



AI TRUST IDENTITY PLATFORM

TRUVIX

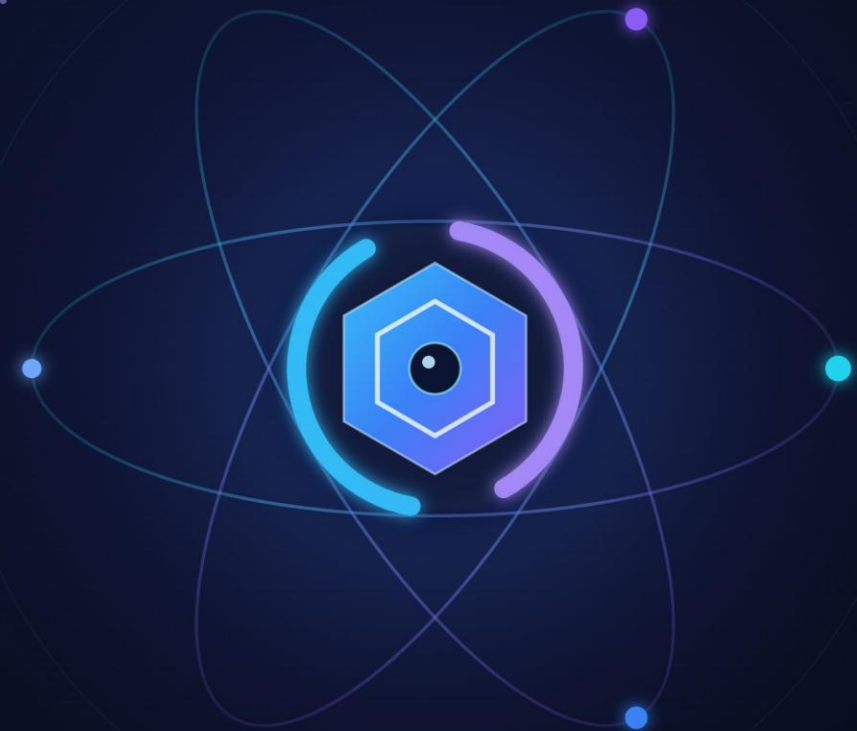
트루빅스 · 인증을 넘어 접속의 신뢰를 판단하는 제로트러스트 인증 플랫폼

인증에 성공했는지를 넘어, **지금 이 접속을 신뢰할 수 있는지** 판단합니다.

Zero Trust

Identity Trust

Adaptive Authentication



AI TRUST IDENTITY PLATFORM

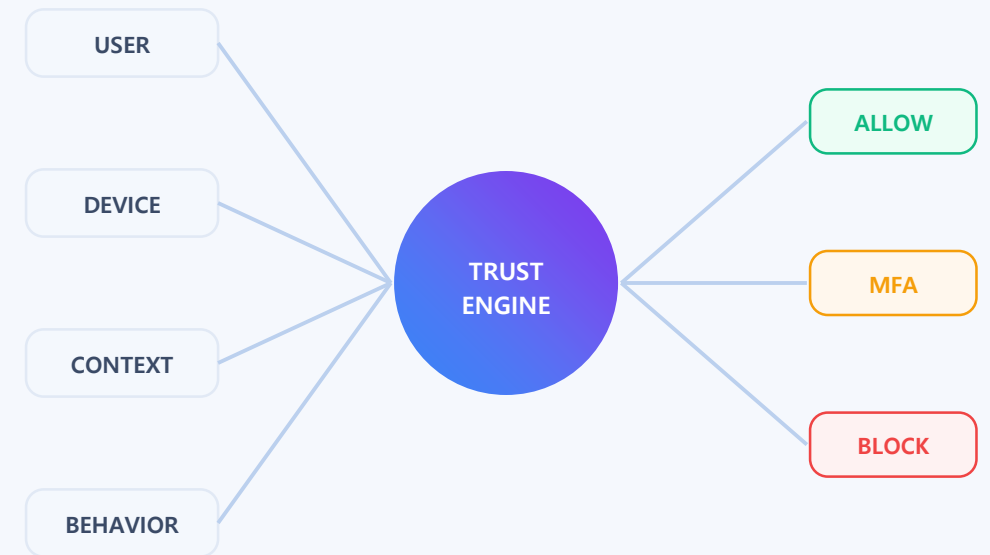
신뢰를 판단하고, 위험에 따라 접근을 결정합니다

사용자·단말·접속환경과 인증 이력을 종합 분석해 지금 이 접속의 신뢰도를 판단하고, 위험수준에 따라 인증과 접근정책을 동적으로 적용하는 제로트러스트 플랫폼입니다.

Zero Trust

Identity Trust

Adaptive Authentication



인증 성공만으로는 충분하지 않습니다

"인증에 성공했는가"를 넘어 "지금 이 접속을 신뢰할 수 있는가"를 판단합니다.

기존 인증

인증 성공/실패만 확인

ID / PW



MFA



접근 허용

자격증명만 맞으면 통과 — 누가·어디서·어떤 상태로
접속하는지는 판단하지 않습니다.

VS

TRUVIX

접속의 신뢰도를 판단

Identity

Device

Context

Behavior



Trust Evaluation



Policy Decision



Allow · MFA · Restrict · Block

하나의 플랫폼, 네 가지 신뢰 요소

접속을 구성하는 네 가지 요소를 함께 분석해 신뢰도를 산정합니다.



사용자 신뢰

Identity Trust

계정 상태·인증 이력.
인증수준으로 신뢰도 판단.



단말 신뢰

Device Trust

단말·브라우저·등록정보
와 환경정보로 신뢰성 확인.



접속환경 신뢰

Context Trust

IP·위치·시간·네트워크
등 상황적 위험을 판단.



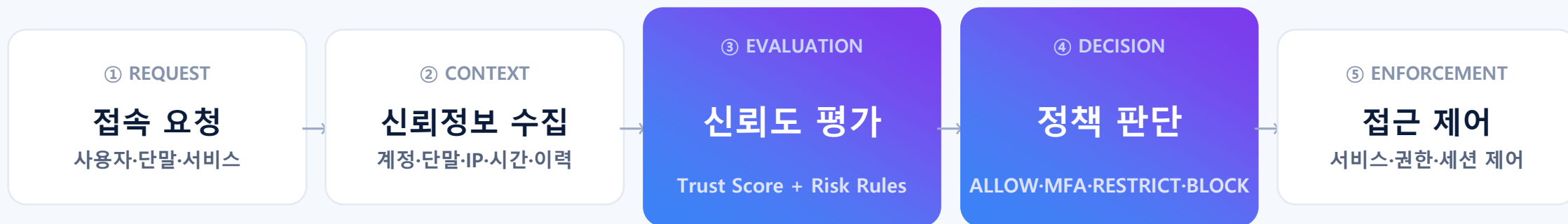
행위 신뢰

Behavior Trust

로그인 이력·이상행위
패턴으로 차이를 평가.

요청은 검증을 거쳐 결정에 이릅니다

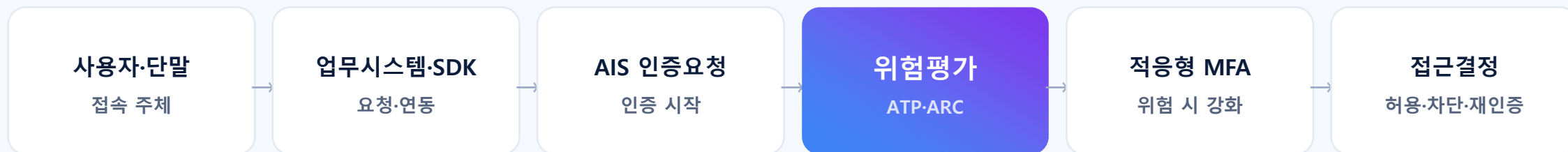
모든 접속 요청은 신뢰도를 평가하고, 정책 판단을 거쳐 최종 접근 수준이 결정됩니다.



TRUVIX의 차별성은 ③ **신뢰도 평가**와 ④ **정책 판단** — 접속의 신뢰수준에 따라 결정이 달라집니다.

요청은 실제 인증 흐름을 거쳐 결정됩니다

모든 접근 요청이 인증·위험평가·MFA를 통과하는 실제 흐름 — 전 구간은 하이브리드 TLS로 보호됩니다.



전 통신구간 하이브리드 TLS 보호

고전 + 양자내성 결합 — 선수집·후복호(HNDL) 위협까지 대비합니다.

X25519 · 고전 ECDH

ML-KEM-768 · 양자내성 KEM

TLS 1.3

위험도와 환경에 맞는 인증을 적용합니다

일반 접속에는 편리한 인증을, 위험도가 높아지면 더 강력한 인증을 요구합니다.

NXOTP

Mobile OTP

모바일 앱 기반 일회용 코드.

안드로이드·iOS

PUSH / QR 인증

Push · QR Scan

앱 알림 승인 · QR 스캔 인증.

실시간 승인

FIDO / FIDO2

U2F · WebAuthn

보안키 · 생체
복제 불가 기기전용(device-bound)

고신뢰 · 패스워드리스

Passkey

Mobile · Browser · Security Key

모바일 패스키 · 브라우저
기기전용 신뢰도 연계

적응형 신뢰

PKI

X.509

공인·사설 인증서 신원 인증.

인증서

외부 IdP

SAML · OIDC

기존 IdP·소셜 로그인 연계.

페더레이션

HW OTP

Hardware

전용 하드웨어 기반 OTP.

카드·토큰형

정책에 따라
인증 수준 변화

어떤 시스템과 연결됩니까

표준 프로토콜부터 SDK·API 연계까지 다양한 업무 및 인프라 환경과 연결합니다.



SDK 연동

다국어 SDK

Java·Python·NET·Node·PHP 탑재형 접근통제.

5개 언어



SAML 2.0

표준 웹 SSO

SAML 2.0 SP 연동, 무수정 SaaS 연계.

SSO · IdP



OIDC · OAuth 2.0

OpenID Connect

토큰 기반 웹·모바일 앱 인증.

OP · JWT



RADIUS

VPN · 네트워크

VPN·네트워크 장비 인증을 정책과 연계.

AAA · VPN



REST API

제어 API

인증검증·세션종료·토큰폐기 원격 제어.

REST · API



포털 리다이렉트

웹 액세스 포털

인증 포털로 리다이렉트해 레거시 웹을 보호.

라이브러리 연동

적용 환경 업무포털 · ERP · 그룹웨어 · VPN · VDI · SaaS · 관리자시스템 · 네트워크 장비

신뢰도를 계산하고, 규칙으로 판단합니다

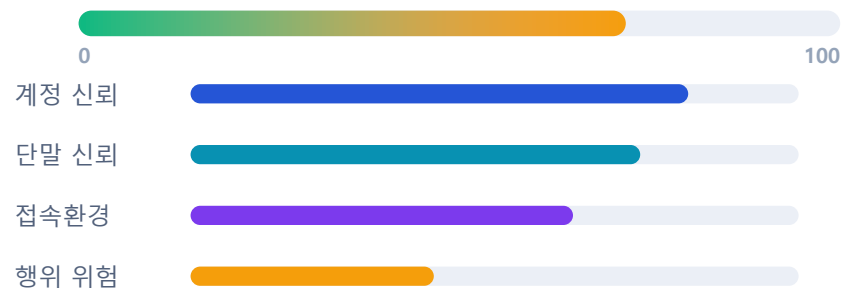
로그인 이력과 현재 접속환경을 분석해 신뢰도를 산정하고, 위험수준에 따라 조치를 결정합니다.

Trust Score

신뢰도 산정

72

SAFE



Adaptive Policy

신뢰수준별 대응

● SAFE

→ 정상 접근

● CAUTION

→ 추가 인증

● DANGER

→ 인증 강화 · 접근 제한

● BLOCK

→ 접속 차단

ATP · Account Trust Profile

ARC · Adaptive Risk Control

신뢰도를 계산하고, 규칙으로 판단합니다

ATP가 접근의 신뢰도를 점수화하고, ARC 규칙엔진이 이상행위를 탐지해 정책 액션을 실행합니다.

ATP 신뢰도

Adaptive Trust Profiling

단말



위치



행위



네트워크



접근 상황을 실시간 점수화

ARC 규칙 엔진

Adaptive Risk Control

- 불가능 이동
- MFA 피로 공격
- 신규 단말
- 휴면 계정
- 위험 네트워크
- 동시 세션
- 비정상 시간
- 권한 상승
- IOC 매칭

탐지된 규칙에 따라 정책 액션 실행

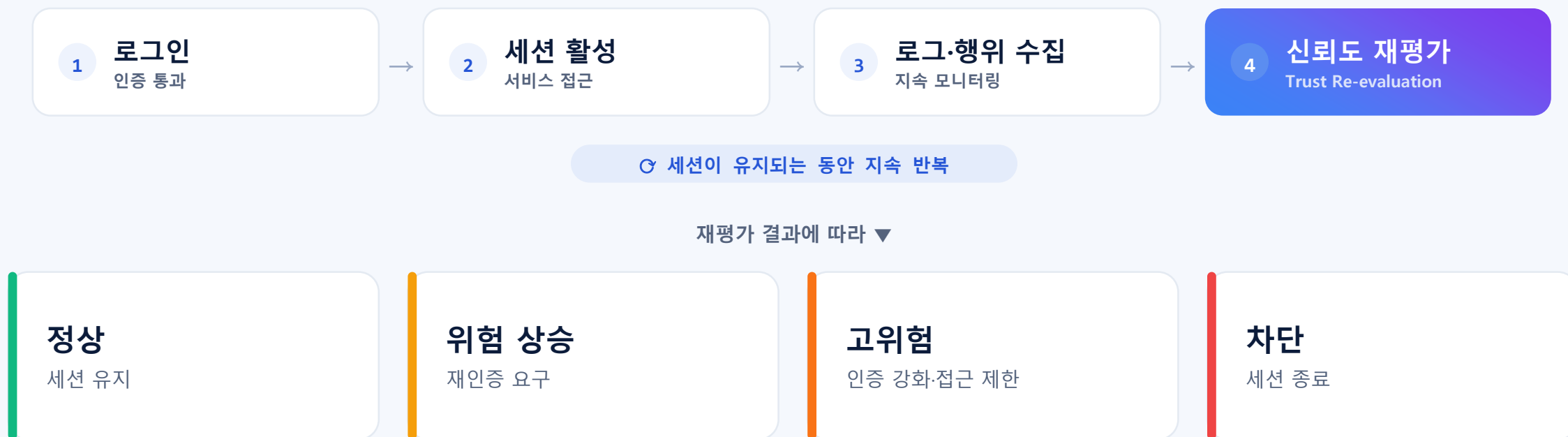
정책 액션

Policy Action

- 추가 인증**
MFA 상향 요구
- 접근 제한**
기능·권한 축소
- 세션 종료**
활성 세션 차단
- 계정 잠금**
자격 일시 정지

로그인 이후에도 신뢰는 계속 확인됩니다

접속 이후에도 로그.행위를 수집해 신뢰도를 재평가하고, 세션 탈취·복제는 소지증명으로 차단합니다.



제로트러스트를 미래 암호 보안까지 확장합니다

PQC는 TRUVIX 플랫폼을 미래 암호환경까지 확장하는 보안 기술입니다.

FUTURE-READY SECURITY

미래의 암호위협까지 대비합니다

현재의 인증·접근보호를 넘어, 양자내성 하이브리드 키교환을 전 구간에 적용하고 암호 민첩성을 확보했습니다.

Hybrid Cryptography

기존 암호 + PQC 병행

Crypto Agility

알고리즘·Provider 교체 대응

PQC Key Exchange

양자내성 키교환 적용

PQC Signature

양자내성 전자서명 확장

장기 보호가 필요한 인증·보안정보에 대해 Harvest Now, Decrypt Later와 같은 미래 암호위협에 대비한 PQC 적용 구조.



국제·국가 표준을 기반으로 설계했습니다

제로트러스트·인증·암호 표준 위에서 동작하며 국내 규제 프레임워크 연계를 고려합니다.



Zero Trust

아키텍처 원칙

지속 검증·최소권한 기반 설계.

NIST SP 800-207

KISA 2.0



Authentication

국제 인증 표준

패스워드리스 공개키 인증·표준 채널.

FIDO2 · WebAuthn

TLS 1.3



Security & Compliance

국가 보안 프레임워크

N2SF 등급별 인증 강도 요구·암호모듈 연계.

N2SF

KCMVP 연계

확장 대응 · NIST FIPS 203/204/205(PQC) · WS-Federation · SCIM 2.0 · LDAP/AD 동기화

변화하는 접속환경, 인증만으로는 충분하지 않습니다

접속 환경과 위협은 빠르게 바뀌고 있습니다. TRUVIX는 인증을 넘어 접속의 신뢰를 판단합니다.



복잡해진 접속환경

Cloud · SaaS · Remote

경계가 사라진 환경에서 접속은 어디서든 발생합니다.



고도화되는 계정공격

Credential Attack

탈취·피싱·MFA 피로 공격이 자격증명을 노립니다.



확대되는 인증수단

Passwordless · MFA

다양한 인증을 상황에 맞게 조합해야 합니다.



변화하는 보안기준

Zero Trust · N2SF

규제와 기준이 지속 검증·등급제로 이동합니다.

지금 도입하고, 미래의 위협까지 대비하세요

인증·위험분석·양자내성암호를 하나의 플랫폼으로 통합해 운영 부담을 줄이고 보안 수준을 높입니다.



통합 플랫폼

One Platform

인증·위험분석·암호를
하나로 운영·관리.



폭넓은 연동

Broad Integration

SDK·SAML·OIDC·RADIUS
·포털까지 유연 연동.



표준 준수

Standards

NIST·KCMVP·제로트러스트
국제·국가 표준 대응.



점진적 PQC 전환

Crypto Agility

기존 인증 흐름을 유지하며
양자내성 암호를 단계 적용.

TRUVIX는 인증에 성공했는지를 넘어, 지금 이 접속을 신뢰할 수 있는지를 판단합니다.

TRUVIX로 인증을 넘어, 신뢰 기반의 접속제어 환경을 구축하세요.

CONTACT

제품 도입 문의

TRUVIX 도입 상담과 기술 지원을 도와드립니다. 아래 채널로 문의해 주세요.

웹사이트

<https://www.nexhatch.co.kr/truvix>

이메일

sales@nexhatch.co.kr

전화

010-9686-1345 / 032-349-1117

문의 유형

제품 도입 · 기술 상담

