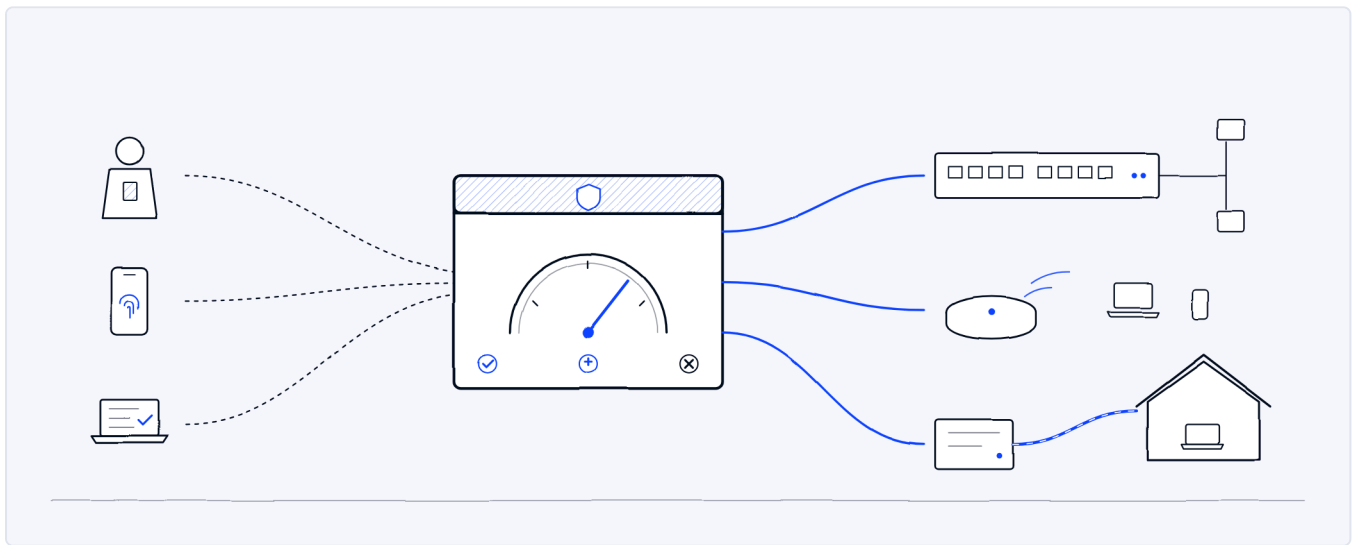




제로트러스트 PDP

보안은 무엇을 허용할지 결정하는 곳에서 정해집니다

NPass PDP는 과기정통부 제로트러스트 가이드라인 2.0의 구조를 따르는 정책결정지점 (Policy Decision Point)입니다. 사내 스위치와 무선 AP, 원격 접속까지 하나의 정책으로 제어합니다.

**기준**

과기정통부 제로트러스트 가이드라인 2.0 (2024.12)

역할

정책결정지점(PDP)

제어 대상

L2 스위치, 무선 AP, 원격 접속 게이트웨이 등

계정 연동

Okta, Microsoft Entra ID, Google Workspace

왜 제로트러스트인가

한 번의 로그인만 모든 접근을 허용하던 시대는 끝났습니다

최근 대형 침해 사고의 공통 원인은 개별 솔루션의 실패가 아니라 "내부는 안전하다"는 암묵적 신뢰였습니다.

내부망 전체를 암묵적으로 신뢰합니다

관리 서버 한 대가 뚫리면 내부 계정정보를 타고 전체가 무너집니다.

인증한 뒤에는 다시 확인하지 않습니다

VPN을 통과하거나 한 번 로그인하면 이동과 접근이 사실상 무제한입니다.

임직원과 기기의 권한을 실시간으로 관리하지 못합니다

퇴사자 계정과 미등록 장비가 내부망에 그대로 접근합니다.

가이드라인 2.0

여섯 가지 기본 원리와 NPass의 대응

No	기본 원리	NPass의 대응
01	모든 접근을 신뢰하지 않고, 명시적으로 확인한 뒤 허용	신뢰 평가 엔진이 접속 중에도 계속 검증. 의심스러우면 추가 인증을 요구하거나 세션을 끊음
02	일관되고 중앙집중적인 정책 관리와 접근제어	NPass PDP가 사내와 원격 접속의 정책을 한곳에서 결정
03	사용자와 기기의 관리, 강력한 인증	셀프서비스 포털의 기기 등록, 인증서 기반 802.1X 인증, 생체인증 MFA
04	리소스 분류와 최소 권한 부여	사용자와 기기에 따른 Dynamic VLAN, 허용된 서비스만 연결하는 원격 접속
05	논리 경계 생성, 세션 단위 접근 허용, 통신 보호	세션마다 발급하는 접속 토큰, 암호화된 원격 접속
06	모든 상태의 모니터링과 로그, 신뢰성의 지속 검증	통합 관리 콘솔의 접속 로그와 실시간 대시보드

NPass PDP 구조

확인하고, 결정하고, 집행합니다

여러 종류의 정책집행지점(PEP)을 함께 제어합니다. 접속 경로가 달라도 같은 정책이 적용됩니다.

확인하는 정보

누가, 어떤 기기로

기업 계정(Okta, Entra ID, Google Workspace; SAML, OIDC, SSO), NPass Authenticator의 생체인증 MFA, 기기 정보와 위치, 권한 등급

정책결정지점(PDP)

NPass PDP

신뢰 평가: 접속의 신뢰도와 위험도를 실시간 평가. 정책 결정: 허용, 거부, 추가 인증 요구. 지속 검증: 허용한 뒤에도 계속 확인하고 접속 토큰을 관리

정책집행지점(PEP)

결정을 집행하는 곳

사내 유선 L2 스위치(802.1X, Dynamic VLAN), 무선 AP, 원격 접속 게이트웨이와 커넥터

연동할 수 있는 PEP L2 스위치, 무선 AP, SDN, 원격 접속 게이트웨이, 5G 특화망, 5G 상용망, 비지상망(NTN)

신뢰 평가

접속할 때마다, 접속하는 동안 계속 평가합니다

01 신호 수집

접속 상황을 여러 각도로 봅니다

1차와 2차 인증 결과, 기기 정보와 OS, 필수 앱 설치 여부, 위치, 권한 등급을 실시간으로 모읍니다.

02 위험 평가

신뢰도와 위험을 함께 평가합니다

실시간 신뢰 평가와 위험 평가를 결합해 접속의 위험도를 판단합니다.

03 동적 판단

상황에 따라 다르게 대응합니다

접속을 허용하거나 거부하고, 필요하면 추가 인증을 요구합니다.

04 지속 검증

허용한 뒤에도 끝나지 않습니다

인증에 성공한 뒤에도 계속 검증해, 의심스러운 상황에 바로 대응합니다.

PDP가 제어하는 제품

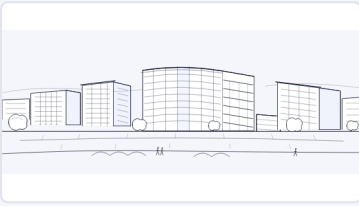
하나의 정책, 여러 접속 경로

제품	역할
유무선 인증 · IP 모빌리티	사내 유선과 무선 접속을 인증하고 IP마다 사용자를 파악합니다.
ZTNA 원격 접속	사무실 밖에서도 사내와 같은 권한, 같은 IP로 접속합니다.

넷큐브

주식회사 넷큐브는 2003년 설립 이후 네트워크 인증 한 분야에 집중해 왔습니다. 2005년 국내 최초의 802.1X 무선랜 인증 어플라이언스를 내놓았고, 인증 서버와 IP 관리, 인증서 발급의 핵심 엔진을 모두 직접 개발합니다. 지금은 기업 업무망을 지키는 NPass, 이동통신망에 연결되는 단말과 현장을 보호하는 NSure, 5G 특화망 단말 공급까지 넓혔습니다.

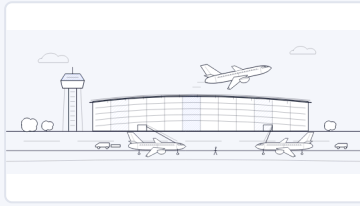
가장 큰 업무망에서 먼저 검증했습니다



세계 가전 1위 기업

15년 이상 운영

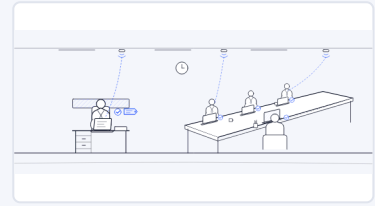
본사와 글로벌 연구소 캠퍼스 전체의 유무선 네트워크 인증과 IP 모빌리티를 15년째 운영하고 있습니다.



대한항공

220개 거점

본사를 포함한 글로벌 220개 거점 전체의 유무선 통합 인증과 IP 모빌리티를 구축해 운영하고 있습니다.



정부·공공기관

5G 업무망·정부망 인증

과기정통부, 행정안전부, 기획재정부, 감사원, 특허청, 우주항공청, 수자원공사, 해양경찰청 등에 인증솔루션을 공급했습니다.

제로트러스트, 정책을 결정하는 곳부터 시작해 보시겠습니까

가이드라인 2.0 기준의 적용 범위와 단계별 도입 방법을 상담에서 안내드립니다.

도입 상담: sales@netcube.com · IP 가시성 무료 진단 신청: netcube.com

서비스 · 제품 문의

sales@netcube.com

전화

02-557-6801

도입 솔루션 기술 지원

support@netcube.com

주소

서울 금천구 가산디지털1로 204, 반도아이비밸리 608호