트에 대한 자세한 분석을 제공합니다.

확장된 탐지 및 대응 (XDR)

엔드포인트와 서버를 넘어 방화벽, 이메일 및 기타 데이터 소스를 가져옵니다*.상세한 세부정보로 드릴다운하는 기능을 통해 조직의 사이버 보안 상태를 전체적으로 파악할 수 있습니다. 예를 들어, 사무실 네트워크 문제와 이러한 문제를 일으키는 애플리케이션을 이해합니다.

*Sophos Cloud Optix 및 Sophos Mobile XDR 출시 예정

직관적인 관리

Intercept X는 모든 Sophos 솔루션을 위한 클라우드 관리 플랫폼인 Sophos Central을 통해 관리됩니다. Sophos Central은 모든 기기와 제품을 위한 단 하나의 관리 콘솔이므로 원격 작업 설정에서도 환경을 쉽게 배포, 구성 및 관리할 수 있습니다.

기술 사양

Intercept X는 Windows 및 macOS 배포를 지원합니다.최신 정보는 Windows 시스템 요구사항 및 Mac 데이터시트를 참조하십시오.

Licensing Overview

Features	Intercept X Advanced	Intercept X Advanced with XDR	Intercept X Advanced with MTR Standard	Intercept X Advanced with MTR Advanced
기본 보호기능 (앱제어, 행동 감지 포함)	✓	✓	✓	✓
차세대 보호 기능 (딥러닝, 랜섬웨어 방지, 파일리스 공격 보호 등 포함)	✓	✓	✓	✓
EDR / XDR (엔드포인트 및 확장된 네트워크 감지 및 대응)		✓	✓	✓
관리형 위협 대응 (MTR – 연중무휴 24시간 공격 추적 및 대응 서비스)			✓	✓
Advanced 관리형 위협 대응 (리드리스 추적(leadless hunting, 전담 연락 담당자 등)				✓

Intercept X for Server

Intercept X Advanced for Server
Intercept X Advanced for Server with XDR
Intercept X Advanced for Server with MTR

Sophos Intercept X for Server 는 최신 사이버 보안 위협으로부터 클라우드, 사내 및 가상 서버를 보호합니다.

Sophos Intercept X for Server는 서버 보안에 대한 포괄적이고 심층적인 접근 방식을 사용합니다. 강력한 방어 기술과 가시성 기능의 조합은 조직의 최신 위협에 대한 최상의 보호 기능을 제공합니다.

Highlights

- 클라우드, 사내 및 가상 서버 구축 보안
- 딥 러닝 AI로 이전에 본 적이 없는 위협 차단
- 랜섬웨어를 차단하고 영향을 받는 파일을 안전한 상태로 복원
- 공격 체인 전체에서 사용되는 취약점 악용 기술 차단
- XDR을 사용하여 중요한 IT 운영 및 위협 추적 관련 질문에 대한 답변 제공
- 방화벽, 이메일 및 기타 데이터소스 확인 및 활용*
- S3 버킷 및 데이터베이스과 같은 광범위한 클라우드 환경 이해 및 보호
- 완전 관리형 서비스로 연중무휴 24시간 보안 제공

*Sophos Mobile XDR 통합 예정

알려지지 않은 위협 차단

Intercept X for Server의 딥 러닝 AI는 이전에 본 적이 없는 멀웨어를 감지하고 차단하는 데 탁월합니다. 시그니쳐 없이 위협을 식별하기 위해 수억 개의 샘플에서 파일 속성을 조사하여 이를 수행합니다.

랜섬웨어 차단

Intercept X에는 랜섬웨어 공격에 사용되는 악성 암호화 프로세스를 감지하고 차단하는 지능형 랜섬웨어 방지 기능이 포함되어 있습니다. 암호화된 파일은 안전한 상태로 롤백되어 비즈니스에 미치는 영향을 최소화합니다.

계층화된 방어

Intercept X는 강력한 차세대 기능 외에, 입증된 기존의 보안 기술도 활용합니다. 예를 들어, 애플리케이션 Lockdown, 웹 제어, 데이터 손실 방지 (DLP) 및 시그니쳐 기반 멀웨어 탐지 기능이 있습니다. 차세대 기술과 기존 보안 기술을 조합하여, 공격 지점을 줄이고 최고의 심층 방어를 가능하게 합니다.

서버 제어

서버 Lockdown (어플리케이션 화이트리스팅)은 사용자가 승인한 응용프로그램만 서버에서 실행될 수 있도록 합니다. 중요한 파일을 변경하려는 무단 시도가 있을 경우 파일 무결성 모니터링에서 사용자에게 알립니다.

광범위한 클라우드 환경 확인

전체 멀티 클라우드 인벤토리를 이해하고 보호합니다. 클라우드 워크로드는 물론 S3 버킷, 데이터베이스 및 서버리스 기능을 비롯한 중요한 클라우드 서비스를 탐지하고 의심스러운 활동을 식별하며 안전하지 않은 배포를 찾아내고 보안 격차를 좁힐 수 있습니다.

Sophos Intercept X for Server

확장된 감지 및 대응 (XDR)

Sophos XDR은 조직에 중요한 위협 추적 및 IT 운영 질문에 신속하게 답변할 수 있는 도구를 제공합니다. 엔드포인트 및 서버 외에도 네트워크, 이메일, 클라우드 및 모바일 데이터*를 통합하여 기존의 EDR (Endpoint Detection and Response)을 뛰어넘습니다. 예를 들어 활성 RDP 세션이 있는 서버를 식별하거나 클라우드 보안 그룹을 분석하여 공용 인터넷에 노출된 리소스를 식별합니다.

*Sophos Mobile XDR 통합 예정

매니지드 위협 탐지 서비스 (MTR)

Sophos 전문가 팀이 365일 연중무휴 24x7 위협 탐지 및 대응 서비스를 제공합니다. Sophos 분석가는 잠재적 위협에 대응하고, 침해 지표를 찾으며, 발생 내용, 장소, 방법 및 이유 등 자세한 분석을 제공합니다.

AI 및 전문가 기반 데이터

딥러닝 AI와 SophosLabs 전문가의 사이버 보안 지식을 결합한 Intercept X for Server는 업계 최고의 위협 인텔리전스로 조직에 두 가지 장점을 모두 제공합니다.

간편한 관리

Intercept X for Server는 모든 Sophos 솔루션의 클라우드 관리 플랫폼인 Sophos Central을 통해 관리됩니다. 모든 서버, 장치 및 제품을 위한 단일 콘솔을 통해 클라우드, 사내, 가상 및 혼합 구현에서 쉽게 배포, 구성 및 관리할 수 있습니다.

Features	Intercept X Advanced for Server	Intercept X Advanced for server with XDR	Intercept X Advanced for Server with MTR Advanced
기본 보호 기능 (앱제어, 행동 감지 포함)	✓	✓	✓
차세대 보호 기능 (딥러닝, 랜섬웨어 방지, 파일리스 공격 보호 등 포함)	✓	✓	✓
서버 제어 (서버 잠금, 파일 무결성 모니터링 등)	✓	✓	✓
CSPM (Cloud Security Posture Management) (광범위한 클라우드 환경 확인 및 보호)	✓	✓	✓
EDR / XDR (엔드포인트 및 확장된 네트워크 감지 및 대응)		✓	✓
매니지드 위협 탐지 서비스 (MTR - 연중무휴 24x7 위협 추적 및 대응 서비스)			✓

Sophos Phish Threat

피싱은 기업이 직면한 가장 큰 문제점입니다.

공격자들은 스팸, 피싱 및 지능형 사회 공학 공격으로 조직을 끊임없이 공격합니다.
IT 전문가의 41%는 최소한 매일 피싱 공격을 보고합니다.
일반 사용자는 종종 사이버 방어에서 쉬운 표적이자 가장 약한 연결점입니다.
효과적인 피싱 시뮬레이션, 자동화된 교육 및 Sophos Phish Threat의 포괄적인 보고서를 통해 사용자와 비즈니스를 안전하게 보호하십시오.

Highlights

- 500개 이상의 이메일 위협 템플릿 및 60개 이상의 관련 교육 모듈
- PC 및 Mac용 Outlook 추가 기능을 사용한 모의 공격 보고서
- 피싱 및 트레이닝 결과에 대한 자동화된 보고서 제공
- 10개의 언어 지원
- 다수의 국제 호스팅 지역 선택 (미국, 영국, 독일)

사이버 보안에서 가장 중요한 이메일 훈련 및 교육

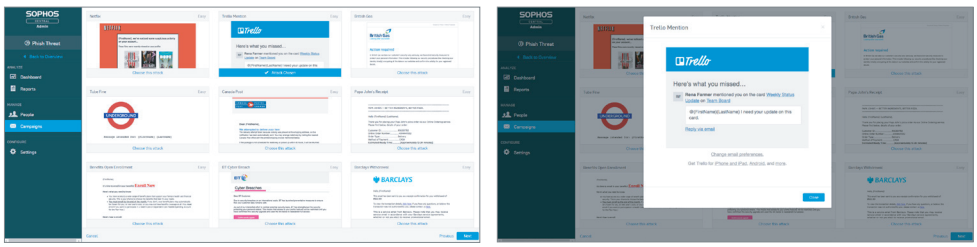
공격자에게 피싱은 큰 비지니스입니다. 피싱 공격은 최근 몇 년 동안 기록적인 성장을 보여 주었습니다. 현재 악성 이메일의 66%가 악성 이메일 첨부 파일을 통해 설치되고 지능형 스피어 피싱 공격으로 인해 기업에 사고당 평균 1억 7천만원이 소요됩니다.
대부분 조직의 사이버 보안에서, 일반적인 사용자는 공격자의 가장 쉬운 표적이 되고 있습니다. 허나, 훈련을 받고 피싱을 인식하는 직원으로 구성된 조직은 이러한 위협에 대한 방어를 제공할 수 있습니다.

Sophos Phish Threat은 다양한 피싱, 첨부파일, 계정탈취 등의 공격 유형들을 직접 임직원들에게 훈련시키고 맞춤형 교육 프로그램을 제공하여 피싱 인식, 이메일 보안 등에 대한 사용자 인식을 효과적으로 높여줍니다.

실제 공격 템플릿 및 커스터마이징 제공

클릭 몇 번으로 500개 이상의 현실에서 사용되는 매우 까다로운 피싱 공격을 시뮬레이션할 수 있습니다. Sophos의 글로벌 SophosLabs 분석가들은 매일 수백만 개의 이메일, URL, 파일 및 기타 데이터 지점에서 최신 위협을 모니터링합니다.
이러한 지속적인 인텔리전스 흐름을 통해 사용자 교육이 사회적으로 관련된 공격 시뮬레이션 템플릿을 사용하여 여러 시나리오를 다루며 10개 언어로 번역된 현재의 피싱 전술을 다룰 수 있습니다.

- 한국어
- 영어
- 중국어
- 독일어
- 일본어
- 스페인어
- 프랑스어
- 이탈리아어
- 포르투칼어



Access a continually growing library of international templates from beginner to expert

효과적인 교육 프로그램

60개 이상의 대화형 교육 모듈은 의심스러운 이메일, 자격 증명 수집, 암호 강도 및 규정 준수와 같은 특정 위협에 대해 사용자를 교육합니다. 10개 언어를 제공하여 훈련 대상자는 유용한 정보를 얻을 수 있으며, 보안 담당자는 향후 실제 공격에 대해 안심할 수 있습니다.

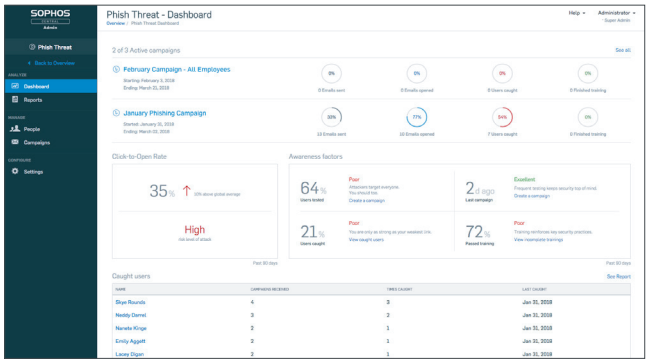
대화형 교육 프로그램을 제공하세요.

다양한 리포팅

직관적인 대시보드 온디맨드 결과를 통해 조직의 보안 상태를 이해하고 실제 훈련을 통해 보안 결과를 확인하세요. Phish Threat 대시보드는 사용자 취약성에 대한 캠페인 결과를 한눈에 제공하고 다음을 포함한 실시간 보안 인식 수준 데이터를 사용하여 전체 사용자 그룹의 전반적인 위험도를 측정할 수 있습니다.

- 가장 높은 수준의 캠페인 결과치
- 조직 내 피싱에 속은 사용자 및 피싱 신고자 트렌드
- 탐지된 총 사용자 수
- 테스트 범위
- 마지막 캠페인 이후 일 수

드릴 다운 보고서는 조직 혹은 개별 사용자의 성과에 대한 더 깊은 통찰력을 제공합니다. 포함된 Outlook 추가 기능은 받은 편지함에서 바로 시뮬레이션된 공격을 보고할 수 있는 기능을 제공하여 받은 편지함에서 실제 보안 인식 수준을 추적하고 조직 전체의 보안 상태에 대한 새로운 통찰력을 제공합니다.



대쉬보드에서 제공하는 전반적인 위험 수준. 사용자별 데이터를 측정합니다.

Sophos Central 환경에서의 구현

Phish Threat은 클라우드 기반 통합 보안 콘솔인 Sophos Central의 일부이며, 단 하나의 창에서 모든 솔루션을 관리할 수 있습니다. 즉, 하드웨어나 소프트웨어를 설치할 필요가 없으며 이메일, 엔드포인트, 모바일 등에 대한 보안과 함께 피싱 시뮬레이션 및 사용자 교육을 관리할 수 있는 유일한 솔루션의 이점을 누릴 수 있습니다. 매우 간단하고 직관적인 Sophos Central 플랫폼을 무료로 사용하세요.

손쉬운 시작

Sophos Phish Threat은 웹 브라우저 전체를 통해 편리하게 실행됩니다. Phish Threat 이메일이 성공적으로 전달되도록 하려면 Sophos Central 콘솔에 제공된 IP 주소와 Phish Threat 캠페인에 사용된 이메일 주소 및 도메인을 화이트리스트로 지정하기만 하면 됩니다. 이후 CSV 파일이나 편리한 Active Directory 동기화 도구를 사용하여 사용자를 가져오면 됩니다. 사용자가 업로드되면 첫 번째 캠페인을 보낼 준비가 된 것입니다.

구매 방법

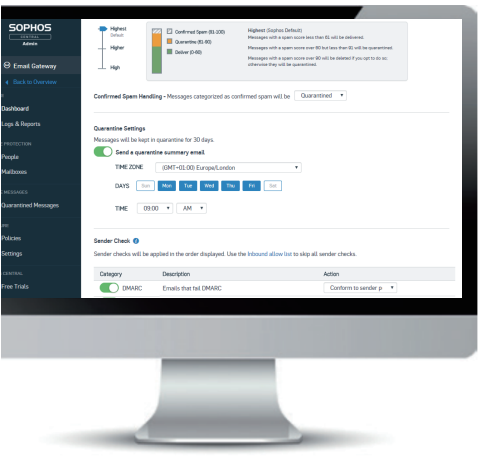
1~5,000개 이상의 대역으로 사용자당 가격이 책정된 Sophos Phish Threat의 단일 라이선스 유형은 사용자당 무제한 테스트를 제공하므로, 오늘날의 지능형 피싱 공격으로부터 사용자와 비즈니스를 안전하게 보호하는 데 집중할 수 있습니다.

Sophos Central Email

인공지능에 기반한 클라우드 이메일 보안시스템인 Sophos Email은 Sophos Central의 쉬운 단일 관리 콘솔을 통해 이용가능한 이메일 보안 솔루션 입니다. 최신 인공지능 기술을 이용하여 악성 이메일 위협으로 부터 조직을 보호하세요.

Highlights

- 선제적 이메일 방어로 Known 및 Unknown 위협 차단 가능
- 랜섬웨어, 스팸 및 피싱 공격 차단
- 이메일 암호화와 데이터 유출 방지 기능을 통한 민감 데이터 보호
- M365 모든 주요 플랫폼 지원
- Active Directory 자동 동기화
- Self- Service 포탈을 이용한 사용자 및 관리자 제어



지능형 이메일 보안

최근의 이메일 위협은 더 빠르게 변화하고 있으며, 악성파일들은 점점 더 정상 파일처럼 보입니다. 성장하는 기업은 기업의 미래를 위협하는 현재의 위협을 차단하는 예측 가능한 이메일 보안 시스템이 필요합니다.

최신 기술이 포함된 이메일 보안

많은 수상 경력을 자랑하는 Intercept X와 동일한 기술을 사용하는 Sophos Email의 Sandstorm sandboxing 기능은 내장된 인공지능의 딥러닝 신경망 기술을 이용하여 실시간 위협, 멀웨어 및 원치 않는 응용프로그램을 포함하는 의심스러운 페이로드는 물론, 랜섬웨어를 비롯한 문서에 내장된 높은 수준의 위협을 탐지할 수 있습니다.

Sophos Sandstorm은 이러한 파일들을 실제 사용자 환경과 동일한 가상 머신에서 실행시켜 동작을 모니터링 하고 시뮬레이션 합니다. 단순히 PDF의 변환이 아니라 안전한 문서를 전달합니다.

랜섬웨어 방지

Sophos의 Email Security는 업계에서 가장 앞선 지능형 랜섬웨어 방지 기술을 활용합니다. 이는 행위 분석 기술을 통해 완전히 새로운 랜섬웨어와 부트 레코드 공격을 차단합니다.

숨겨진 공격 방어 - 메일 내 URL 보호

악성 웹 사이트 링크로부터 직원을 보호하는 Sophos의 지능형 URL 보호 기능은 이메일이 전달될 때까지 악성 파일의 업로드를 지연시켜 기존의 이메일 게이트웨이를 우회하는 공격을 방어할 수 있습니다. Sophos Time-of-Click은 이메일 전송 전 그리고 URL 클릭 시점에 웹사이트 평판을 검사하여 숨겨지거나 지연된 공격을 차단할 수 있습니다.

신뢰할 수 있는 메일 박스

Sophos의 다계층 접근 방식은 BEC (Business Email Compromise)를 포함한 피싱 공격을 정확하고 적극적으로 차단합니다. Sophos의 최첨단 NLP (Natural Language Processing -자연어 처리)는 콘텐츠 및 발신자 인증으로 표적화된 스피어 피싱 이메일을 탐지합니다. 최첨단 NLP (Natural Language Processing) AI 모델 활용하여 Sophos 이메일은 '긴급'이나 '요청'과 같은 개념들을 개별적으로 추출하지 않고 문맥에 맞는 단어를 이해할 수 있습니다.

피싱 사기 방어는 SPF, DKIM 및 DMARC 인증 기술, 헤더 이상 분석, 발신자명 및 도메인 확인의 조합을 이용합니다. 이 조합을 통해 사용자는 피싱을 방지하면서 적합한 이메일을 식별하고 허용할 수 있으므로 받은 편지함을 다시 신뢰할 수 있습니다.

유연한 관리 기능

Sophos Email은 유연함을 가지고 있습니다. 개인, 그룹 또는 전체 도메인에 대한 개별 보안정책을 쉽게 만들 수 있기 때문에 정책을 관리하는데 드는 당신의 소중한 시간을 절약할 수 있습니다.

Microsoft Office 365, Google G Suite, 사내 Exchange 2003+ 및 더 많은 전자 메일 공급자와 완벽하게 통합되므로 도메인 및 DNS 레코드를 제어하는 모든 이메일 서비스를 보호할 수 있습니다.

Office 365 보호

이메일, 오피스 및 공동작업을 위해 이용하는 비지니스 이메일을 위한 해결책 - MS Office365는 비지니스 생산성을 유지하는데 유용한 도구입니다. 하지만 고객이 Office365로 전환하였을 때 보안 기능은 기대만큼 만족스럽지 않을 수 있습니다.

높은 수준의 작업을 위해서는 안전한 보안이 필요하며 Sophos Email은 간단한 솔루션을 제공합니다.

- 단일 어드벤스 라이선스는 Office365를 최신 스팸, 피싱 및 지능형 위협으로부터 보호합니다.
- 이메일 검사 및 샌드박스 분석을 위한 위치 선택에 대한 규정 준수 보장
- 쉬운 단일 관리 콘솔 제공

민감한 데이터 보호

Sophos Email 푸시 기반 암호화 및 DLP를 통해 민감한 데이터를 보호하고 규정을 쉽게 준수하십시오.

콘텐츠 제어

모든 이메일 및 첨부 파일에서 재무, 기밀 콘텐츠, 건강 정보 및 PII를 검색하여 중요한 정보를 보호하십시오.

- 원활한 암호화 통합을 통해 그룹 및 개별 사용자를 위한 다중 규칙 정책을 포함한 데이터 침해 방지 정책의 세부적인 제어
- Sophos Content Control List를 사용하여 사용자 정의 CCL을 만들거나 특정 CCL에 대해 즉시 사용자 정의
- 차세대 엔드포인트 보호 기능과 함께 전자 메일에 대한 데이터 손실 방지 (DLP) 관리

이메일 암호화

민감한 데이터를 보호하고 규정을 쉽게 준수합니다.
Sophos Email 푸시 기반 암호화는 메시지 본문 및 첨부 파일에서 민감한 데이터를 자동으로 검색하여 몇 번의 클릭만으로 메시지를 차단하거나 암호화하는 정책을 쉽게 수립할 수 있습니다.
또는 사용자에게 M365 추가 기능으로 전자 메일을 직접 암호화할 수 있는 옵션을 제공합니다.

통합 리포팅

Sophos Email은 Sophos Central 콘솔 내의 통계 보고서를 표 및 그래프 형식으로 제공하며, 모든 사용자 지정 날짜 범위를 선택할 수 있습니다. 이러한 보고서에는 다음이 포함됩니다.

- 메시지 기록 (메시지 삭제, 검역, 처리, 전송 성공, 실패 및 메일 큐에 대기)
- 메시지 세부 정보 (발신자/수신자 정보, 상태, 원본 헤더 세부 정보 및 첨부 파일)
- 메시지 요약 (메시지 방향, # 스캔됨, # 합법적, # 스팸, # 바이러스, # DLP 정책 위반, # 지능형 위협, # RBL 실시간 차단 목록, # 회사 차단 목록, # 인증 실패)
- 샌드박스에 의해 분석된 메시지 양 (Sophos Sandstorm)
- Time-of-Click 보호 URL 보호 (스캔된 상위 100개 URL)

Sophos Email 기능

Protection and Management	Email Advanced
Inbound Message Scanning	✓
Outbound Message Scanning	✓
Domain / Group / User Policies	✓
Admin and User Quarantine	✓
Admin Allow / Block Lists	✓
AD Sync or Azure AD Sync	✓
24/7 Emergency Inbox	✓
Sophos Sandstorm Locations (U.K., Germany, USA)	✓
Anti Spam Filters	✓
Inbound SPF, DKIM and DMARC	✓
Display Name and Lookalike Domain Analysis	✓
BEC Protection	✓
Anti Virus Filters	✓
Time-of-Click URL Protection	✓
Sophos Sandstorm	✓
Push-based Email Encryption	✓
Enforced TLS encryption	✓
Data Loss Prevention	✓
Content control policies (keyword and file types)	✓
Reporting dashboard and detailed reports	✓
Role-based access via Sophos Central	✓

Sophos ZTNA

Zero Trust Network Access

언제 어디서나 모든 애플리케이션에 안전하게 연결할 수 있습니다.
Sophos ZTNA는 투명하게 사용자들을 중요한 비즈니스 애플리케이션 및 데이터에 연결하여 기존의 원격 액세스 VPN에 비해 향상된 세분화, 보안 및 가시성을 제공합니다.
Sophos ZTNA는 단독 제품으로 사용하거나 소포스 제품에 통합된 동기화된 보안 (Synchronized Security) 솔루션으로서, Sophos Firewall및 Intercept X와 함께 사용할 수 있습니다.

Highlights

- Zero trust: 아무것도 믿지 않고, 모든 것을 확인
- Sophos Intercept X와 통합
- 단일 에이전트, 단일 콘솔 솔루션
- VPN을 대체하는 더 강력한 원격 보안 솔루션
- 마이크로 세그먼트와 네트워크 애플리케이션 보호
- 네트워크 상태에 영향 없이 어디서나 접근 가능
- 클라우드를 통한 관리 및 서비스 제공
- 투명성을 통한 사용자 편의
- 애플리케이션에 대한 우수한 가시성과 통찰력
- 기기의 보안 상태에 따른 접근 정책 적용
- 더 간편한 사용자 연간 구독 라이선스와 무료 게이트웨이

제로 트러스트 환경에서의 신뢰성 확보

Sophos ZTNA는 제로 트러스트 원칙 아래 활동, 즉 아무것도 믿지 않고 모든 것을 확인합니다. 개인 사용자와 장치는 지속적으로 검증되고 확인되는 자신만의 고유한 마이크로 세그먼트 경계가 됩니다. 더 이상, 이 장치들은 일반적으로 암묵적인 신뢰와 접속을 허용하고 있는 네트워크에 있는 것이 아닙니다. Zero Trust에서 신뢰는 주어지는 것이 아니라 확보하는 것입니다.

안전한 원격 사용자 활성화

Sophos ZTNA를 사용하면 원격 사용자가 배포, 등록 및 관리를 하면서도 기존 VPN보다 더 안전하고 원활하게 정보와 애플리케이션에 접근할 수 있습니다.

애플리케이션 마이크로 세그먼트

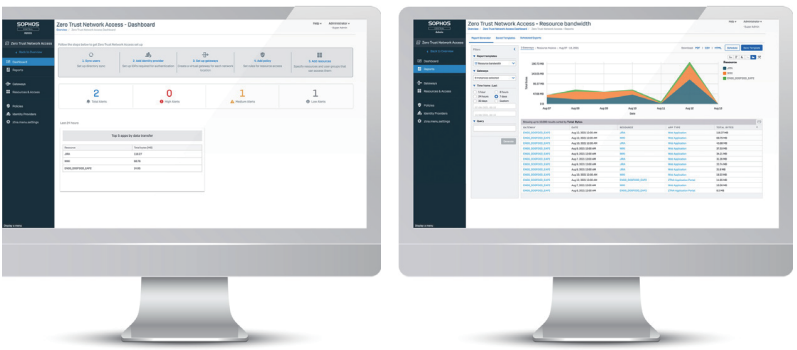
Sophos ZTNA는 상세한 마이크로 세그먼트를 제공하여, 온프레미스, 데이터 센터 혹은 퍼블릭 클라우드에서도 안전한 애플리케이션 접근을 제공합니다. 사용자는 상태, 보안 현황 및 사용에 대한 애플리케이션 활동을 실시간으로 파악할 수 있습니다.

랜섬웨어 및 위협 차단

ZTNA 환경에서, 감염된 장치가 네트워크를 통해 랜섬웨어와 같은 위협을 전파할 가능성은 더 이상 신경 쓸 문제가 아닙니다. 이는 VPN의 핵심 문제 중 하나인 암묵적 신뢰와 공중망 접속의 불안정성을 제거합니다.

신속한 배포, 조정 및 확장

Sophos ZTNA는 다이나믹하게 변화하고 급속도로 성장하며 클라우드 환경으로 빠르게 전환하고 있는 최신 네트워크를 위해 구축되었습니다. 이것은 신속하게 새 애플리케이션을 안전하게 설치하고 사용자/장치를 등록 및 제거하며 애플리케이션 상태 및 사용에 대한 중요한 통찰력을 얻을 수 있는 신속하고 간편한 솔루션입니다.



클라우드를 통한 관리 및 서비스 제공

Sophos ZTNA는 제로 트러스트 네트워크 액세스를 쉽고 안전하며 통합적으로 이용이 가능하게 만들어졌습니다. Sophos ZTNA는 클라우드 제공 및 클라우드 관리 방식으로, 세계에서 가장 신뢰받는 사이버 보안 클라우드 관리 및 보고 플랫폼인 Sophos Central에 통합됩니다.

Sophos Central에서는 ZTNA 뿐만 아니라 Sophos Firewall, 엔드포인트, 서버 보호, 모바일 기기, 클라우드 보안, 전자메일 보호 등을 관리할 수 있습니다. 언제 어디서나 모든 장치에 로그인하여 IT 보안 관리가 가능합니다.

단일 에이전트 배포

Sophos ZTNA는 Sophos Intercept X 차세대 엔드포인트 보호와 통합되어 단일 클라이언트 배포가 가능합니다. 단일 클라이언트 구축으로 세계 최고의 엔드포인트 및 랜섬웨어 보호 기능과 애플리케이션 보안 및 세분화를 모두 활용할 수 있습니다. 브라우저 기반 애플리케이션을 위한 클라이언트리스 액세스 또한 가능합니다.

확장 가능한 애플리케이션 게이트웨이

Sophos ZTNA 게이트웨이는 어디든지 자유롭게 배치될 수 있습니다. 가상 어플라이언스로 사용이 가능함으로, 고가용성 게이트웨이를 쉽게 배치하고 조직이 성장함에 따라 확장할 수 있습니다.

단일 에이전트, 단일 콘솔, 단일 공급업체

Sophos ZTNA는 Sophos의 사이버 보안 생태계와 독보적으로 통합되어 업무를 훨씬 쉽게 수행할 수 있으며, 단일 에이전트를 통해 ZTNA와 차세대 엔드포인트 보호를 동시에 사용할 수 있습니다. 또한, Sophos Central의 단일 웹 인터페이스 콘솔을 통해 모든 IT 보안 제품에 대한 새로운 통찰력을 얻을 수 있습니다.

고객들은 이 통합된 Sophos 사이버 보안 솔루션이 보안 운영 시간을 엄청나게 절약하며, IT 팀의 규모를 두배로 늘리는 것과 같다고 평가하고 있습니다.

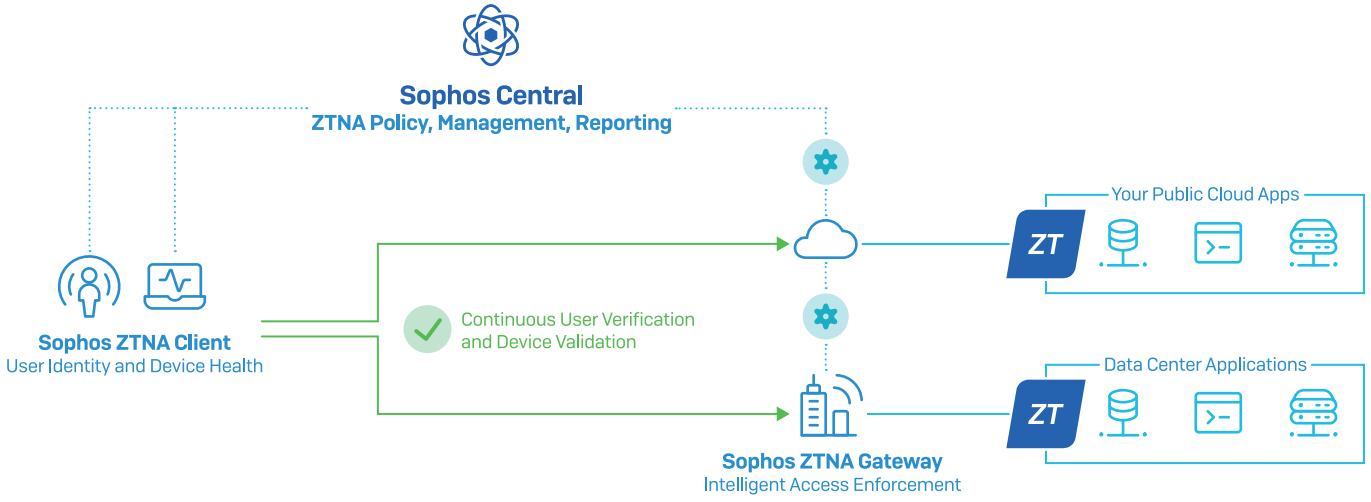
장치 상태 동기화

Sophos ZTNA는 Sophos Intercept X 엔드포인트와 Sophos Central, 그리고 ZTNA 사이의 Security Heartbeat™ 를 활용하여 기기 상태를 평가하고 활성 위협 및 침해 증상을 식별함으로써 Sophos 동기화된 보안 (Synchronized Security)을 최대한 활용합니다.

그 결과 네트워크 안팎에서 침해되거나 규정을 준수하지 않는 장치에 대한 액세스를 제한하는 즉각적인 대응이 가능합니다.

통합 아이덴티티

제로 트러스트 환경에서는 아이덴티티가 핵심입니다. Sophos ZTNA는 Microsoft Azure 및 Okta를 포함하여 가장 널리 사용되는 IDP 솔루션을 지원하여 사용자의 신원을 지속적으로 확인합니다.
또한 IDP와 통합된 MFA (Multi-Factor Authentication) 솔루션을 활용하여 자격 증명 도용이나 손상된 장치를 보호할 수 있습니다.



Sophos ZTNA 구성요소

Sophos Central 클라우드 관리는 클라우드에서의 간편한 배포, 세분화된 정책 제어, 통찰력 있는 가시성 및 리포팅 기능을 제공합니다. ZTNA는 Intercept X와 통합되어 Synchronized Security Heartbeat™를 활용합니다.

Sophos ZTNA Client 는 Intercept X와 함께 클릭 한 번으로 배포되며 ID 및 장치 상태에 따라 애플리케이션에 투명하고 원활한 원격 액세스를 제공합니다.

Sophos ZTNA Gateway는 VMware 및 AWS에서 가상 어플라이언스로 제공되어 무료 및 구축이 쉬운 네트워크 애플리케이션을 보호할 수 있습니다. 보호된 애플리케이션은 온프레미스, 데이터 센터 또는 AWS 퍼블릭 클라우드 인프라에 구축 가능합니다.

SOPHOS

Cybersecurity made simple.

DAOU DATA

㈜다우데이타

주소: 서울시 마포구 독막로311 재화스퀘어 11층

홈페이지: https://members.daoudata.co.kr

대표번호: 02 - 3410 - 5100