한국투자증권

팰로 앨토 네트웍스

2026년 5월 13일

PANW – NASDAQ

Enterprise Software

매수

목표주가 $185

Idira: CyberArk IMPACT26 키노트 주요 내용

기업개요

팰로 앨토 네트웍스(PANW)는 차세대 방화벽(NGFW) 시장의 선도 기업으로, 현재는 이를 기반으로 더 넓은 사이버보안 플랫폼을 구축하고 있다. 회사의 플랫폼은 다양한 IT 환경에서 사용자, 애플리케이션, 데이터, 네트워크, 디바이스를 보호하는 데 초점을 맞추고 있다.

Summary

5월 12일 화요일, 당사는 텍사스 오스틴에서 열린 CyberArk의 연례 사용자 컨퍼런스인 IMPACT26 키노트에 온라인으로 참석했다. 예년과 마찬가지로 이번 행사의 핵심 주제는 ID 보안의 중요성 확대였다. 특히 사람, 기계, AI 에이전트 등 다양한 ID 유형을 아우르는 보안 필요성과, 모든 ID와 IT 환경을 통합적으로 보호하기 위한 CyberArk 플랫폼의 확장 방향이 중점적으로 다뤄졌다. 예상대로 PANW의 CEO Nikesh Arora도 키노트에 참여했다. 그는 PANW의 전반적인 플랫폼화 전략을 설명하면서, 기존에 분산되어 있던 여러 ID 보안 영역을 통합하는 것뿐 아니라, 더 나은 보안 성과를 위해 Identity를 PANW의 네 번째 전략 축으로 추가하는 것이 중요하다고 강조했다. 이러한 전략의 일환으로 PANW는 CyberArk를 Idira로 리브랜딩했으며, Oracle에서 오랜 기간 근무한 Sonny Singh을 Idira의 사장 겸 총괄책임자(President/GM)로 선임했다. 이에 따라 Identity Security(Idira)는 PANW의 기존 핵심 축인 Network Security(Strata), SecOps/Cloud(Cortex), AI Security(Prisma AIRS)에 더해 네 번째 전략 축으로 자리 잡게 됐다.

Key Points

행사에서 발표된 여러 제품 업데이트를 정리하기에 앞서, 먼저 핵심 내용을 간단히 짚어보면 다음과 같다.

- Idira는 CyberArk의 새로운 브랜드명으로, PANW의 차세대 Identity Security 플랫폼이다. Idira는 클라우드, SaaS, 온프레미스 등 모든 환경에서 사람, 기계, AI 에이전트 등 모든 종류의 ID를 찾아내고, 통제하며, 관리하는 역할을 한다.
- AI와 AI 에이전트의 확산은 이미 높아진 보안 위협 환경을 한층 더 복잡하게 만들고 있다. 이에 따라 Identity, 즉 ID 보안은 보안 체계의 핵심 기반으로서 중요성이 더욱 커지고 있다.
- 앞서 언급했듯이 Sonny Singh이 PANW에 합류해 Idira 사업을 이끌 예정이다. 그는 이전에 Oracle에서 36년간 근무했으며, 가장 최근에는 Oracle Financial Services Global Business Unit의 EVP 겸 GM을 맡았다.

(다음 페이지에 계속)

- 경영진에 따르면 현재 비인간 ID와 인간 ID의 비율은 109:1까지 높아졌다. 이는 2025년 IMPACT 행사 당시 82:1, 2024년 45:1에서 크게 상승한 수준이다. 여기서 비인간 ID는 코드, 컨테이너, 애플리케이션, API, 디바이스, IoT/OT, AI 에이전트 등 다양한 유형을 포함한다.
- 당사 채널 점검 결과와도 일치하게, 경영진은 ID 기반 보안 위협을 줄이기 위해 다양한 ID 보안 영역을 통합할 필요가 있다고 강조했다. 공격자는 자격증명을 탈취하고, 권한을 상승시키며, 시스템 내부에서 횡적으로 이동하는 방식으로 침투한다. 이를 막기 위해 IAM, PAM, ITDR, IGA, machine identity, AI Agent 등 여러 ID 보안 영역을 하나로 묶어 모든 ID 유형을 통합적으로 식별·통제·관리해야 한다는 설명이다. 특히 항상 부여된 고정 권한(standing privileges)이 아니라, 필요할 때만 부여되는 동적·일시적 권한(dynamic / just-in-time privileges)이 중요하다고 봤다.
- AI 시대에는 보호해야 할 AI 에이전트도 크게 두 가지로 나뉜다. 하나는 인간의 권한을 빌려 작업을 수행하는 위임형 에이전트(delegated agents)이고, 다른 하나는 사람의 직접적인 감독 없이 여러 워크플로를 실행하는 자율형 에이전트(autonomous agents)다. 이번 발표는 이 두 유형의 AI 에이전트를 모두 안전하게 보호하기 위한 기능 개선을 포함한다.
- 또한 PANW의 AI 애플리케이션 및 보안 플랫폼인 Prisma AIRS 3.0은 Idira와 기본적으로 통합될 예정이다.

제품 발표 및 주요 내용

Human Identity Security / Modern PAM

- **지속적인 가시성 확보:** Idira는 사용자, SaaS 애플리케이션, 클라우드 환경, 기타 ID 관련 영역 전반을 탐지해 어떤 권한이 어디에 존재하는지, ID가 어떤 방식으로 행동하는지, 어떤 데이터에 접근하는지를 파악할 수 있도록 지원한다.
- **동적·최소 권한 통제:** Idira는 고객이 기존의 정적인 권한 체계에서 벗어나도록 돕는다. 대신 고정 권한을 없애고, 특정 작업이나 특정 기간 동안에만 필요한 접근을 허용하는 zero standing privileges 및 just-in-time access 모델을 적용한다. 접근 권한은 지속적으로 평가되며, 실제로 필요한 경우에만 부여된다.
- **환경 및 워크로드 전반의 권한 통제:** Idira는 전통적인 IT 인프라를 넘어 웹 애플리케이션, SaaS, 클라우드, 서비스 계정 등 현대적인 환경까지 특권 접근 통제를 확장한다. 또한 Terraform 및 CLI 기반 자동화를 통해 고객이 배포 파이프라인 안에 ID 보안 통제를 직접 내장할 수 있도록 지원한다.
- **AI Remediation Agent:** AI Remediation Agent는 지속적인 가시성, 분석, 리스크 점수를 활용해 기업 전반의 인간 ID 리스크를 찾아내고 이를 개선하도록 돕는다. 리스크 점수에 대한 설명도 제공하며, 최종 판단과 실행에는 사람이 개입하는 human-in-the-loop 구조를 유지한다.

Non-Human Identity Security

- **탐지 및 중앙화된 가시성:** Idira는 관리 중인 비인간 ID와 관리되지 않는 비인간 ID를 모두 포함하는 통합 인벤토리를 제공한다. 여기에는 자동화된 서비스 계정, 마이크로서비스, 컨테이너, 워크로드, AI 에이전트 등이 포함된다. 이를 통해 복잡한 하이브리드·멀티클라우드 및 레거시 환경에서도 machine identity와 secrets를 식별할 수 있으며, 관련 리스크 점수와 접근 패턴도 함께 제공한다.
- **Secrets Hub:** PANW는 Secrets Hub의 신규 기능도 발표했다. 참고로 Secrets Hub는 CyberArk의 클라우드 기반 secrets 관리 솔루션이다. 사용자는 Secrets Hub를 통해 여러 퍼블릭 클라우드 환경, 외부 vault, CI/CD 파이프라인 등에서 secrets를 탐지하고, 온보딩하며, 중앙에서 관리할 수 있다. 개발자는 기존에 사용하던 도구를 그대로 활용하면서도, 보안 및 IT 조직은 중앙화된 거버넌스와 통제력을 확보할 수 있다.
- **Secure Workload Access:** PANW는 기계 환경에도 zero-trust 원칙을 적용하는 Secure Workload Access를 공개했다. 이 기능은 워크로드가 접근 권한을 받기 전에 자신의 ID를 먼저 증명하도록 요구한다. 장기간 유지되는 "forever secrets"에 의존하는 대신, PANW는 몇 분 내 만료되는 단기 machine identity인 SPIFFE ID를 도입했다. 참고로 SPIFFE는 소프트웨어 워크로드를 식별하고 인증하기 위한 오픈소스 표준이다.
- **자동화된 개선 조치:** Idira는 탐지된 비인간 ID를 자동으로 인벤토리에 등록할 수 있으며, SPIFFE 기반 자동 개선 조치 같은 도구를 활용해 기계 간 접근을 더 안전하게 만들 수 있다. 이 기능은 현대적인 환경뿐 아니라 레거시 환경도 지원한다.

AI Agent Identity Security

- **가시성 강화:** PANW는 Idira가 SaaS, 클라우드, 개발자 환경 전반에서 AI 에이전트를 탐지할 수 있는 기능을 발표했다. 또한 소유자, 권한, 접근 패턴 등을 기반으로 AI 에이전트의 리스크 점수를 산정할 수 있다.
- **동적 권한 부여:** Idira는 AI 에이전트에도 zero standing privileges와 just-in-time access를 적용한다. 즉, 에이전트는 특정 작업이나 일정 기간 동안에만 데이터 접근 권한을 부여받고, 작업이 끝나면 해당 권한은 제거된다.
- **거버넌스**: Idira는 AI 에이전트의 행동과 통신 내역에 대한 감사 로그를 생성한다. 여기에는 에이전트가 어떤 데이터에 접근했는지, 어떤 사용자를 대신해 작업을 수행했는지, 어떤 권한을 부여받았는지가 포함된다.

별도로 PANW의 보도자료에 따르면, 기존 CyberArk SaaS 고객은 현재 사용 중인 제품 등급에 따라 일부 Idira 기능을 사용할 수 있게 된다.

- **Traditional PAM / IT Standard 고객:** Traditional PAM 또는 IT Standard 고객은 새로운 가시성 기능과 사용자 경험 개선을 제공받는다. 다만 zero standing privilege, agentic identity, machine identity 기능은 추가 라이선스를 통해 사용할 수 있다.
- **Modern PAM / IT Enterprise 및 Developer 고객:** Modern PAM, IT Enterprise, Developer 고객은 추가 비용 없이 가시성, zero standing privilege, 사용자 경험 개선 기능을 사용할 수 있다. 다만 agentic identity와 machine identity security 기능은 별도 라이선스가 필요하다.
- **Workforce Access 고객:** Workforce Access 고객은 즉시 사용자 경험 개선 기능을 제공받으며, zero standing privilege, Traditional PAM, 더 넓은 범위의 agentic identity 및 machine identity 기능으로 업그레이드할 수 있다.
- **Machine and Identity Security 고객:** CyberArk Secrets Management 또는 Workload 고객은 추가 라이선스를 통해 Traditional PAM과 zero standing privilege 기능을 추가할 수 있으며, 이를 통해 Idira 플랫폼 내에서 관리를 통합할 수 있다.

투자 의견 제시 근거

PANW는 사이버보안 솔루션 분야의 대표 기업이다. 초기에는 기업 네트워크를 보안 위협으로부터 보호하는 하드웨어 및 소프트웨어 기반 방화벽에서 출발했지만, 이후 자체 개발과 적극적인 M&A를 통해 보다 폭넓은 사이버보안 플랫폼으로 사업을 확장해왔다. 현재 PANW는 사용자, 애플리케이션, 데이터, 네트워크, 디바이스를 다양한 환경에서 통합적으로 보호하는 보안 플랫폼을 구축하고 있으며, 향후 기업들의 보안 예산이 소수의 핵심 플랫폼으로 집중되는 과정에서 자연스러운 수혜를 받을 수 있는 기업이라고 판단한다. 종합적으로 보면 PANW는 신규 고객 확보, 기존 고객 대상 업셀·크로스셀, 신제품 확대, 해외 시장 확장 등 다양한 성장 동력을 보유하고 있다. 이를 바탕으로 향후에도 두 자릿수 매출 성장을 지속할 수 있을 것으로 예상되며, 동시에 수익성 개선도 이어질 가능성이 높다. 이러한 흐름이 확인될수록 주가 역시 밸류에이션 재평가를 받을 수 있다고 판단한다.

목표주가 산정 방법 및 위험 요인

12개월 목표주가 185달러는 2027년 예상 잉여현금흐름(FCF)에 28배 EV/FCF를 적용해 산출했다. 이는 동종업체 평균 23배 대비 프리미엄을 반영한 수준이다.

목표주가에 대한 주요 리스크로는 매크로 경기 둔화, 지정학적 리스크, 경쟁 심화, 성장 기회가 예상만큼 실현되지 않을 가능성, 인수 기업 통합 과정에서의 어려움, 그리고 보안 침해 발생 시 평판 리스크 등이 있다.