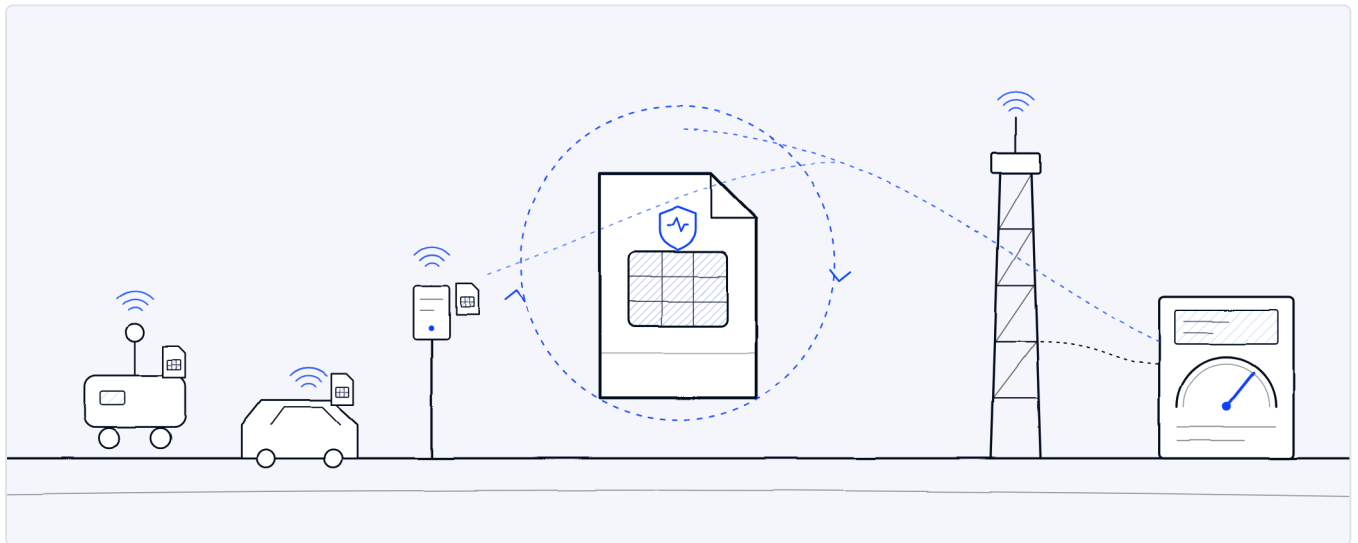




NSure USIM

IoT 단말을 위한 USIM 기반 제로트러스트 보안

NSure USIM은 단말 OS가 아니라 USIM 안에서 동작하는 이동통신 단말 보안 솔루션입니다. 단말의 망과 셀 정보, 무선 신호 상태를 USIM 안에서 상시 수집하고, AI가 단말별 신뢰도를 실시간으로 산출해 위험도에 따라 단계적으로 대응합니다.



실행 위치

USIM 내부(Secure Element)

판단 방식

단말별 신뢰도(Trust Score 0~100) 상시 산출

배포

USIM 교체로 적용, 하드웨어 추가 없음

망 연동

기존 이동통신망 표준 인터페이스 사용

문제

IoT 단말이 늘수록 커지는 보안 사각지대

서비스 로봇, 무인 기기, 센서 단말처럼 이동통신망에 연결되는 IoT 단말에는 세 가지 구조적 제약이 있습니다.

01

보안 앱을 설치하기 어렵습니다

화면과 입력장치가 없고 저장공간과 연산 자원이 제한적입니다. 백신이나 MDM 같은 보안 앱이 들어갈 자리가 없습니다.

02

OS에 의존하는 보안에는 한계가 있습니다

보안 앱은 단말 OS 위에서 동작합니다. OS가 감염되거나 권한을 빼앗기면 그 위의 보안 기능도 함께 무력화됩니다.

03

현장에 사람이 없습니다

단말이 무인 환경에 흩어져 있어 이상 징후를 현장에서 알아챌 사용자가 없습니다. 침해가 일어나도 인지와 대응이 늦어집니다.

불법 기지국(Fake gNB) 유도

단말을 가짜 기지국에 붙여 트래픽을 가로채거나 서비스를 방해합니다.

USIM 복제와 탈취

단말의 통신 신원을 복제해 과금 사기나 위장 접속에 악용합니다.

비정상 위치와 접속 패턴

탈취된 단말이 정상 범위를 벗어난 시각, 위치, 경로로 활동합니다.

왜 USIM인가

보안을 실행하는 곳을 OS에서 USIM으로 옮깁니다

USIM은 이미 모든 단말에 들어 있는 신뢰 하드웨어(Secure Element)입니다. 통신사가 발급하고 관리하며, 위조와 변조가 어렵고, 단말 OS와 무관하게 독립적으로 동작합니다.

01

모든 단말에 이미 들어 있습니다

하드웨어를 추가하지 않고 모든 이동통신 단말에 탑재된 USIM을 활용합니다. USIM을 교체하는 것이 곧 배포 절차입니다.

02

OS와 독립적으로 실행됩니다

보안 로직이 Secure Element 안에서 실행됩니다. OS가 감염되거나 우회되어도 상태 수집과 정책 실행은 계속됩니다.

03

통신 계층을 직접 관측합니다

망 접속 상태와 무선 신호 정보를 통신 계층에서 직접 관찰하므로, 앱 계층에서는 보이지 않는 위협을 포착합니다.

왜 제로트러스트인가

한 번의 인증에서 상시 검증으로

NSure USIM은 접속하는 순간이 아니라 사용하는 내내 단말을 검증합니다.

구분	경계 기반 보안(기존)	제로트러스트(NSure USIM)
신뢰 판단 시점	접속할 때 한 번 인증	사용 중 상시 재검증
판단 근거	자격 증명(누구인가)	단말의 현재 상태(지금 어떤가)
인증 이후의 이상 행위	탐지 수단 없음	AI가 즉시 탐지해 신뢰도에 반영
대응 방식	차단 아니면 허용	위험도에 따른 단계적 대응

시스템 구성

세 가지 구성요소가 하나의 보안 루프로 동작합니다

넷큐브가 직접 개발한 USIM 제로트러스트 아키텍처입니다.

온-SIM 보안 에이전트

USIM 안에서 독립 실행

단말의 망과 셀 정보, 무선 신호 상태를 상시 수집하고 이상 이벤트를 감시합니다. 서버가 내린 대응 정책을 OS를 거치지 않고 직접 실행합니다.

NSure 보안 서버

AI 분석과 정책 결정(PDP)

수집한 데이터를 AI로 분석해 이상을 탐지하고, 단말별 신뢰도(Trust Score 0~100)를 상시 산출합니다. 점수 구간에 따라 대응 정책을 결정합니다.

보안 채널

상시 양방향 연결

단말 상태 데이터는 위로, 대응 정책과 실행 명령은 아래로 흐릅니다. 기존 이동통신망의 표준 인터페이스를 그대로 써서 망을 고칠 필요가 없습니다.

적용 분야

제로트러스트가 필요한 현장

보안 요구가 높고 무인으로 흩어져 운영되는 환경일수록 USIM 기반 상시 검증의 효과가 큼니다.

공공·국방 무인기기

순찰 로봇, 감시 장비, 원격 계측 단말

높은 보안 요구와 무인 운영이 겹치는 영역입니다. 단말을 위장하거나 탈취하려는 시도를 통신 계층에서 일찍 포착합니다.

스마트팩토리·산업 IoT

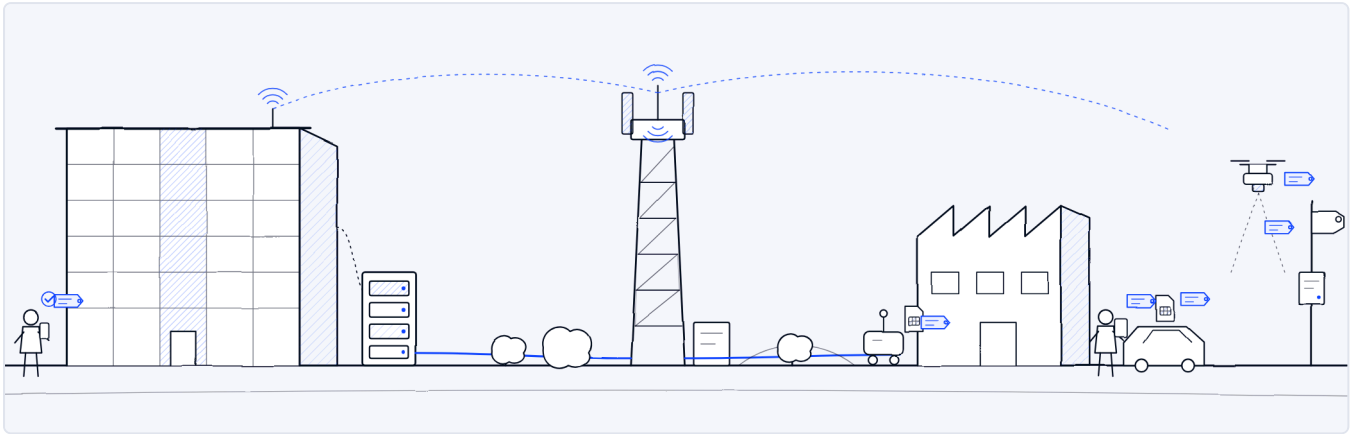
생산 설비 센서, AGV, 품질 검사 장비

설비가 멈추면 큰 손실로 이어질 수 있습니다. 위험 등급에 따라 대응하므로 과하게 차단하지 않고 위협을 관리합니다.

물류·차량 M2M

차량 관제 단말, 물류 추적기, 텔레매틱스

전국에 흩어져 이동하는 단말입니다. 비정상적인 위치와 경로 패턴을 신뢰도에 반영해 탈취와 오용을 탐지합니다.



네티큐브

주식회사 네티큐브는 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.

무인 단말의 보안, USIM에서 시작해 보시겠습니까

적용 단말과 이동통신망 환경을 알려 주시면 도입 방법을 상담에서 안내드립니다.

도입 상담: sales@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