Palo Alto Networks Product Brochure 2026

Palo Alto Networks 소개



© 2026 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.



팔로알토 네트웍스 소개

팔로알토 네트웍스는 2005년에 설립된 회사로 현재는 미국 샌프란시스코에 본사를 두고 있으며, 약 20000명의 직원이 150여개의 나라에서 보안 사업을 이끌고 있습니다. 글로벌 사이버 보안 선도 기업으로 팔로알토 네트웍스는 AI 기반 보안 솔루션을 통해 기업들이 위협에 앞서 나갈 수 있도록 지원하며, AI가 비즈니스와 보안 모두를 재편하는 시대에 발맞춰 나갈 수 있도록 돕고 있습니다.

Why Palo Alto Networks?

최고의 사이버 보안 파트너:

팔로알토 네트웍스는 세계 10대 제조 기업 중 8곳을 포함하여 전세계 약 90,000개의 기업이 Palo Alto Networks 제품/서비스를 선택하여 사용하고 있는 사이버 보안 파트너입니다.

플랫폼 접근 방식:

팔로알토 네트웍스의 보안 솔루션은 네트워크, 클라우드 및 보안 운영 센터(SOC)를 보호하기 위한 최고 수준의 2개의 통합 플랫폼으로 기업의 보안을 위한 End to End를 제공합니다. 이는 기업에게 최상의 보안과 운영 간소화 사이에서 선택해야 하는 고민을 해결해 줍니다.

검증된 리더십:

팔로알토 네트웍스는 Gartner, Forrester, Omdia를 포함한 25개 이상의 분석 기관 평가에서 업계 선두 기업으로 인정받았습니다.

500 Fortune 대 기업

사이버 보안 업체로는
유일하게 Fortune 500대 기업

85 개 고객사

Fortune 100대 기업중
85개의 고객이 팔로알토를 사용

55 %

Global 2000 기업 중 55%가
팔로알토 네트웍스 솔루션을
통해 보안지원

Global 우수의 평가기관으로부터 인정 받은 최고의 기술력

Gartner Recognitions

- 보안 서비스 엣지(SSE): 2025 매직 쿼드런트 리더(3년 연속).
- SASE 플랫폼: 2025 매직 쿼드런트 리더(3년 연속).
- 단일 벤더 SASE: 2024 매직 쿼드런트 리더.
- SD-WAN: 2024 매직 쿼드런트 리더.
- 엔드포인트 보호 플랫폼(EPP): 2025 매직 쿼드런트 리더(3년 연속).
- 하이브리드 메시 방화벽: 2025 매직 쿼드런트 첫 번째 발표에서 리더.
- 네트워크 방화벽: 11회 이상 연속 리더로 선정.

Forrester Recognitions

- 제로 트러스트 플랫폼, 2025년 3분기: "현재 제공 제품" 부문에서 리더
- SASE(구 Zero Trust Edge), 2025년 3분기: 2년 연속 리더
- 운영 기술(OT) 보안 솔루션, 2024년 2분기: 리더
- 클라우드 네이티브 애플리케이션 보호 솔루션(CNAPP), 2026년 1분기: 우수 제품(Cortex Cloud)
- IoT 보안 솔루션, 2025년 3분기: 우수 제품 확장형 탐지 및 대응
- (XDR): XDR 평가에서 리더

Other Key Recognitions

- DC MarketScape: 2025년 엔터프라이즈 하이브리드 방화벽 솔루션 부문 리더
- Frost & Sullivan: 2025년 최신 SIEM 부문 리더
- KuppingerCole: SOAR 및 공격 표면 관리(ASM) 부문 Leadership Compass에서 종합 리더
- MITRE ATT&CK: Cortex XDR은 최근 평가(예: Turla, Wizard Spider/Sandworm)에서 100% 보호 및 높은 분석 탐지 범위를 일관되게 제공

95%
OF THE FORUTUNE 100

70 K
CUSTOMERS

700+
PARTNER INTEGRATIONS

480 B
ENDPOINTS SCANNED DAILY

90%
RISK REDUCTION WITH SHIFT LEFT

25x
REDUCTION IN ALERTS & REMEDIATION WORKFLOWS

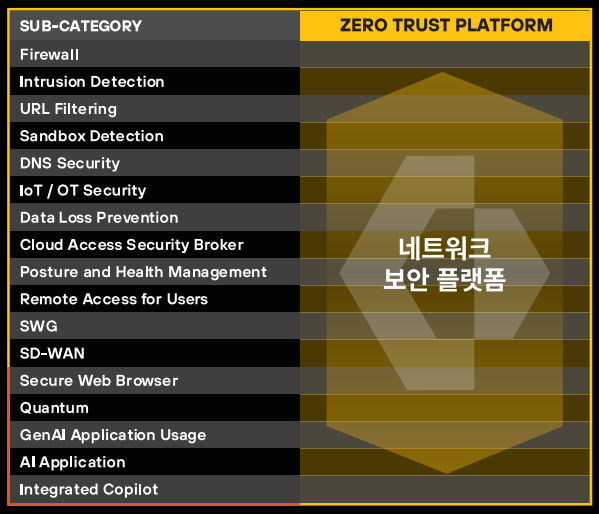
1 K+
MATTERS PER YEAR

24 / 7 / 365
INCIDENT RESPONSE

팔로알토 네트웍스
통합 Platform 보안과 사고 대응

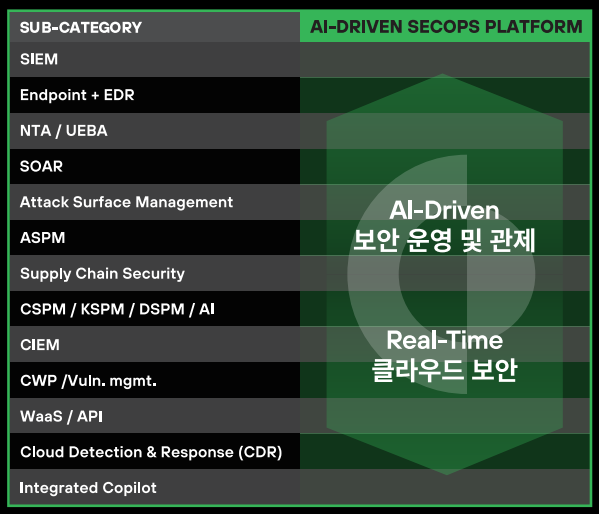
Zero Trust Network Security Platform

- 차세대 방화벽 (하드웨어, 소프트웨어, Container)과 SaaS base의 다양한 Security Service (OT/IOT 보안 서비스 포함)
- SASE(보안 액세스 서비스 에지) + 웹 브라우저 보안



AI 기반의 Cloud 보안 및 보안 운영(SOC)

- Cortex Cloud(클라우드 보안): 업계 최고의 클라우드 보안 플랫폼으로, 코드부터 클라우드까지 애플리케이션을 보호하고 보안 팀과 DevOps 팀 간의 협업을 지원
- Cortex(보안 운영): 최신 SOC(보안 운영 센터)를 위한 플랫폼으로, 보안 분석가가 피해를 입히기 전에 위협을 찾아 차단할 수 있도록 데이터를 수집 및 분석



Unit 42 - 사고 대응, 자문 서비스 및 위협 정보

인텔리전스 중심의 즉시 대응 가능한 팀

팔로알토 네트웍스의 보안 인텔리전스 그룹인 Unit 42는
언제나 최신 위협 인텔리전스를 수집 및 분석하고
사이버 공격 대응에 분석 결과를 적용하는 데 초점을 맞춥니다.
아무리 최악의 상황을 겪은 날이라도 Unit 42의 도움을
받는다면 보다 나은 결과를 얻을 수 있도록 노력합니다.
랜섬웨어가 두려우신가요?
Unit42와 함께라면, 단 한 순간도 걱정할 필요가 없습니다.

업계 최고 수준의 지원

위협 인텔리전스
신속한 조사 및 해결을 위한 광범위한 원격 측정 및 인텔리전스

기술
심층적 가시성을 제공하여 더 빠르게 위협 요소를 발견하고, 차단, 제거하며 운영 중단을 최소화하는 Palo Alto Networks 플랫폼

경험
연간 1,000건이 넘는 인시던트에 신속하게 대응하고 단호하게 대처하는 신뢰할 수 있는 전문가

Palo Alto Networks 방화벽은 '보이는 것만 막는 방화벽'이 아니라 '보이지 않는 위협까지 제어하는 보안 플랫폼' 입니다.

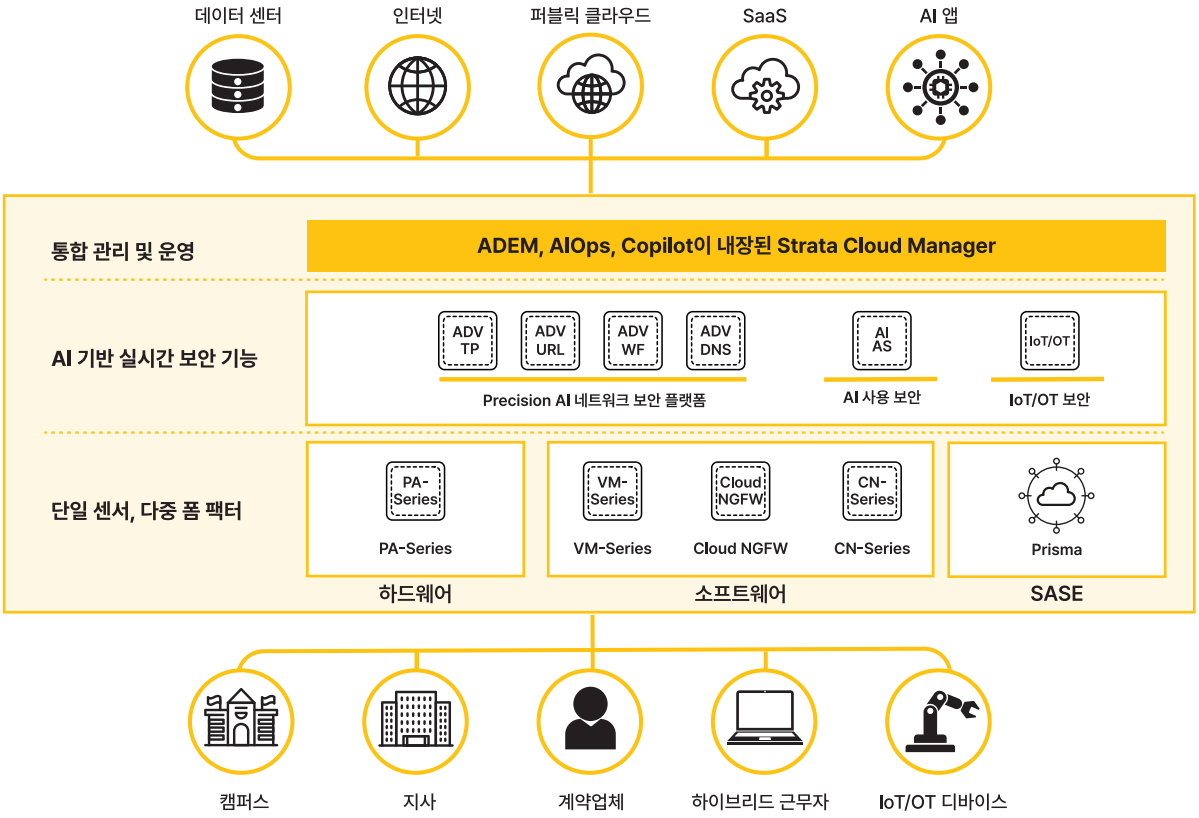


그림 1. Precision AI를 기반으로 하는 Strata 네트워크 보안 플랫폼

모든 위치에서 최신 위협으로부터 모든 사람과 모든 것을 보호합니다.
제로 트러스트를 위해 구축되고 AI를 기반으로 하는 Strata™ 네트워크 보안 플랫폼은 복잡성을 줄이면서 정교한 위협을 실시간으로 선제적으로 모니터링, 분석 및 방지하여 조직의 안전한 성장과 혁신을 지원합니다.

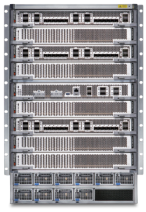
Palo Alto Networks NGFW의 10가지 특징

Palo Alto Networks 차세대 방화벽이 제공하는 주요 특징



"모든 트래픽을 식별하고, 모든 위협을 차단하는 차세대 보안의 새로운 기준"

Hardware – NGFW Line-Up

중소기업, 소규모 회사 프랜차이즈 매장 등		중견기업, 교육기관 등	대기업 지사, 대학 캠퍼스	대형제조공장 금융데이터 센터	CSP, Telco, 대형금융그룹	국가기간망, 초대형 IDC
PA-400 Series	PA-500 Series	PA-1400 Series	PA-3400 Series	PA-5400 Series	PA-5500 Series	PA-7500 Series
 PA-460 4.4 Gbps App-ID	 PA-560 8.5 Gbps App-ID	 PA-1420 9.5 Gbps App-ID	 PA-3440 24 Gbps App-ID	 PA-5450 Up to 200 Gbps App-ID	 PA-5580 375 Gbps App-ID	 PA-7500 1 Tbps App-ID
 PA-455 3.6 Gbps App-ID	 PA-555 7.5 Gbps App-ID	 PA-1410 6.8 Gbps App-ID	 PA-3430 20.5 Gbps App-ID	 PA-5445 93 Gbps App-ID	 PA-5570 300 Gbps App-ID	
 PA-450 2.9 Gbps App-ID	 PA-550 6.5 Gbps App-ID		 PA-3420 16.9 Gbps App-ID	 PA-5440 72 Gbps App-ID	 PA-5560 240 Gbps App-ID	
 PA-445 2.2 Gbps App-ID	 PA-545 5 Gbps App-ID		 PA-3410 11 Gbps App-ID	 PA-5430 61 Gbps App-ID		
 PA-440 2.2 Gbps App-ID	 PA-540 3.8 Gbps App-ID			 PA-5420 56 Gbps App-ID	 PA-5550 175 Gbps App-ID	
 PA-415 1.2 Gbps App-ID	 PA-520 2.8 Gbps App-ID			 PA-5410 43.5 Gbps App-ID	 PA-5540 150 Gbps App-ID	
 PA-410 1.1 Gbps App-ID	 PA-510 1.8 Gbps App-ID					
	 PA-505 1.2 Gbps App-ID					

Software – 가상/클라우드 방화벽

VM-Series	CN-Series	Cloud NGFW
주요 적용 환경	**주요 적용 환경**	**주요 적용 환경**
• Vmware • KVM • Nutanix • Public Cloud	• Kubernetes - EKS - AKS - GKE - OpenShift	• AWS • Managed 서비스 (Azure 전용)
핵심 특징	**핵심 특징**	**핵심 특징**
기존 가상화 환경을 위한 다목적 가상 방화벽	컨테이너 간(East-West) 트래픽 보호 및 K8s 네이티브 통합	인프라 관리 부담 없이 클릭 몇 번으로 배포하는 SaaS형 방화벽

CDSS (Cloud-Delivered Security Services)

CDSS는 Palo Alto Networks 방화벽에 클라우드 기반 보안 서비스를 실시간으로 제공하여 장비 교체 없이도 최신 위협에 자동 대응할 수 있는 보안 서비스 체계입니다. 또한, 클라우드 연동을 통해 알려지지 않은 공격에도 효율적으로 대응하며, 파일 및 웹 기반 공격에 대해 인라인 머신러닝 기반의 보호를 제공합니다.

ADV WF

회피형 및 알려지지 않은 악성 소프트웨어를 자동으로 실시간 분석하고 탐지, 차단합니다.

실시간 네트워크 트래픽을 실시간으로 분석하여 알려지지 않은 위협과 고도로 회피적인 위협까지 즉시 차단하여 최초의 감염됨을 예방

ADV URL

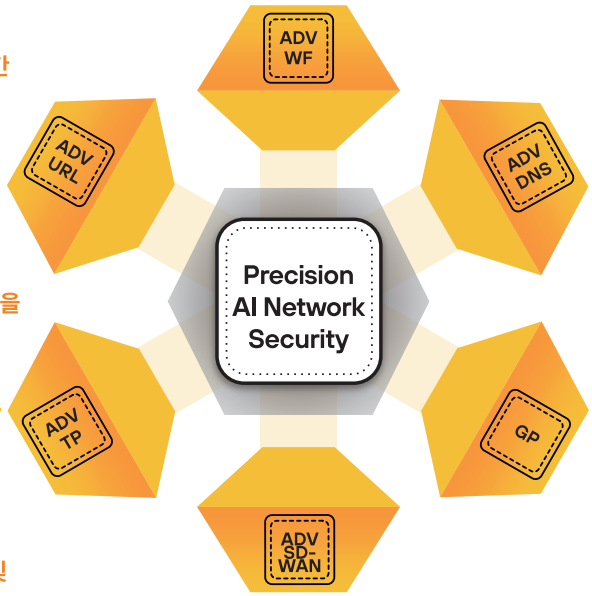
딥러닝 기반의 실시간 웹 보안을 통해 DGA, 유해 웹 사이트를 실시간 차단

기존 웹 필터링 데이터베이스보다 웹 기반 위협물 40% 더 효과적으로 차단

ADV TP

알려지지 않은 익스플로잇, 멀웨어, 스파이웨어 및 명령 및 제어(C2) 공격을 차단합니다.

웹 기반 C2 공격을 96% 차단하여, 주요 IPS 솔루션보다 48% 더 강력한 보호 기능을 제공



ADV DNS

타 보안 업체보다 2배 이상 더 강력한 실시간 위협 대응 능력을 제공합니다.

보안 장비가 놓치기 쉬운 DNS 위회 경로와 터널링 공격까지 실시간 AI 분석으로 틈새없이 차단

GP

원격 사용자에게 사내 네트워크에 안전하게 접속 환경을 제공합니다.

원격 모바일(iOS, Android, Chrome), PC(Windows, Mac, Linux), IoT 환경 등 다양한 환경에 최적화된 보안 환경을 제공

ADV SD-WAN

보안을 손상시키지 않고 지사들을 연결하세요.

보안 기능이 기본적으로 통합된 SD-WAN 솔루션

1. 사전·예측형 위협 대응 구조

CDSS는 알려진 공격뿐 아니라 패턴이 존재하지 않는 신규·변종 공격까지 AI·머신러닝 기반 분석으로 사전에 탐지하고 차단합니다. 이를 통해 패치 이전 공격이나 Zero-Day 공격에도 효과적으로 대응할 수 있습니다.

2. 시그니처 + AI/ML 하이브리드 방어

기존 시그니처 기반 방어 방식의 한계를 극복하기 위해 CDSS는 머신러닝 기반 행위 분석을 결합합니다.
이로 인해 위협 탐지 정확도가 높아지고 오탐은 최소화됩니다.

3. 클라우드 실시간 업데이트

모든 위협 정보와 보안 정책은 클라우드에서 자동으로 업데이트됩니다.
장비 교체, 수동 패치, 운영자의 개입 없이도 항상 최신 보안 상태를 유지할 수 있습니다.

4. 글로벌 위협 인텔리전스 기반 대응

전 세계 Palo Alto Networks 고객과 보안 센서에서 수집된 위협 정보를 실시간으로 공유하여 단일 고객의 공격 사례도 전체 고객 보호로 확장됩니다.

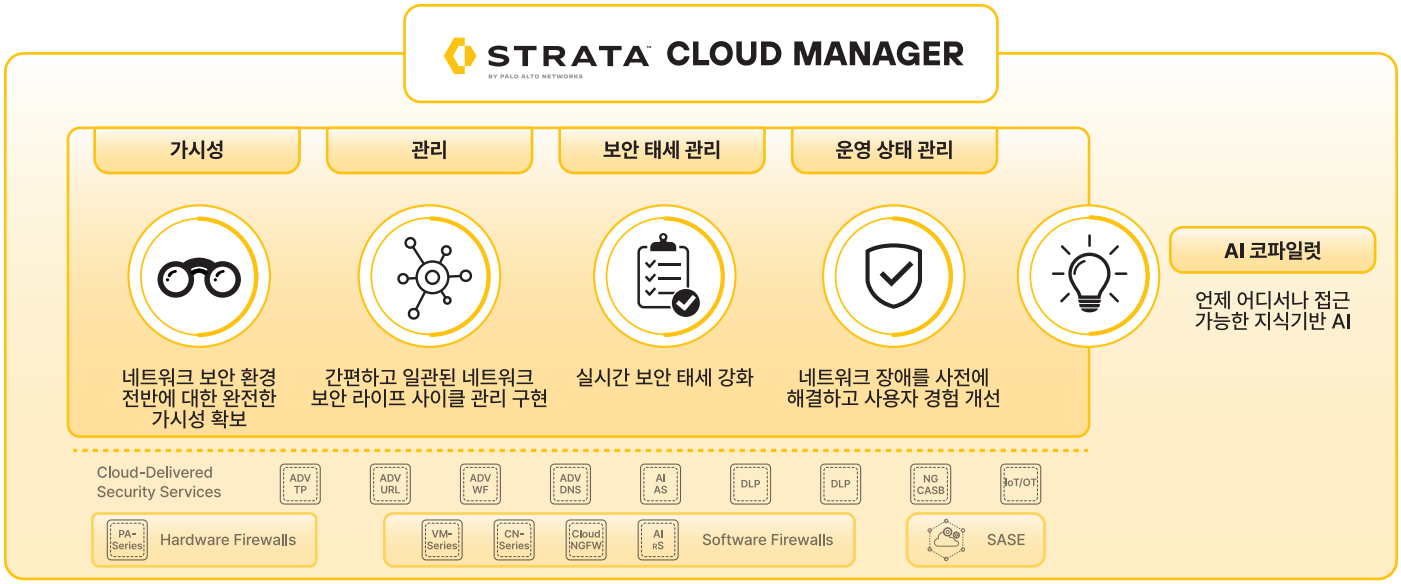
5. 암호화 트래픽까지 포함한 완전한 가시성

SSL/TLS 암호화 트래픽 내부까지 분석하여 보안 사각지대를 제거하고 은닉된 위협까지 식별합니다.
현대 네트워크 환경에 필수적인 핵심 기능입니다.

클라우드 보안 관리 플랫폼 SCM(Strata Cloud Manager)

SCM(Strata Cloud Manager)

Strata Cloud Manager는 Palo Alto Networks 방화벽과 SASE 등의 STRATA 제품군을 클라우드에서 통합 관리·운영하기 위한 차세대 보안 관리 플랫폼입니다. 온프레미스, 지사, 데이터센터, 클라우드 환경 전반을 단일 콘솔에서 관리할 수 있도록 설계되었습니다.



SCM(Strata Cloud Manager) 핵심 특장점

1. 단일 클라우드 콘솔 기반 통합 관리

SCM은 STRATA(NGFW, SASE, AIRS 등) 제품을 통합 관리할 수 있는 플랫폼으로,
하나의 클라우드 관리 화면에서 중앙 집중적으로 운영할 수 있게 합니다.
플랫폼별 관리 도구 분산으로 인한 복잡성을 제거합니다.

2. 정책 일관성 및 자동화된 정책 관리

모든 환경에 동일한 보안 정책을 일관되게 적용할 수 있으며, 정책 변경 사항은 자동으로 배포·반영됩니다.
이를 통해 설정 오류와 운영 리스크를 최소화합니다.

3. CDSS와 완전 통합된 운영 경험

SCM은 CDSS(Threat Prevention, WildFire, DNS Security 등)와 완전히 통합되어 위협 정보, 정책, 대응 상태를 한 화면에서 가시화합니다. 보안 운영과 위협 대응이 분리되지 않습니다.

4. 클라우드 기반 확장성과 신속한 운영

관리 서버 구축이나 유지보수 없이 즉시 사용 가능한 클라우드 관리 환경을 제공합니다.
환경 확장 시에도 추가 인프라 없이 유연하게 대응할 수 있습니다.

5. 운영 효율 및 관리 부담 최소화

SCM은 보안 정책 관리, 변경 이력, 가시성을 통합 제공하여 보안 운영 인력의 업무 부담을 획기적으로 줄입니다.
특히 다수 지사·다수 방화벽 환경에서 효과가 큽니다.

AI Security Platform

Prisma AIRS® 런타임 보안

기업은 AI를 통해 혁신하고 있지만, 기존 보안으로는 막을 수 없는 AI 특화 위협과 복잡한 취약점에 직면해 있습니다.
민감한 내부 데이터와 연결된 AI '복합 시스템'은 공격자에게 새로운 기회를 제공하므로 기존 보안으로는 한계가 있습니다.

Prisma AIRS 플랫폼은 개발부터 배포 단계에 이르기까지 모든 앱, 에이전트, 모델, 데이터를 보호합니다. Prisma AIRS를 통해 완벽한 가시성과 방어 체계를 갖춘 엔터프라이즈 AI 보안솔루션을 도입하여 , 위협 걱정 없는 안전한 AI 혁신을 실현 할 수 있습니다.



AI 라이프사이클 전반에 걸친 완벽한 보호

1. 애플리케이션 & URL 무결성

- 악성 URL 필터링으로 AI 학습 데이터와 RAG 프로세스 오염을 원천 차단합니다.
- 통신 세분화와 매개변수 검증으로 데이터 유출 및 제로 데이 공격을 방어합니다.

2. AI 모델 & 프롬프트 방어

- 직접/간접 프롬프트 인젝션을 식별하여 AI 모델의 신뢰성을 유지합니다.
- 'DAN' 같은 탈옥(Jailbreak) 시도를 차단해 AI가 정해진 규범 내에서만 작동하게 합니다.

3. 엔터프라이즈급 데이터 유출 방지 (DLP)

- 1,000개 이상의 패턴과 ML 탐지로 프롬프트/응답 내 민감 정보 노출을 감시합니다.
- AI 생성 DB 쿼리 권한을 제어해 데이터의 무단 변경이나 삭제를 봉쇄합니다.

4. AI 에이전트 위협 보호

- 노코드/로우코드 환경의 AI 에이전트 신원 사칭이나 메모리 조작을 방어합니다.
- API 도구 오용 등 새로운 유형의 에이전트 보안 위협으로부터 시스템을 보호합니다.

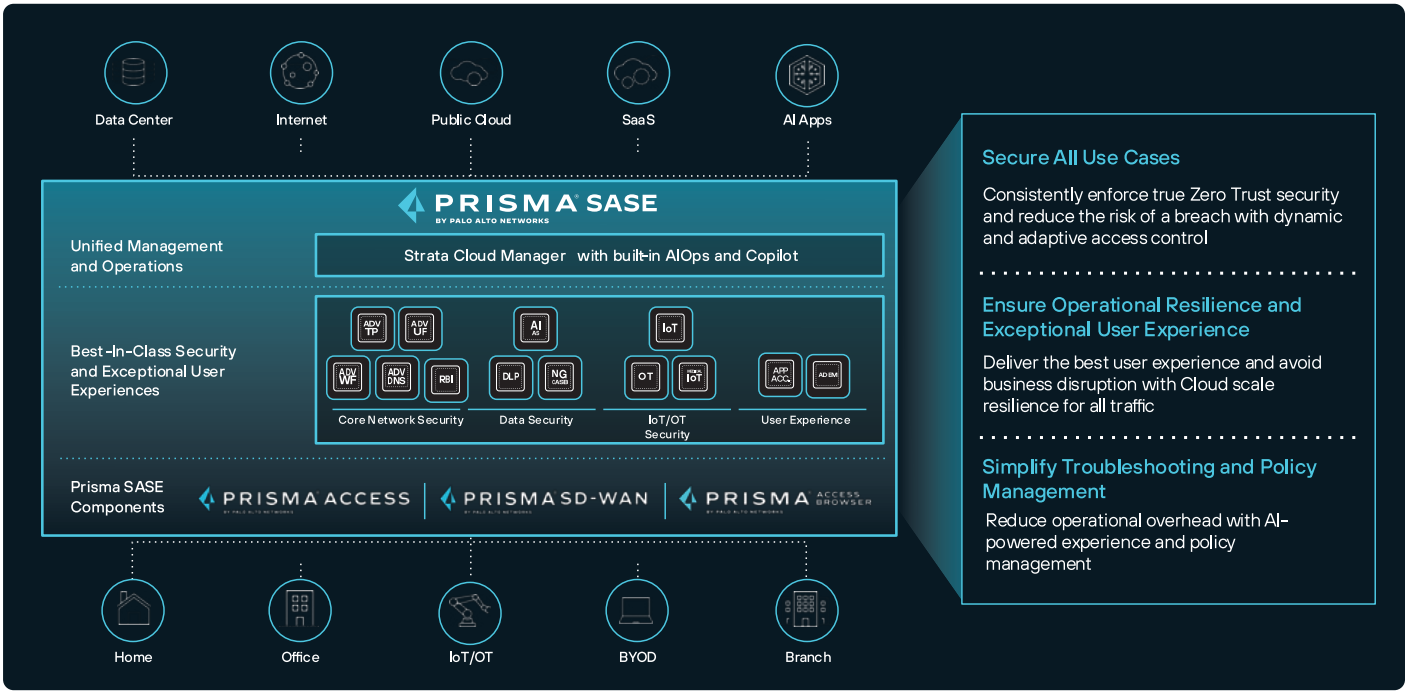
5. 유연한 배포 & 런타임 모니터링

- 멀티 클라우드(AWS, Azure 등)에서 네트워크 및 API 인터셉트 방식을 모두 지원합니다.
- 실시간 모니터링으로 위험한 통신 경로를 즉각 식별하고 대응 체계를 구축합니다.

Prisma SASE(Secure Access Service Edge)

업계에서 가장 완벽한 단일 공급업체 SASE 솔루션

보안 액세스 서비스 에지(SASE)는 SD-WAN과 SWG, CASB, FWaaS, ZTNA와 같은 보안 기능을 하나의 서비스로 통합하는 클라우드 네이티브 아키텍처입니다. SASE는 네트워킹 및 보안 기능을 단일 클라우드 제공 서비스로 통합하여 네트워크 관리를 간소화하고 보안을 강화합니다. 이 아키텍처는 분산 환경을 위한 확장 가능한 통합 액세스 및 보호 기능을 제공하여 현대 조직의 역동적인 요구 사항을 지원합니다.



Prisma SASE 주요 이점

1. 통합 관리 및 운영 효율화 (Single Pane of Glass)

- Prisma Access와 SD-WAN을 하나의 콘솔에서 관리하여 운영의 복잡성을 획기적으로 낮춥니다.
- 여러 도구를 오갈 필요 없이 일관된 보안 정책을 설정하고 전체 위협 환경을 한눈에 모니터링합니다.

2. 강력한 보안: ZTNA 2.0 및 통합 프레임워크

- App, Device, User-ID 기술을 결합한 ZTNA 2.0으로 사용자 경험을 해치지 않는 엄격한 보안을 구현합니다.
- 네트워크와 보안을 하나의 통합된 패브릭으로 작동시켜 모든 앱과 사용자를 사각지대 없이 보호합니다.

3. 데이터 중심의 AI 및 자동화 (AIOps)

- SD-WAN, 보안, 사용자 데이터를 단일 데이터 레이크로 통합하여 가시성을 극대화합니다.
- 지능형 상관관계 분석과 AIOps를 통해 보안 인사이트를 제공하고 운영 업무를 자동화합니다.

4. 탁월한 사용자 및 애플리케이션 경험

- L7 수준의 앱 인식을 통해 최적의 트래픽 경로를 보장하고 서비스 수준(SLA)을 안정적으로 유지합니다.
- ADEM(자율 DEM) 기술로 앱과 디바이스의 장애를 사전에 격리하여 문제를 신속하게 해결합니다.



Prisma SASE

Prisma Access

- SCM(Strata Cloud Manager) 에서 통합관리
- GCP/AWS 클라우드, GCP 백본
- PanOS 의 차세대 방화벽을 기반한 CDSS 보안 기능 지원
- 전세계 110개이상의 모바일 노드 지원
- 지점/본사/모바일 동일 수준의 보안 가시성
- 연결옵션: IPSEC, SSL, SD-WAN, Clientless, Web Proxy
- 모든 트래픽에 대한 보안: HTTP/S 뿐 만 아니라 모든 포트 NGFW, SWG 제로 트러스트 내부 통신 제어, DLP, DNS, 보안 우회하는 Tor, DNS Tunnel 차단

Prisma SD-WAN

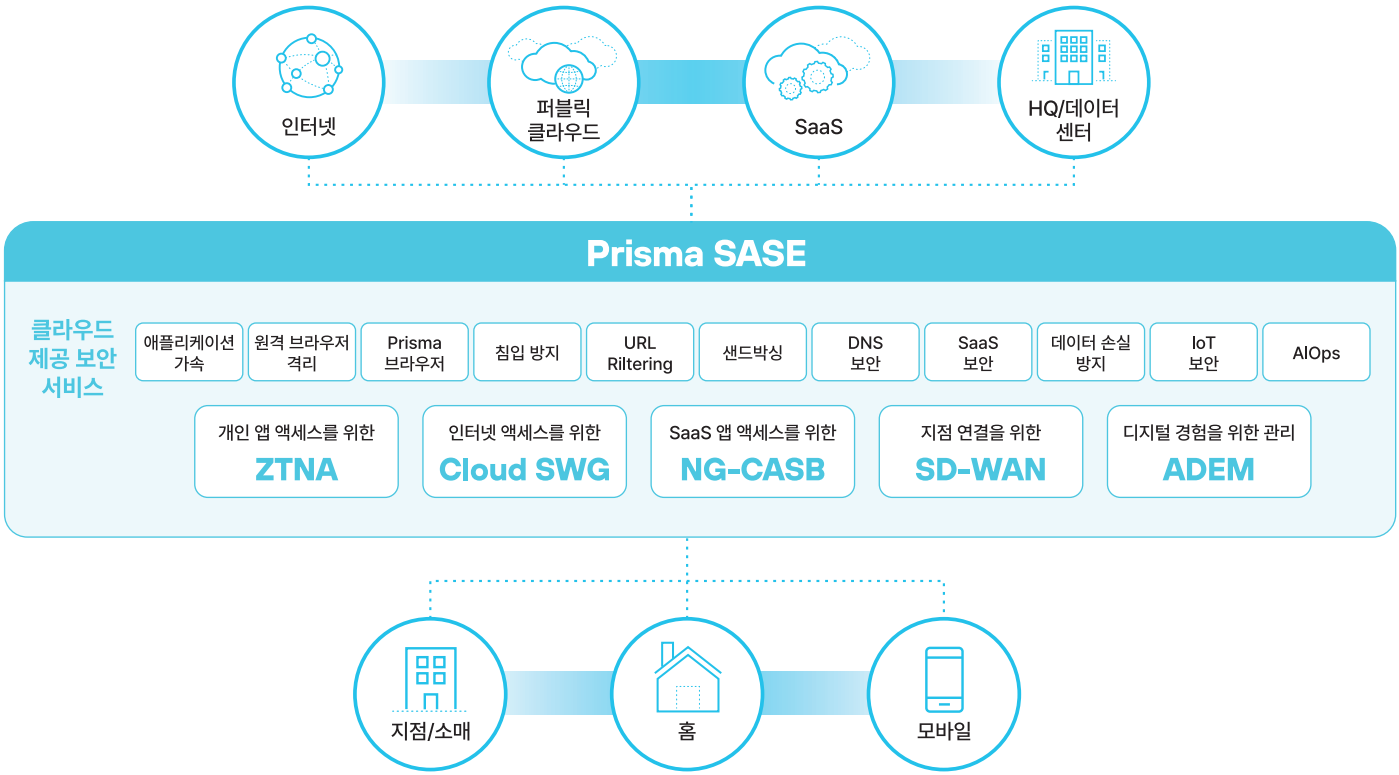
- SCM(Strata Cloud Manager) 에서 통합관리
- 전용 SD-WAN 장비 및 소프트웨어 엣지 지원
- 어플리케이션 기반의 최적 경로 선정
- 네트워크 링크 및 어플리케이션 성능 모니터링 기능제공

Prisma Browser

- Just-In-Time MFA를 통합하여 민감한 작업에 대한 추가 보안 제공
- 민감한 데이터를 동적으로 마스킹하여 기밀 정보 보호
- 민감한 화면에서 구성 가능한 회사 워터마크를 사용하여 스크린샷 찍기, 협업 도구를 통한 공유, 복사/붙여넣기, 인쇄를 차단하여 무단 캡처를 방지
- 콘텐츠 및 소스를 기반으로 파일 다운로드/업로드를 제한

Prisma Access

Prisma Access는 Palo Alto Networks 차세대 방화벽(NGFW)의 모든 기능이 포함된 FWaaS(Firewall-as-a Service)를 제공합니다. 인바운드 및 아웃바운드 보호, 네이티브 사용자 인증 및 액세스 제어, 레이어 3~7 싱글 패스 검사를 통한 지사 사무실 보호 등이 포함됩니다.



Prisma ACCESS 주요 이점

1. 클라우드 보안 웹 게이트웨이 (SWG)

- 원격 사용자가 어디서든 웹 및 애플리케이션에 안전하게 접속할 수 있도록 보호하며, 에이전트 및 VPN 등 유연한 연결 옵션을 제공합니다.
- Threat Prevention, DNS 보안, DLP 등 필수 보안 기능을 통합 제공하며, RBI(원격 브라우저 격리)를 통해 고위험 웹 사용을 완벽히 격리합니다.

2. 차세대 클라우드 액세스 보안 브로커 (CASB)

- 실시간 데이터 보호 기능을 강력한 보안과 결합하여, 급증하는 기업 내 SaaS 애플리케이션 사용 환경에 빈틈없이 대응합니다.
- 승인 및 미 승인 앱 모두에 대해 인라인과 API 기반 보안을 동시에 제공하며, 데이터 유출 리스크와 컴플라이언스 부담을 획기적으로 낮춥니다.

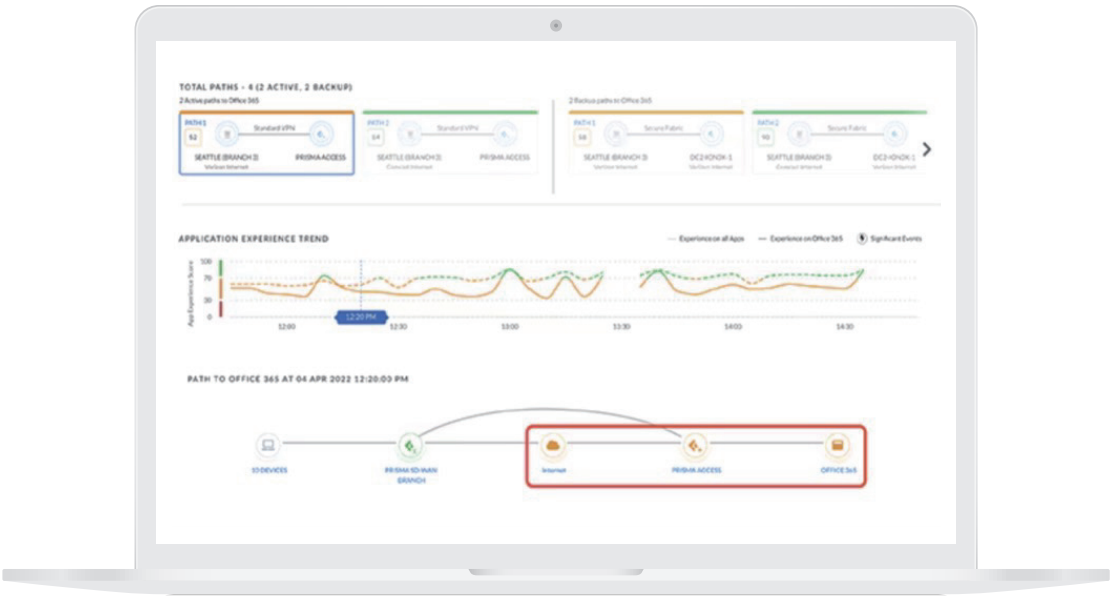
3. 하이브리드/모바일 사용자 연결 최적화 (GlobalProtect)

- **Always-On** 및 온디맨드 연결을 통해 사용자 경험은 유지하면서도, 원격·모바일 환경 어디서나 일관된 보안 기준을 적용합니다.
- 리스크와 대역폭 사용량 기반의 **분할 터널링**을 지원하여, 안정적인 접속 품질과 강력한 보안 통제를 동시에 실현합니다.

SD-WAN

차세대 SD-WAN 기반의 완전한 SASE 솔루션 개요

Prisma SD-WAN은 차세대 접근으로 운영을 단순화하고 보안 성과를 강화해 사용자 경험을 개선합니다. AI/ML 기반 자동화로 구축·라우팅 문제의 복잡성을 줄여 운영 부담을 간소화하며 , 지사까지 일관된 보안을 확장해 보안 침해를 최대 45%까지 줄이는 방향을 제시하여 최대 243%의 ROI(투자수익률)를 제공하는 유일한 솔루션 입니다.



1. 운영 효율화 및 간소화

- 애플리케이션 정책에 따라 각 디바이스를 중앙에서 관리하며, 보안 규칙을 실시간으로 업데이트할 수 있습니다.
- 자동 구축 기능을 통해 새로운 사이트 확장 시 발생하는 운영 경비와 복잡성을 획기적으로 줄여줍니다.

2. 고성능 애플리케이션 경험(QoEx) 보장

- SLA를 기준으로 트래픽을 자동 조정하고, 성능 저하 시 더 나은 경로로 즉시 전환하여 최적의 앱 속도를 유지합니다.
- 트래픽을 중앙으로 우회시키지 않는 '로컬 인터넷 브레이크아웃'을 통해 SaaS 및 클라우드 리소스 접속 지연을 최소화합니다.

3. 강력한 보안 및 네트워크 안정성

- 소프트웨어 정의 네트워킹을 통해 DDoS 및 멀웨어 등 외부 위협을 방어하고, 미승인 디바이스 접속을 자동 차단합니다.
- 특정 통신사(ISP)에 종속되지 않고 여러 회선을 사용하므로, 한 곳에 장애가 발생해도 끊김 없는 네트워크 환경을 제공합니다.

4. 획기적인 비용 절감

- 고가의 MPLS를 저렴한 광대역 회선으로 대체하거나 보완할 수 있어 자본 지출을 줄여줍니다.
- 기존 네트워크 대비 구성이 간편하고 관리가 쉬워, 장기적인 유지 관리 및 지원 비용이 크게 절감됩니다.

Prisma Browser

일반적인 업무의 85% 이상은 브라우저를 통해 이루어집니다.
하이브리드 근무, BYOD, 독립 근무자의 증가와 함께 비즈니스 크리티컬 애플리케이션에 액세스하기 위해 브라우저에 의존하는 것은 상당한 보안 리스크를 초래합니다. Prisma Browser로 브라우저 기반 작업 공간을 보호하고 관리형 또는 비관리형 모든 디바이스에서 웹, SaaS, GenAI 및 비공개 애플리케이션에 안전하게 액세스할 수 있습니다.

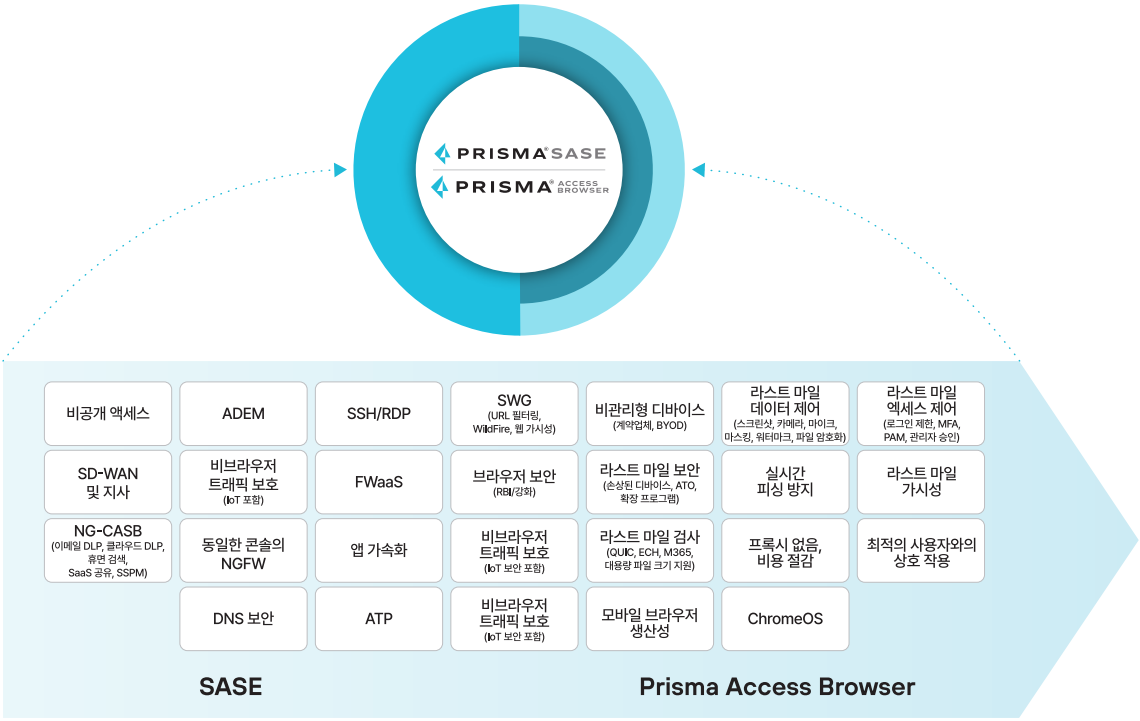
Prisma Browser는 관리형 디바이스 및 비관리형 디바이스를 모두 보호하여 현대 조직과 하이브리드 인력의 진화하는 보안 요구 사항을 해결합니다. Prisma Browser는 SASE의 보호 범위를 몇 분 만에 모든 디바이스로 확장하여 다양한 위협으로부터 비즈니스 애플리케이션과 데이터를 보호합니다.

Prisma Browser 주요 이점

- **노트북 배송 대비 85% 절감:**
  Prisma Browser의 안전하고 비용 효율적인 기능을 대신 사용하여 기업 노트북을 원격/재택 근무자 및 계약업체에 배송할 필요가 없어짐으로써 비용을 크게 절감할 수 있습니다.
- **VDI 대비 79% TCO 절감:**
  Prisma Browser의 효율적인 클라우드 네이티브 아키텍처와 운영 간소화 덕분에 기존 VDI 솔루션과 비교했을 때 TCO(총 소유 비용)가 크게 절감됩니다.
- **모든 디바이스 보호:**
  모든 관리형 또는 비관리형 디바이스에 걸쳐 포괄적인 적용 범위를 보장하여 보안 프로그램의 격차를 해소합니다. Prisma Browser는 강력한 보안 조치를 모든 엔드포인트로 확장하여 디바이스의 출처나 사용자의 위치에 관계없이 기업 데이터를 보호합니다.

Prisma Browser 주요 기능

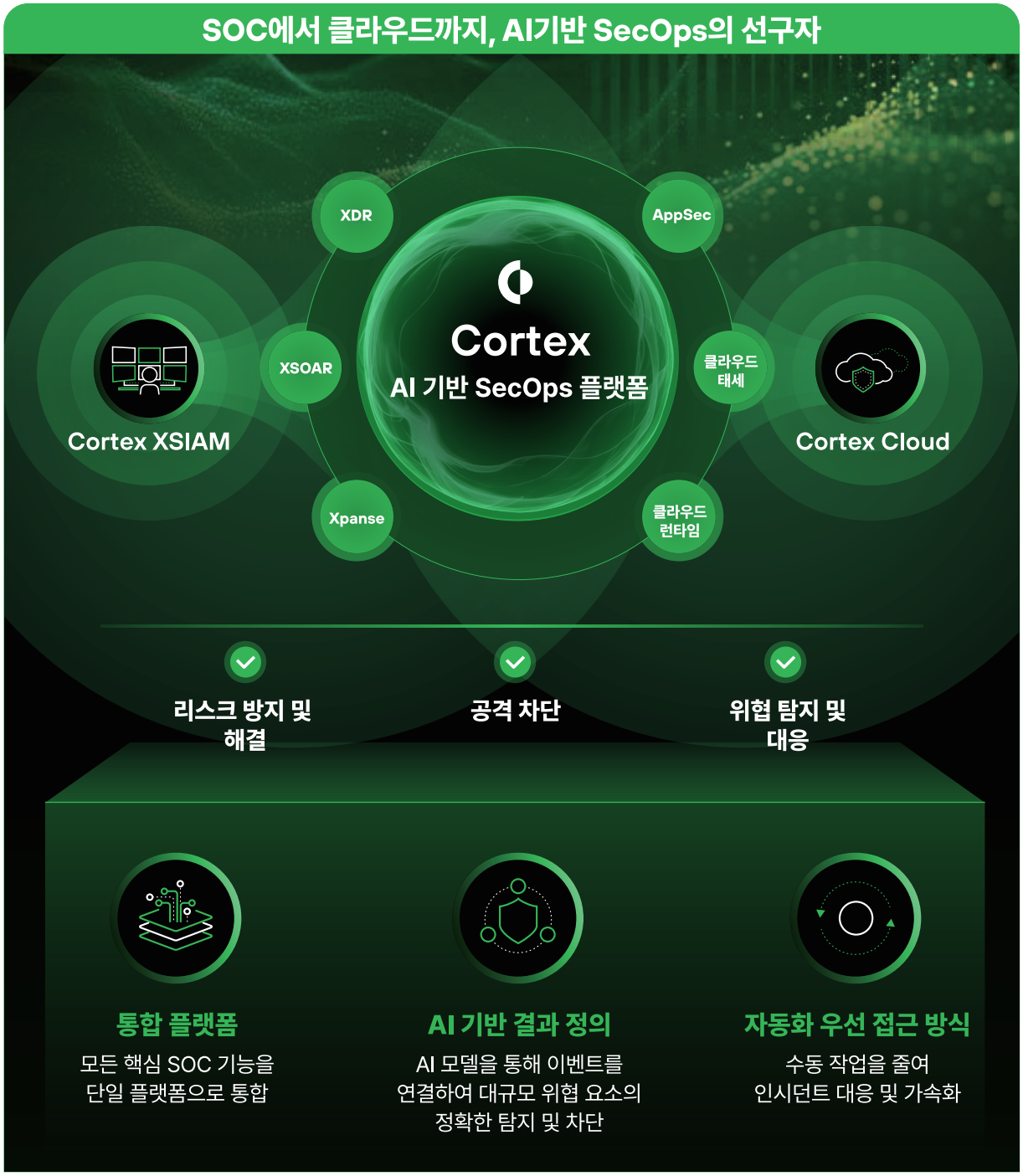
Prisma Browser는 SASE를 확장하고 브라우저를 통해 보안을 확장하여 탁월한 보호 기능을 제공합니다.



Cortex

AI 기반 차세대 보안 운영 플랫폼

Cortex는 엔드포인트, 네트워크, 클라우드 등 다양한 보안 데이터를 통합 분석하여 위협 탐지와 대응을 자동화하는 AI 기반 보안 운영 플랫폼입니다. XDR, XSIAM, XSOAR, XPANCE 기능을 통해 공격 표면을 관리하고 보안 운영을 자동화하여 SOC의 효율성을 높입니다.

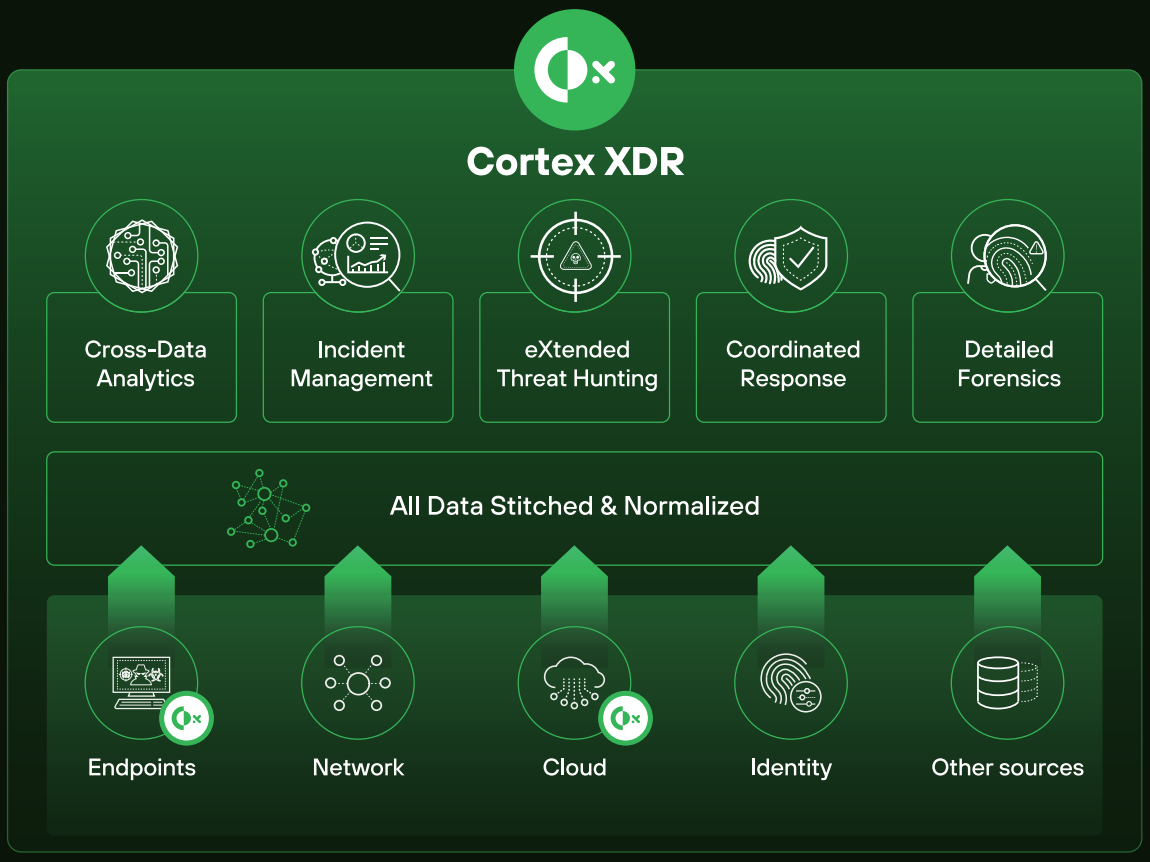


Cortex XDR

AI 기반 차세대 엔드포인트 보안 플랫폼

Cortex XDR은 AI 기반 분석 기술을 활용해 엔드포인트를 실시간으로 보호하는 차세대 보안 플랫폼입니다. 단일 에이전트로 다양한 운영체제를 보호하며, 최신 위협 행위를 분석해 공격을 사전에 차단합니다. 다양한 보안 데이터를 통합 분석해 높은 탐지 정확도를 제공하고, 관련 경보를 하나의 공격 시나리오로 자동 분석하여 보안 운영 부담을 크게 줄입니다. 또한 자동화된 대응과 MDR 서비스를 통해 빠른 위협 대응과 효율적인 SOC 운영을 지원합니다.

엔드포인트 보안의 새로운 표준



100% 탐지

현재 놓치고 있는 공격을 탐지하여 리스크 축소

최신 MITRE ATT&CK 평가에서 지연이나 구성 변경 없이 탐지율 100%를 달성하며 성능을 입증

0% 오탐

중단 없이 엔드포인트 위협 차단

최신 MITRE ATT&CK 평가에서 오탐률 0%를 기록

98% 알림 감소

AI 및 자동화로 SOC 효율성 향상

인적 분류가 필요한 알림이 98% 감소

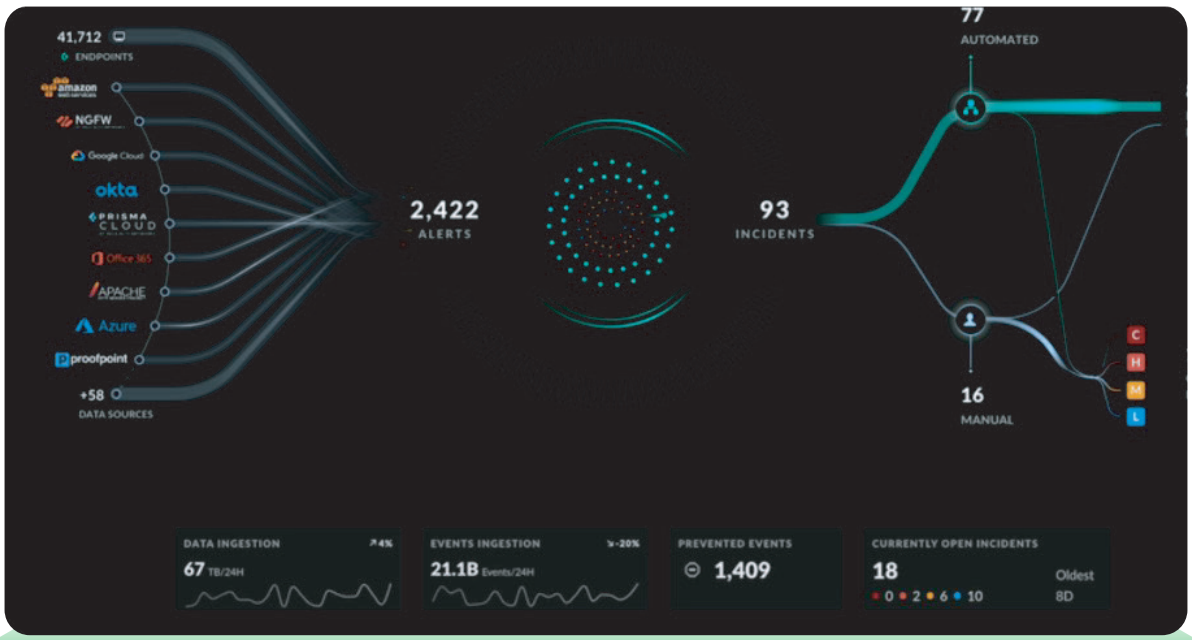
Cortex XSIAM

AI 기반 보안 운영 자동화 플랫폼, Cortex XSIAM

Cortex XSIAM은 보안 데이터, 분석, 자동화를 통합하여 보안 운영(SOC)을 혁신하는 AI 기반 SecOps 플랫폼입니다. 다양한 보안 로그와 텔레메트리를 하나의 데이터 플랫폼에서 통합 분석하고, AI와 자동화를 통해 위협 탐지와 대응을 빠르게 수행합니다. 이를 통해 보안팀은 수많은 경보를 효율적으로 관리하고, 보안 운영 부담을 줄이며 보다 빠르고 정확한 보안 대응 체계를 구축할 수 있습니다.



Cortex XSIAM



보안 데이터 통합 플랫폼

엔드포인트, 네트워크, 클라우드 등 다양한 보안 데이터를 하나의 데이터 플랫폼으로 통합하고, 대량의 데이터를 빠르게 분석하여 보안 위협을 식별합니다.

보안 운영 자동화

반복적인 보안 운영 업무를 자동화하고 대응 프로세스를 자동 실행하며, 이를 통해 SOC 운영 효율성과 대응 속도를 크게 향상시킵니다.

AI 기반 위협 탐지

AI 분석 기술을 활용해 보안 이벤트를 자동 분석과 고도화된 공격 패턴을 탐지하고, 이를 통해 보안 위협을 빠르게 발견하고 대응할 수 있습니다.

통합 보안 운영 관리

탐지, 조사, 대응 과정을 하나의 플랫폼에서 관리하고, 보안 담당자는 한눈에 보안 상황을 확인하고 빠르게 대응할 수 있습니다.

Cortex XSOAR

보안 운영을 자동화하는 AI 기반 SOAR 플랫폼

Cortex XSOAR는 보안 운영(SOC)을 자동화하고 효율적으로 관리할 수 있도록 지원하는 SOAR(Security Orchestration, Automation and Response) 플랫폼으로 다양한 보안 솔루션과 데이터를 하나의 플랫폼에서 통합 관리하고, 자동화된 플레이북을 통해 반복적인 보안 업무를 자동으로 처리하고, 이를 통해 보안 담당자는 위협 분석과 대응에 집중할 수 있으며, 사고 대응 시간을 단축하고 보안 운영 효율성을 크게 향상시킬 수 있습니다.

사고 대응을 간소화하고 자동화



바쁜 업무 제거

자동화를 통해 잡음을 줄이고, 반복적이고 시간 소모적인 작업을 처리하여 중요한 업무와 보안 태세 개선에 집중할 수 있습니다. 다양한 사용 사례에 걸쳐 자동화 콘텐츠 팩을 제공하여 구축을 가속화할 수 있도록 지원합니다.



실시간 분석

인시던트 데이터, 지표, 위협 인텔리전스 등 인시던트를 해결하는 데 필요한 모든 것이 한 곳에서 완벽하게 통합되어 있습니다. 실시간으로 협업하고, 티켓을 관리하고, 사고 후 분석 및 보고를 수행할 수 있는 워룸을 확인하세요.



SOC 전반에 걸친 오케스트레이션

자동화만으로는 충분하지 않습니다. 사람, 프로세스, 기술을 효율적으로 통합하는 총체적인 접근 방식이 필요합니다. XSOAR을 사용하면 팀, 도구 및 네트워크 전반에서 사고 대응을 오케스트레이션하고 중앙 집중화 할 수 있습니다.

Cortex XPANSE

보이지 않는 공격 표면까지 관리하는 차세대 ASM 플랫폼

Cortex XPANSE는 기업의 외부 공격 표면(Attack Surface)을 지속적으로 식별하고 관리하는 Attack Surface Management(ASM) 플랫폼입니다. 인터넷에 노출된 자산과 취약점을 자동으로 발견하고, 보안 위험을 사전에 식별하여 공격자가 악용하기 전에 대응할 수 있도록 지원합니다. 또한 기업이 인지하지 못한 IT 자산과 노출된 시스템까지 탐지해 전체 공격 표면에 대한 가시성을 제공하며, 이를 통해 보안 리스크를 줄이고 보다 선 제적 보안 운영을 가능하게 합니다.

외부 공격 표면 관리의 차별화된 접근



보안 취약점 및 리스크 식별

노출된 자산의 보안 설정, 취약점, 잘못된 구성 등을 분석하여 공격 가능성이 높은 보안 리스크를 식별합니다. 이를 통해 공격자가 악용하기 전에 선제적으로 대응할 수 있습니다.



실시간 공격 표면 가시성 확보

인터넷 전체를 지속적으로 분석하여, 기업의 공격 표면을 실시간으로 확인할 수 있습니다.
이를 통해 보안팀은 외부에 노출된 자산과 위험 요소를 한눈에 파악할 수 있습니다.



자동화된 대응 및 보안 운영 지원

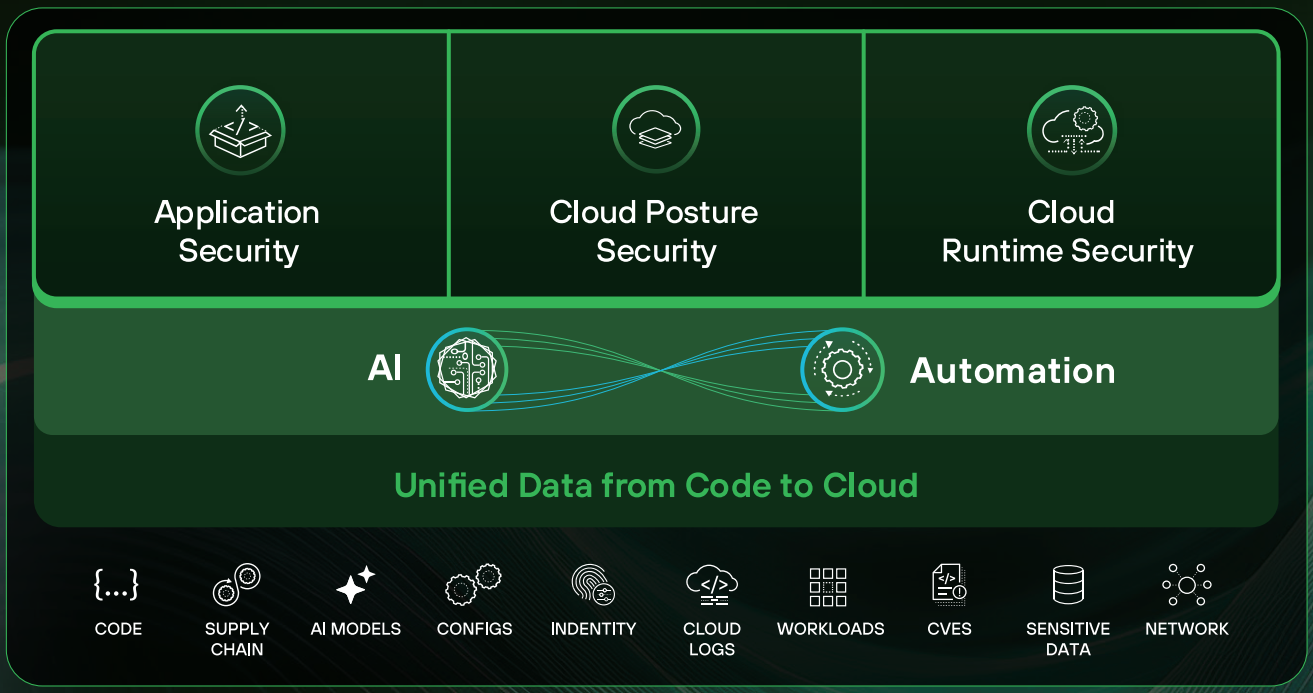
위험 자산을 자동으로 분류하고 대응 우선순위를 제시하여 보안팀의 운영 효율성을 높입니다.
보안 운영 플랫폼과 연계해 빠른 대응과 지속적인 보안 관리가 가능합니다.

Cortex Cloud

실시간 클라우드 보안

업계 최고의 클라우드 네이티브 애플리케이션 보호 플랫폼(CNAPP)과 동급 최고의 CDR을 결합한 유일한 플랫폼에서 독립적인 멀티 클라우드 보호 기능을 통해 더 많은 것을 확인하고, 더 빠르게 문제를 해결하고, 다른 사람들이 놓치는 것을 방지하세요.

실시간 보안을 위해 업계 최고의 CNAPP와 통합된 동급 최강의 CDR



보안 데이터 통합 플랫폼

개발부터 운영까지 애플리케이션 전체 라이프사이클에서 취약점과 보안 위험을 사전에 식별하고 차단합니다.

클라우드 태세 보안

클라우드 자산, 설정, ID, 데이터에 대한 보안 상태를 통합 분석하여 클라우드 환경의 보안 가시성과 통제를 제공합니다.

클라우드 런타임 보호

VM, 컨테이너, 서버리스 환경에서 발생하는 공격을 실시간으로 탐지하고 차단합니다.

클라우드 탐지 및 대응

AI 기반 분석으로 클라우드 위협을 빠르게 탐지하고 자동 대응하여 보안 사고 대응 시간을 단축합니다.

UNIT 42

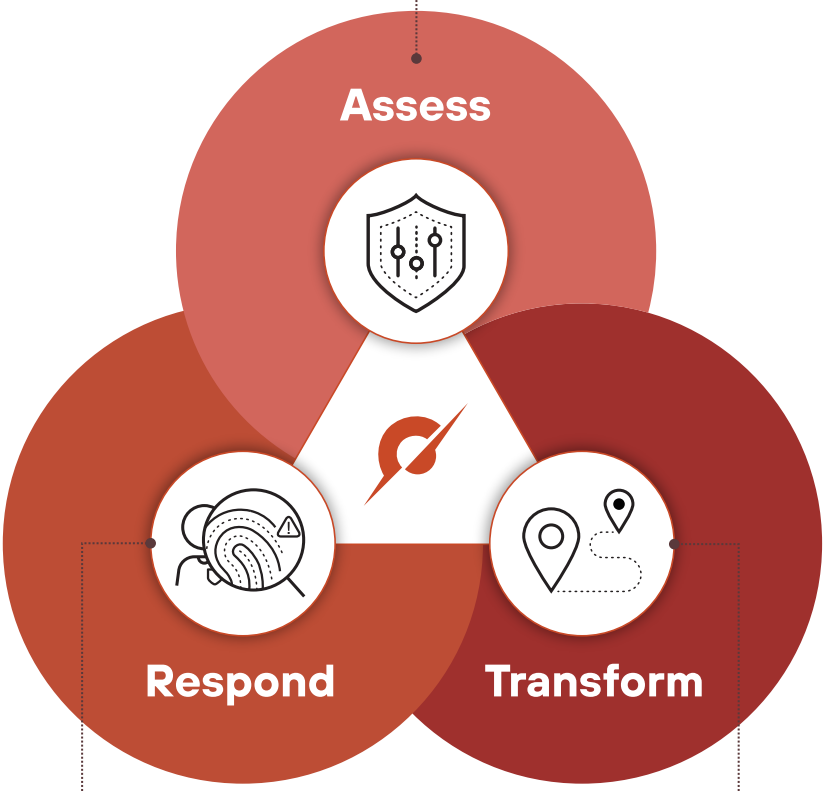
Unit 42는 팔로알토 네트웍스 내에서 세계적으로 유명한 위협 인텔리전스, 사고 대응 및 사이버 위험 관리 조직입니다.
이 기관의 임무는 "지능 기반, 대응 준비 완료"로 요약됩니다.
즉, 대규모 데이터와 인간 전문가의 역량을 결합하여 조직이 사이버 위협에 대비하고, 대응하고, 복구할 수 있도록 지원합니다.

Cyber Risk Management

평가

사이버 위험 관리

사전 예방적 평가 및 사고 시뮬레이션 서비스를 통해 적절한 위협에 대응하여 보안 제어 기능을 평가하고 테스트하십시오.



Incident Response

대응

인시던트 대응과 관리형 탐지 및 대응

사고 대응 및 디지털 포렌식 서비스를 통해 최단 시간 내에 대응하세요.

Advisory Service

혁신

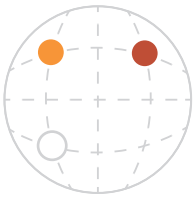
사이버 위험 관리 및 위협 인텔리전스

전략적 자문 서비스를 통해 위협 정보를 기반으로 한 접근 방식으로 보안 전략을 혁신하십시오.

Unit 42 네가지 핵심 요소

1 위협 인텔리전스 (Threat Intelligence)

- **What they do :**
  전 세계에 걸쳐 활동하는 위협 헌터, 악성코드 분석가, 리버스 엔지니어 팀이 적대 세력(국가, 사이버 범죄 조직)을 추적하여 공격 방식을 파악합니다.
- **The Scale :**
  팔로알토네트웍스의 방대한 고객 기반(10만 명 이상)에서 얻은 원격 측정 데이터를 활용하여 매일 5천억 건의 이벤트와 3천만 건의 악성코드 샘플을 분석합니다.
- **Outcome :**
  이러한 인텔리전스는 Palo Alto Networks 제품(예: Cortex XDR 및 차세대 방화벽)에 내장되어 새로운 위협을 자동으로 차단합니다.



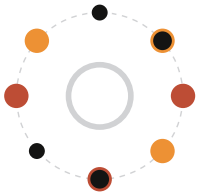
2 사고대응 (Incident Response (IR))

- **What they do :**
  조직이 침해당했을 때(예: 랜섬웨어, 비즈니스 이메일 침해) 24시간 연중무휴로 대응하는 글로벌 팀입니다.
- **The Service :**
  그들은 공격을 조사하고, 위협을 차단하며, 기업이 회복하도록 돕습니다.
- **Retainer :**
  고객들은 종종 Unit42 Retainer(선불 크레딧)를 구매하여 이러한 전문가들에게 "빠른 연락"을 할 수 있도록 합니다.



3 사이버 위험 관리(사전 예방 서비스) Cyber Risk Management

- **What they do :**
  공격 발생 전에 보안을 평가하고 테스트하도록 설계된 서비스입니다.
  - **Tabletop Exercises :**
    팀의 대응 능력을 테스트하기 위해 모의 공격을 실시합니다.
  - **Assessments :**
    특정 위험 평가 (예: AI 보안 평가, 클라우드 보안 평가, SOC 평가)
  - **Penetration Testing :**
    취약점을 찾아내는 모의 해킹.



4 매니지드 서비스 Managed Services (MDR)

- **Unit 42 MDR :**
  Unit 42의 전문가들이 Cortex XDR/XSIAM을 사용하여 고객 환경을 24시간 내내 모니터링하고 고객을 대신하여 공격을 탐지하고 차단하는 관리형 탐지 및 대응 서비스입니다.



Unit 42 사고 대응 프로세스

준비

- 모의 훈련 및 사고 시뮬레이션
- 침해 대응 계획 수립
- 랜섬웨어/침해 대비 태세
- 위협 모델링

테스트 및 평가

- 공격적 보안: 침투 테스트(레드/퍼플 팀)
- 침해 평가
- 공격 표면 평가

탐지 및 모니터링

- 관리형 위협 탐지
- 관리형 탐지 및 대응
- 관리형 XSIAM

사고대응

- 랜섬웨어 | APT | BEC | 클라우드 등
- 랜섬웨어 협상
- 포렌식 조사
- 복구 및 문제 해결

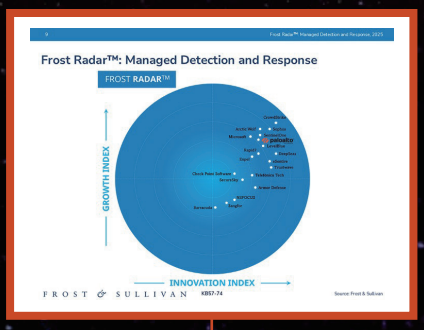
위협 인텔리전스

- 다크 웹 모니터링
- 현장 배치 분석가
- 연구, 보고및 정보요청

자문 및 변혁

- AI 보안 평가
- 클라우드 보안 평가
- SOC 성숙도 평가
- 제로 트러스트 자문

공식적으로 인정받은 공격 대응 리더 Unit 42



LEADER

2025 Frost & Sullivan
MDR Radar



LEADER

2024 Forrester Wave
Cyber Incident Response



LEADER

2025 IDC Worldwide
IR MarketScape

팔로알토 네트웍스 고객 성공사례

제조업을 위협하는 랜섬웨어, 공장을 지키는 보안 전략

국내 제조 기업은 생산 중단으로 직결되는 랜섬웨어 위협에 직면해 있었고, 팔로알토 네트웍스의 AI 기반 랜섬웨어 대응 보안 아키텍처를 도입해 위협을 사전에 차단하고, 생산을 멈추지 않으면서도 랜섬웨어를 사전에 차단하는 제조 보안 표준 모델을 구축했습니다.

위협 요소

랜섬웨어를 사전에 탐지·차단하면서도
생산 안정성을 유지할 수 있는 보안 체계 필요

- 제조 공정(OT), 네트워크 연결로 랜섬웨어 확산 경로 증가
- 기존 보안 체계로는 암호화·측면 이동 탐지 한계
- 랜섬웨어 감염 시 즉각적인 생산 중단 및 대규모 손실 위험
- 보안 강화를 위해 생산 성능을 희생할 수 없는 구조

해결 방법

AI 기반 네트워크 보안과 통합 보안 체계 구축과
랜섬웨어를 사전 차단하고,생산 라인의 안정성 유지

- 사전 예방 중심 랜섬웨어 전략 수립(침투 전·후 단계 모두 대응)
- 생산 라인과 IT 구간을 분리하는 네트워크 기반 차단
- 랜섬웨어 행위(암호화, C2 통신, 확산 시도) 를 실시간 탐지
- 사고 발생 시 자동 차단 및 확산 방지

비즈니스 효과

60%
운영 효율 향상

0건
데이터 탈취

10sec
응답 시간 단축

도입 솔루션

공격표면 최소화
어플리케이션 보안 정책을 통하여 필수앱만 최소허용 (RDP, SSH 앱 최소허용)

Adv. URL Filtering
고도화 Phising /MalSpam 및 MiTM기반 웹공격 방어

Cortex Xpanse
외부에 노출된 공격표면 분석 및 조치
(노출 RDP 및 취약점 등)

Unit 42/ 침해 대응
글로벌 No.1 사고대응 리더가 제공하는 완벽한 침해 전/후 대응 컨설팅

Adv Threat Prevention
알려진 취약점 Cobalt Strike 등 Unknown C2 방지

Cortex XDR
멀웨어, 파일리스 및 랜섬웨어 프로세스 실시간 탐지/분석/차단

팔로알토 네트워스 고객 성공사례

초연결 물류망 시대, POS부터 클라우드까지, 통합 보안 전략

글로벌 유통 기업들 팔로알토 네트워스 도입을 통해 보안 운영 생산성 50% 향상, 운영 비용 20~40% 절감, 위협 대응 속도 최대 90% 단축이라는 명확한 성과를 달성하며 방화벽 중심 보안에서 풀필먼트 전반의 AI 통합 관리 보안 플랫폼으로 전환했습니다.

위협 요소

유통 기업은 디지털 전환과 함께 구조적 보안 한계에 직면

- IT 환경: 매장·물류·본사·클라우드로 분산된 인프라
- POS, 키오스크, IoT, 물류 장비 등 비가시 자산 증가
- 보안 구조: 방화벽 중심, 포인트 솔루션 난립
- 운영: 위협 알림 과다, 수작업 중심 SOC
- 리스크: 랜섬웨어 및 매장 중단 시 직접적 매출 손실

해결 방법

고객은 단순 장비 교체가 아닌,
보안 운영 모델 자체의 전환을 목표로 설정

- 가시성: 매장·IoT·클라우드 전반 단일 시각 확보
- 대응 방식: 사람 중심 → AI·자동화 중심
- 운영 구조: 분산 운영 → 통합 플랫폼
- 보안 모델: 네트워크 중심 → AI 기반 통합 SOC

비즈니스 효과

60% 운영 효율 향상

30% 보안 운영 비용 절감

90% 위협 대응 시간 단축

도입 솔루션

IoT / OT 보안
Enterprise IoT Security
매장·풀필먼트 장비 가시성

네트워크 보안
차세대 네트워크 방화벽을 통한
매장·센터 트래픽 제어

접근 보안(SASE)
Prisma SASE Access
Zero Trust 기반 연결

클라우드·SaaS
Cortex Cloud
클라우드·SaaS 보호

보안 운영 (AI SOC)
Cortex XSIAM
AI 기반 탐지·대응

팔로알토 네트워스 고객 성공사례

폭발적으로 늘어나는 금융 데이터, 효율적인 보안 관리 방법은?

대한민국의 대표 핀테크·데이터 플랫폼 기업은 팔로알토 네트워스 클라우드 보안 자동화 플랫폼 구축을 통해운영 효율 30% 향상, 1.3M+ 기업 데이터 보호 및 응답 시간 수초 단위 단축을 이루며 금융 데이터 보안 성숙도를 크게 끌어올렸습니다.

위협 요소

대규모 데이터 처리 환경에서 제한된 보안 인력으로 클라우드 보안 운영해야 하는 구조적 한계 직면

- 매일 500GB~1TB 규모의 판매·금융 데이터를 처리하며, 130만 개 이상의 기업 데이터 보호가 필수적인 환경
- 소수의 인력이 클라우드 및 가상 환경 전체를 관리하고, 수동 분석과 대응에 과도한 시간과 리소스 소모 발생
- MTTD/MTTR 단축, 클라우드 보안 컴플라이언스 충족, 클라우드 네이티브 환경에 즉각 대응 역량이 핵심 요구사항

해결 방법

클라우드 보안 태세, 위협 자동 분석, 컴플라이언스 대응을 하나의 흐름으로 통합 구축

- 보안 자동화 → 수동 대응에서 자동 시나리오 기반 대응
- 실시간 위협 인텔리전스 → 탐지 정확도 향상
- 컴플라이언스 강화 → 인증 및 규제 준수
- 클라우드 네이티브 호환성 → 기존 환경과 완전 통합

비즈니스 효과

60%
운영 효율 향상

1.3b
금융 빅데이터 보호

10sec
응답 시간 단축

도입 솔루션

네트워크 보안
차세대 네트워크 방화벽을 통한 트래픽 제어

보안 자동화 및 대응
Cortex XSOAR 플레이북 기반 자동 탐지·분석·대응 및 SOC 운영 효율화

클라우드 보안 자동화
Cortex Cloud
CSPM 중심으로 클라우드 전반 운영 보안 및 규제 준수 관리

보안 운영 (AI SOC)
Cortex XSIAM
AI 기반 탐지·대응

팔로알토 네트웍스 고객 성공사례

멈추지 않는 금융 서비스를 위한 보안 전략

디지털 금융과 클라우드 확산으로 금융 데이터와 고객 정보를 노리는 랜섬웨어 공격이 증가하는 가운데, 금융 기관은 팔로알토 네트웍스의 AI 기반 보안 플랫폼을 도입해 금융 데이터를 보호하고 중단 없는 금융 서비스를 운영할 수 있는 보안 체계를 구축했습니다.

위협 요소

금융 데이터를 보호하면서도 금융 서비스 가용성을 유지할 수 있는 보안 체계 필요

- 금융 데이터를 노리는 랜섬웨어 및 데이터 탈취 공격 증가
- 금융 서비스 인프라의 클라우드 전환으로 공격 표면 확대
- 기존 보안 체계로는 계정 탈취 및 내부 확산 탐지 한계
- 금융 서비스 중단 시 고객 신뢰도 및 비즈니스 손실 발생

해결 방법

AI 기반 통합 보안 플랫폼을 구축하여 금융 데이터를 보호하고 서비스 가용성을 유지

- 금융 인프라 전반에 대한 보안 가시성 확보
- 계정 기반 접근 통제 및 이상 행위 탐지
- 랜섬웨어 및 데이터 탈취 공격 실시간 탐지
- 보안 운영 자동화를 통한 빠른 위협 대응

비즈니스 효과

100% 위협 사전 차단

60% 보안 운영 효율 향상

0건 운영 중단

도입 솔루션

네트워크 보안
차세대 네트워크 방화벽을 통한 트래픽 제어

보안 자동화 및 대응
Cortex XSOAR 플레이북 기반 자동 탐지·분석 · 대응 및 SOC 운영 효율화

Adv Threat Prevention
알려진 취약점 Cobalt Strike 등 Unknown C2 방지

Cortex XDR
멀웨어, 파일리스 및 랜섬웨어 프로세스 실시간 탐지/분석/차단

보안 운영 (AI SOC)
Cortex XSIAM
AI 기반 탐지·대응

Adv DNS Security
DNS쿼리의 무결성 검증 및 DNS C2 DNS터널링 방지

팔로알토 네트워스 고객 성공사례

매장 운영을 멈추는 랜섬웨어, 브랜드 신뢰를 지키는 보안 전략

POS 시스템과 매장 네트워크를 대상으로 한 결제정보 탈취, 악성코드 감염, 랜섬웨어 공격이 증가하는 가운데 F&B 기업은 팔로알토 네트워스 통합 보안 플랫폼을 도입해 매장 운영을 보호하고 안정적인 고객 서비스 환경을 구축했습니다.

위협 요소

고객 결제 정보를 보호하면서도 안정적인 서비스 운영을 유지할 수 있는 보안 체계 필요

- 결제 인프라를 노리는 결제정보 탈취 및 악성코드 공격 증가
- 지점과 본사 시스템 연결로 랜섬웨어 및 내부 확산 위험 증가
- 다수의 지점과 단말 환경으로 인해 보안 가시성 및 중앙 관리 한계

해결 방법

AI 기반 네트워크 및 엔드포인트 보호를 통합하여 고객 결제 데이터를 통합 관리할 수 있는 체계 구축

- 네트워크 및 결제 시스템에 대한 실시간 보안 가시성 확보
- 악성코드, 랜섬웨어 등 지점 단말 위협 탐지 및 차단
- 지점과 본사 시스템 간 보안 정책 기반 접근 통제
- 자동화된 보안 대응으로 운영 무중단 위협 차단

비즈니스 효과

100%
위협 사전 차단

10sec
대응 시간 단축

0건
운영 중단

도입 솔루션

네트워크 보안
차세대 네트워크 방화벽을 통한 트래픽 제어

보안 자동화 및 대응
Cortex XSOAR 플레이북 기반 자동 탐지·분석·대응 및 SOC 운영 효율화

클라우드 보안 자동화
Cortex Cloud
CSPM 중심으로 클라우드 전반 운영 보안 및 규제 준수 관리

보안 운영 (AI SOC)
Cortex XSIAM
AI 기반 탐지·대응

Palo Alto Networks
Product Brochure 2026



Daol TS

서울시 강남구 테헤란로 126, 대공빌딩 4층 2호, 14층 1호
www.daolts.co.kr

영업 문의 연락처
다올티에스(주) 김대봉 이사 010-2700-7384 daebong.kim@daolts.co.kr
다올티에스(주) 정인섭 차장 010-6471-7001 insub.chung@daolts.co.kr

© 2026 Palo Alto Networks, Inc. 미국 및 기타 관할 지역의 당사 상표 목록은 https://www.paloaltonetworks.com/company/trademarks.html에서 확인할 수 있습니다. 여기에 언급된 다른 모든 상표는 해당 회사의 상표일 수 있습니다.