toss

보안위협에 맞서 싸우기 위한 무기
보안 솔루션 구축 전략

비바리퍼블리카
지정호 CISO

금융의 모든 것
토스에서 쉽고
간편하게

토스는 누구에게나 쉽고 상식적인 금융을 만들어 가고 있습니다.

2015년 공인인증서 없이 쉽고 빠르게 송금할 수 있는 간편 송금 서비스를 시작으로
은행, 증권, 결제 등 다양한 영역에서 혁신적인 금융 경험을 선보이며 국민 2명 중 1명이 사용하는 모바일 금융 플랫폼으로 성장했습니다.

토스는 모두를 위한 새로운 금융입니다.

국민 2명 중 1명이 사용하는 금융 서비스

20대의 95%
20대 가입자 수: 약 555만 명

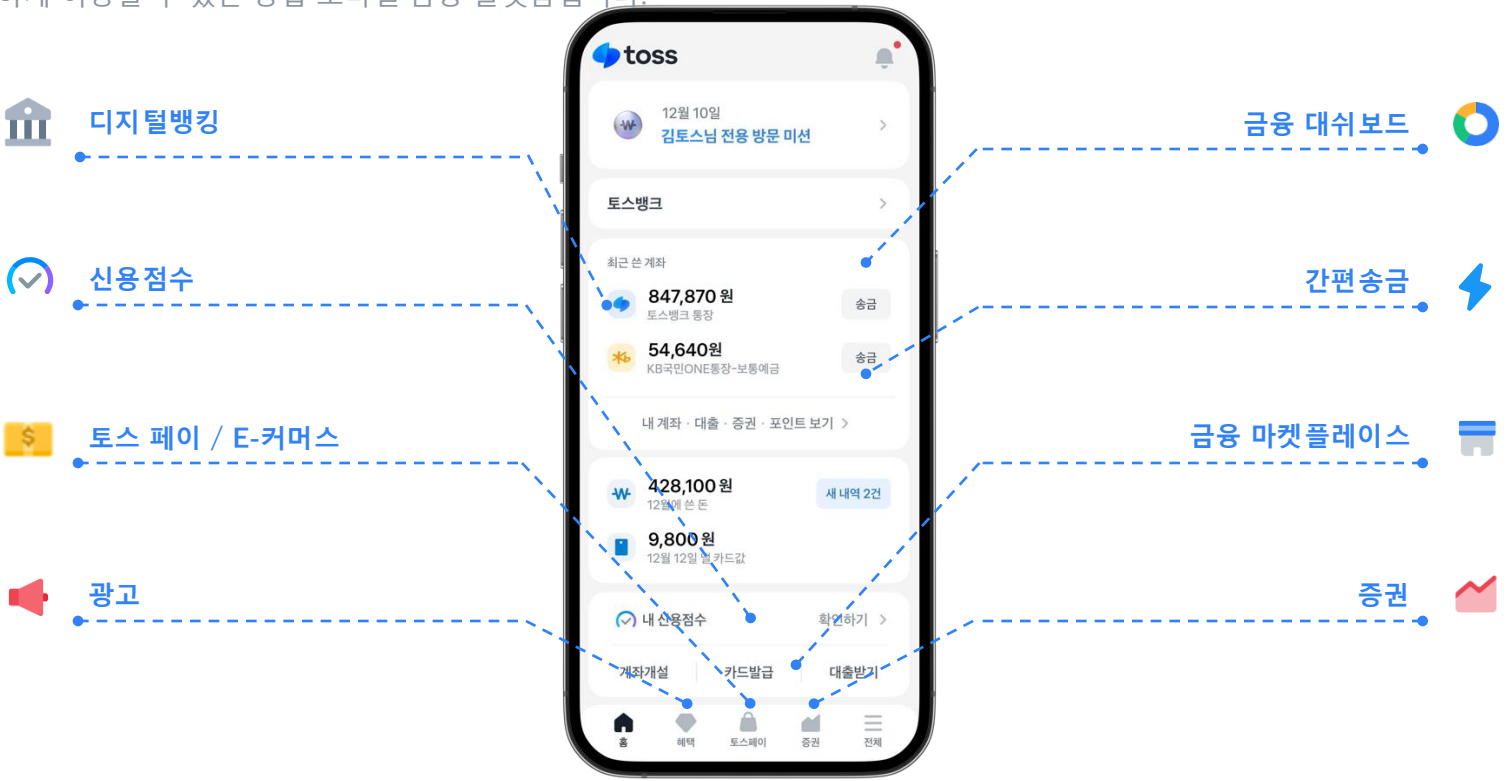
30대의 87%
30대 가입자 수: 약 578만 명

40대의 77%
40대 가입자 수 : 약 588만 명

2025.06. 행정안전부 주민등록인구통계 및 토스 연령대별 가입자 수 기준

금융 수퍼앱, 토스

토스는 앱 하나로 은행, 증권, 결제 등 100종 이상의 다양한 서비스를
쉽고 간편하게 이용할 수 있는 종합 모바일 금융 플랫폼입니다.



서비스 현황

누적 가입자 수

2천 9백 만

월간 활성 사용자 수

2천 4백 만

서비스 수

100 +

누적 송금액

710조

누적 계좌 등록 수

2억 3천 만

누적 카드 등록 수

8천 9백 만

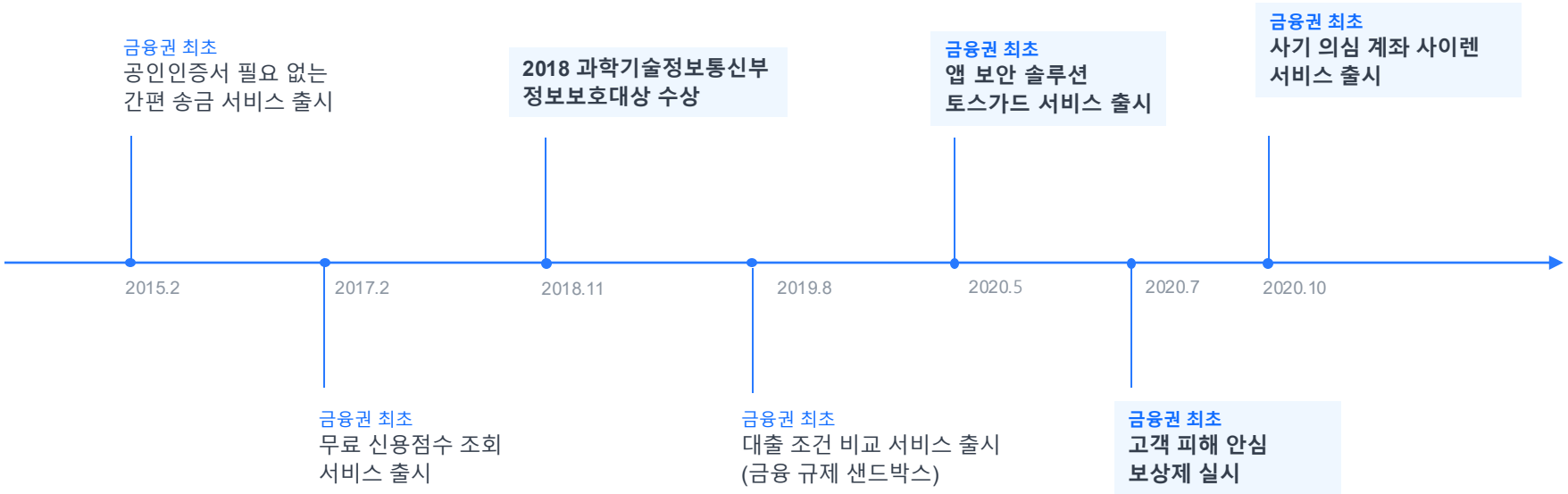
2025.06.30 기준

사용은 간편하게
보안은 강력하게

토스는 고객의 신뢰와 보안을 최우선 가치로 삼고 있습니다.
보안에 대한 끊임없는 투자와 자발적인 인증 취득, 정교한 기술 개발로 간편하고 안전한 금융 서비스를 만들어 갑니다.

혁신의 여정

토스는 금융을 중심으로 다양한 혁신 사업을 전개하고 있습니다.
특히, 소비자의 관점에서 더 저렴하고, 더 좋은 가치를 담은 서비스를 만들어 나가고 있습니다.



혁신의 여정

토스는 금융을 중심으로 다양한 혁신 사업을 전개하고 있습니다.
특히, 소비자의 관점에서 더 저렴하고, 더 좋은 가치를 담은 서비스를 만들어 나가고 있습니다.

안전한 금융 서비스

토스는 안전한 모바일 금융 서비스를 제공하기 위해
정보보호 부문에 대한 업계 최고 수준의 투자를 지속하고 있습니다.

업계 최고 수준의 보안 인력

- 전 계열사에 구축한 자체 화이트해커 팀이 해킹 기술 연구, 보안성 향상에 힘쓰고 있음
- 금융보안원 주최 금융보안 위협대회 우승 등으로 높은 수준의 보안 기술력 인정 받음
- 국내 최고 수준의 보안 인력 약 50여명이 토스의 모든 서비스를 더욱 안전하게 만들고 있음

고객 보호를 위한 기술 / 정책

- 고객 보호를 위한 보안 시스템 직접 개발 및 운영:
  - ✓ 이상행위 감지 시스템(FDS), 악성앱 탐지 솔루션, 모바일 보안 솔루션 등
- 보이스피싱 전담 모니터링 시스템 구축해 이상행위 탐지 시, 해당 고객 연락을 통한 상황 점검 및 자산 보호 조치
- 보이스피싱, 명의도용 등으로 금전 피해 입은 고객에게 보상하는 '토스 안심보상제' 업계 최초 시행

글로벌 수준의 보안 체계

- 국내외 주요 정보보호 인증 자발적으로 취득하며 정보보호 역량 고도화
- 외부 컨설팅 도움 없이 자체 인력으로 국제 표준에 부합하는 정보보호시스템 운영
- 보유 인증 : ISO/IEC 27001, ISO/IEC 27701, ISO/IEC 27017, PCI-DSS, APEC CBPR

정보보호 관리체계

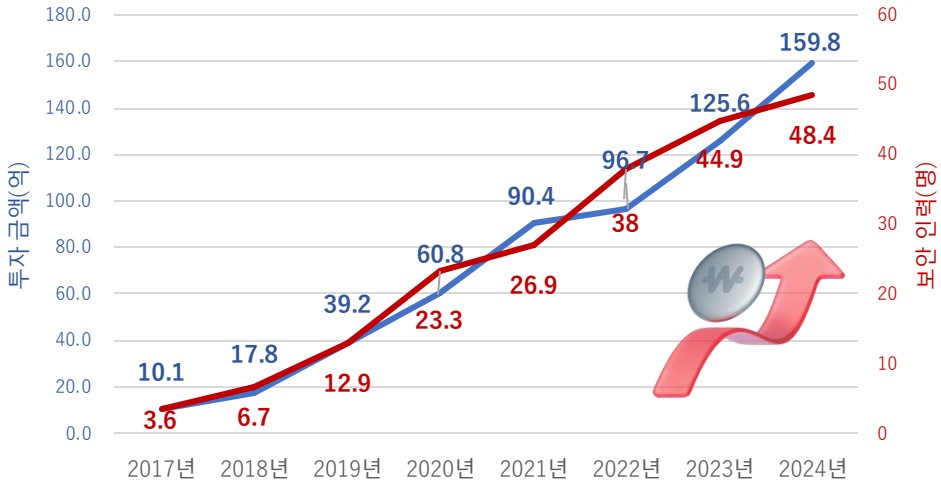
토스는 정보보호 관리체계를 균형 있게 발전시키기 위해 글로벌 수준의 정보보호 표준을 적용하고
심사 기관의 평가를 받아 인증을 유지하고 있습니다.

ISO/IEC 27001	ISO/IEC 27701	ISO/IEC 27017
ISMS-P	PCI-DSS	APEC CBPR

지속적인 정보보호 투자

토스는 지속적으로 정보보호에 투자하고 있습니다.
토스는 금융분야 최초로 2018년부터 매년 정보보호공시를 통해 정보보호 투자현황을 공시

IT 대비 보안 투자 금액 10.5% ~ 17.8%
IT 대비 보안 인력 8.0% ~ 12.0%



NO	공시연도	자율/의무	기업명
8	2025	자율	(주) 비바리퍼블리카
7	2024	자율	(주) 비바리퍼블리카
6	2023	자율	(주) 비바리퍼블리카
5	2022	자율	(주) 비바리퍼블리카
4	2021	자율	(주) 비바리퍼블리카
3	2020	자율	(주) 비바리퍼블리카
2	2019	자율	(주) 비바리퍼블리카
1	2018	자율	(주) 비바리퍼블리카

정보보호 전담 조직

Information & Security Tribe

Security Policy
- 정보보호 관리체계 운영
- 보안성 검토 및 심의

Personal Data Protection
- 개인정보 관리체계 운영
- 개인정보 데이터 보안 관리

Security Build
- 계열사 보안조직 구축 지원
- 계열사 보안점검 지원

Security Purple
- 보안위협 모니터링 체계 구축
- 보안 및 점검 기능 개발

Security Green
- 보안위협 분석 및 대응
- 보안시스템 구축 및 운영

IT Innovation
- 망분리 등 사내 IT 인프라 운영
- 업무용 단말기 보안 관리

Compliance Platform
- 개인정보 관리 시스템 개발
- 데이터 리스크 탐지 시스템 개발

보안 관제
- 24X365 보안 모니터링 지원
- 보안 이벤트 분석 및 대응 지원

위협과 신뢰의 사이를 지키는 보안 솔루션

보안 솔루션은 수 많은 보안 위협으로부터
고객의 자산과 데이터, 서비스 환경, 임직원 업무환경을 지켜주는 무기입니다.

보안 솔루션이란?

📌 보안 솔루션이란?

보안 솔루션(Security Solution)은

정보 자산을 위협으로부터 보호하기 위해 설계된 기술적·관리적 도구와 시스템의 집합입니다.

이는 기업의 내부 시스템, 네트워크, 데이터, 사용자, 기기 등을 안전하게 보호하고

무단 접근, 정보 유출, 악성 공격, 시스템 침해 등의 사이버 위협을 예방·탐지·대응·복구하는 데 핵심적인 역할을 합니다.

어떤 보안 솔루션이 필요한가?

어떤 보안 솔루션이 필요한가?

회사에서 도입해야 할 보안 솔루션은 조직의 규모, 산업군, 보유 정보의 민감도, 보안 리스크 수준에 따라 달라지지만,
모든 기업이 고려해야 할 보안 솔루션의 핵심 카테고리는 다음과 같습니다. (by ChatGPT)

ChatGPT

🔐 1. 네트워크 보안

- **방화벽 (Firewall)**: 내부 네트워크와 외부의 경계를 보호
- **IDS/IPS**: 침입 탐지 및 차단 시스템
- **VPN**: 원격 근무 환경에서 안전한 통신 제공

✅ **추천 솔루션**: Palo Alto, Fortinet, Cisco ASA

🖥️ 2. 엔드포인트 보안

- **백신/안티멀웨어**: 바이러스 및 악성코드 탐지
- **EDR (Endpoint Detection & Response)**: 고급 위협 탐지 및 대응
- **DLP (Data Loss Prevention)**: 내부 정보 유출 방지

✅ **추천 솔루션**: CrowdStrike, SentinelOne, Symantec DLP

☁️ 3. 클라우드 보안 (클라우드 인프라 사용하는 경우)

- **CSPM (Cloud Security Posture Management)**: 설정 오류 탐지 및 리스크 관리
- **CWPP (Cloud Workload Protection Platform)**: 클라우드 워크로드 보호
- **CASB (Cloud Access Security Broker)**: SaaS 보안 및 사용자 활동 가시성 확보

✅ **추천 솔루션**: Wiz, Lacework, Netskope, Prisma Cloud

🧑‍💼 4. 인증 및 접근 제어

- **MFA (Multi-Factor Authentication)**: 다단계 인증
- **SSO (Single Sign-On)**: 단일 로그인 시스템
- **IAM (Identity & Access Management)**: 사용자 권한 제어 및 감사

✅ **추천 솔루션**: Okta, Microsoft Entra ID, Duo Security

🔍 5. 로그 수집 및 위협 대응

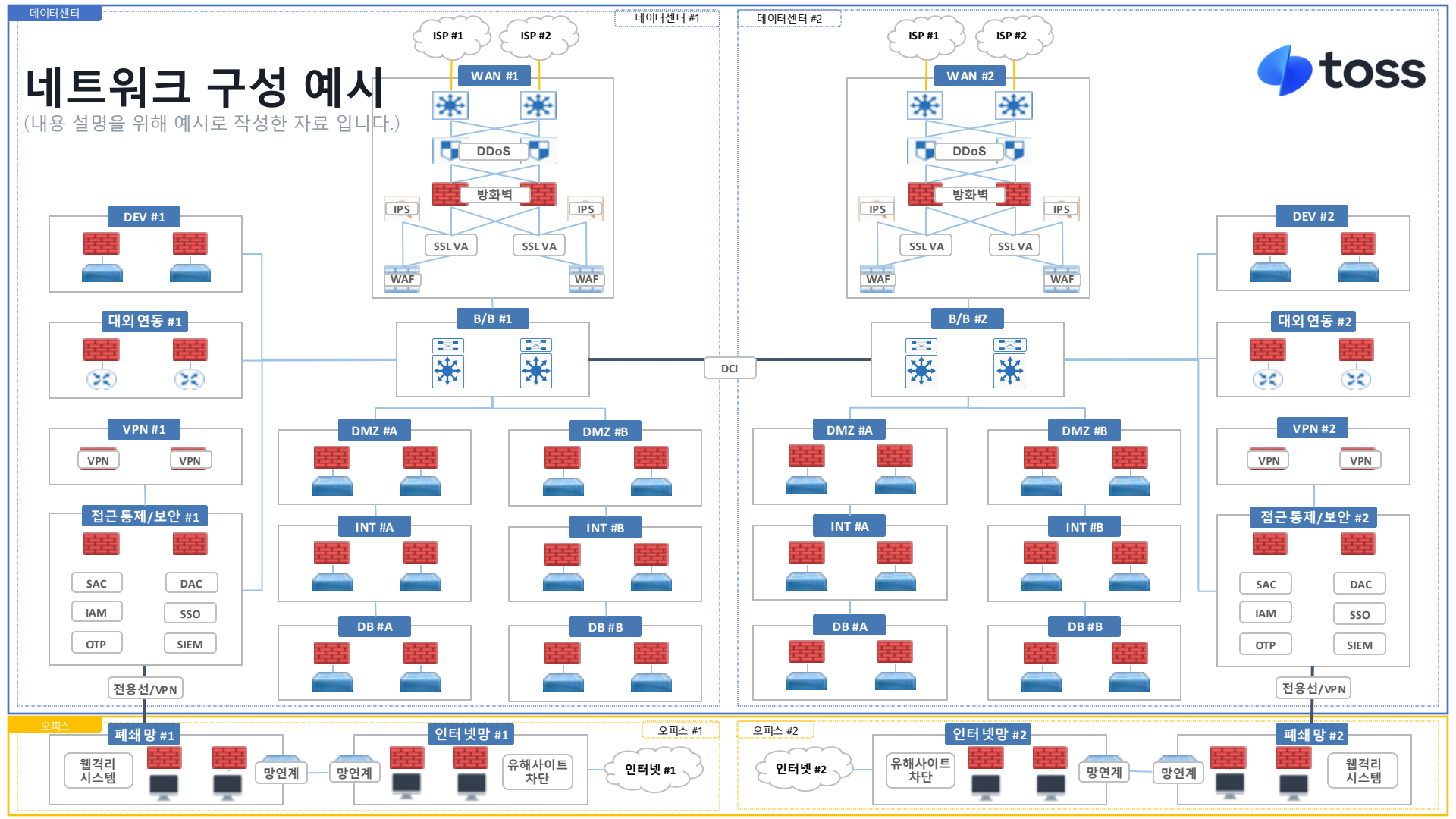
- **SIEM (Security Information and Event Management)**: 로그 통합 분석 및 위협 탐지
- **SOAR (Security Orchestration, Automation and Response)**: 보안 운영 자동화
- **XDR (Extended Detection and Response)**: 다양한 데이터 소스 통합 탐지 및 대응

✅ **추천 솔루션**: Splunk, Microsoft Sentinel, IBM QRadar, Palo Alto Cortex XDR

🛡️ 6. 내부통제 및 컴플라이언스

- **접근 로그 관리 및 감사**: 감사 추적을 위한 필수 요건
- **취약점 진단 및 패치 관리**: 시스템 보안 수준 유지
- **보안 교육 플랫폼**: 직원 보안 인식 제고

✅ **추천 솔루션**: Qualys, Rapid7, KnowBe4


데이터센터
데이터센터 #1
데이터센터 #2
네트워크 구성 예시
(내용 설명을 위해 예시로 작성한 자료 입니다.)
toss
ISP #1
ISP #2
WAN #1
WAN #2
DDoS
방화벽
IPS
SSL VA
WAF
DEV #1
DEV #2
대외연동 #1
대외연동 #2
B/B #1
B/B #2
DCI
VPN #1
VPN #2
VPN
DMZ #A
DMZ #B
INT #A
INT #B
DB #A
DB #B
접근통제/보안 #1
접근통제/보안 #2
SAC
DAC
IAM
SSO
OTP
SIEM
전용선/VPN
오피스
오피스 #1
오피스 #2
폐쇄 망 #1
폐쇄 망 #2
웹격리 시스템
망연계
인터넷망 #1
인터넷망 #2
유해사이트 차단
인터넷 #1
인터넷 #2

법규 준수 관점

관련 법규를 준수하려면 어떤 보안 솔루션이 필요한가?
개인정보보호 안전성 확보조치 기준, 전자금융감독규정, 신용정보업감독규정

개인정보의 안전성 확보조치 기준

계정 및 접근제어
통합계정관리 (IM/IAM)
통합전근관리 (EAM)
사용자 인증
싱글사인온 (SSO)
차세대 인증 (FIDO, DID, IDoT 등)
공개키 기반 구조(PKI)

어플리케이션 및 운영 보안
패치관리시스템 (PMS)

네트워크 및 인프라 보안
방화벽 (UTM, NGFW 등)
침입방지시스템 (IPS)
VPN
SASE (SD_WAN 포함)
SSL 복호화
망분리 (일방향 게이트웨이 포함)
데스크톱 가상화 (VDI, DaaS 등)
네트워크 위협 탐지 및 대응 (NDR)

데이터 보호 및 암호화
DB 보안/암호화
DLP (Data Loss Prevention)
DRM (Digital Rights Management)
보안 USB
인쇄물 보안
키관리시스템 (KMS, HSM)

백업 및 복구
백업/복구 관리 시스템
완전삭제 솔루션

위협 탐지 및 대응
APT 대응
악성코드/랜섬웨어 대응
엔드포인트 위협 탐지 및 대응 (EDR)
확장형 위협 탐지 및 대응 (XDR)
컨텐츠 무해화 (CDR)
메일 보안 솔루션

로그 및 위협 분석
로그 관리/분석 시스템
SIEM (보안 정보 이벤트 관리)
위협 관리 시스템

(※ 법규/인증 요건에서는 구체적으로 보안 솔루션을 언급하지 않습니다. 내용 설명을 위해 대표적인 보안 솔루션을 임의로 분류한 내용입니다.)

법규 준수 관점

관련 법규를 준수하려면 어떤 보안 솔루션이 필요한가?
개인정보보호 안전성 확보조치 기준, 전자금융감독규정, 신용정보업감독규정

신용정보업감독규정

계정 및 접근제어
통합계정관리 (IM/IAM)
통합전근관리 (EAM)
사용자 인증
싱글사인온 (SSO)
차세대 인증 (FIDO, DID, IDoT 등)
공개키 기반 구조(PKI)
서버 접근 통제

어플리케이션 및 운영 보안
패치관리시스템 (PMS)

네트워크 및 인프라 보안
방화벽 (UTM, NGFW 등)
침입방지시스템 (IPS)
Anti DDoS
웹 방화벽
VPN
SSL 복호화

데이터 보호 및 암호화
DB 보안/암호화
DLP (Data Loss Prevention)
DRM (Digital Rights Management)
보안 USB
인쇄물 보안
키관리시스템 (KMS, HSM)

백업 및 복구
백업/복구 관리 시스템
완전삭제 솔루션

위협 탐지 및 대응
APT 대응
악성코드/랜섬웨어 대응
엔드포인트 위협 탐지 및 대응 (EDR)
확장형 위협 탐지 및 대응 (XDR)
컨텐츠 무해화 (CDR)
메일 보안 솔루션

로그 및 위협 분석
로그 관리/분석 시스템
SIEM (보안 정보 이벤트 관리)
위협 관리 시스템

(※ 법규/인증 요건에서는 구체적으로 보안 솔루션을 언급하지 않습니다. 내용 설명을 위해 대표적인 보안 솔루션을 임의로 분류한 내용입니다.)

법규 준수 관점

관련 법규를 준수하려면 어떤 보안 솔루션이 필요한가?
개인정보보호 안전성 확보조치 기준, 전자금융감독규정, 신용정보업감독규정

전자금융감독규정

계정 및 접근제어
통합계정관리 (IM/IAM)
통합전근관리 (EAM)
사용자 인증
싱글사인온 (SSO)
차세대 인증 (FIDO, DID, IDoT 등)
서버 접근 통제

어플리케이션 및 운영 보안
패치관리시스템 (PMS)
어플리케이션 보안 테스트

네트워크 및 인프라 보안
방화벽 (UTM, NGFW 등)
침입방지시스템 (IPS)
Anti DDoS
웹 방화벽
VPN
SASE (SD_WAN 포함)
SSL 복호화
NAC
망분리 (일방향 게이트웨이 포함)
데스크톱 가상화 (VDI, DaaS 등)
무선 네트워크 보안 (WIPS)

데이터 보호 및 암호화
DB 보안/암호화
DLP (Data Loss Prevention)
DRM (Digital Rights Management)
보안 USB
인쇄물 보안
키관리시스템 (KMS, HSM)
개인정보 비식별화 솔루션

백업 및 복구
백업/복구 관리 시스템
완전삭제 솔루션

위협 탐지 및 대응
APT 대응
악성코드/랜섬웨어 대응
엔드포인트 위협 탐지 및 대응 (EDR)
확장형 위협 탐지 및 대응 (XDR)
컨텐츠 무해화 (CDR)
메일 보안 솔루션

로그 및 위협 분석
로그 관리/분석 시스템
SIEM (보안 정보 이벤트 관리)
위협 관리 시스템

(※ 법규/인증 요건에서는 구체적으로 보안 솔루션을 언급하지 않습니다. 내용 설명을 위해 대표적인 보안 솔루션을 임의로 분류한 내용입니다.)

보안 인증 표준 관점

보안 인증을 취득하려면 어떤 보안 솔루션이 필요한가?
ISO 27001/27701, ISMS-P, PCI-DSS

ISO27001/27701

계정 및 접근제어

- 통합계정관리 (IM/IAM)
- 통합전근관리 (EAM)
- 사용자 인증
- 싱글사인온 (SSO)
- 차세대 인증 (FIDO, DID, IDoT 등)
- 서버 접근 통제
- 공개키 기반 구조(PKI)

어플리케이션 및 운영 보안

- 패치관리시스템 (PMS)
- 어플리케이션 보안 테스트

네트워크 및 인프라 보안

- 방화벽 (UTM, NGFW 등)
- VPN
- NAC
- SSL 복호화
- 망분리 (일방향 게이트웨이 포함)

데이터 보호 및 암호화

- DLP (Data Loss Prevention)
- 보안 USB
- 개인정보 비식별화 솔루션

백업 및 복구

- 백업/복구 관리 시스템
- 완전삭제 솔루션

위협 탐지 및 대응

- APT 대응
- 악성코드/랜섬웨어 대응
- 엔드포인트 위협 탐지 및 대응 (EDR)
- 확장형 위협 탐지 및 대응 (XDR)
- 컨텐츠 무해화 (CDR)

로그 및 위협 분석

- 로그 관리/분석 시스템
- SIEM (보안 정보 이벤트 관리)
- 위협 관리 시스템
- 디지털 포렌식 솔루션

(※ 법규/인증 요건에서는 구체적으로 보안 솔루션을 언급하지 않습니다. 내용 설명을 위해 대표적인 보안 솔루션을 임의로 분류한 내용입니다.)

보안 인증 표준 관점

보안 인증을 취득하려면 어떤 보안 솔루션이 필요한가?
ISO 27001/27701, ISMS-P, PCI-DSS

ISMS-P

계정 및 접근제어

- 통합계정관리 (IM/IAM)
- 통합전근관리 (EAM)
- 사용자 인증
- 싱글사인온 (SSO)
- 차세대 인증 (FIDO, DID, IDoT 등)
- 서버 접근 통제
- 공개키 기반 구조(PKI)

어플리케이션 및 운영 보안

- 패치관리시스템 (PMS)
- 어플리케이션 보안 테스트

네트워크 및 인프라 보안

- 방화벽 (UTM, NGFW 등)
- 침입방지시스템 (IPS)
- Anti DDoS
- 웹 방화벽
- VPN
- SASE (SD_WAN 포함)
- SSL 복호화
- NAC
- 망분리 (일방향 게이트웨이 포함)
- 데스크톱 가상화 (VDI, DaaS 등)
- 무선 네트워크 보안 (WIPS)

데이터 보호 및 암호화

- DB 보안/암호화
- DLP (Data Loss Prevention)
- DRM (Digital Rights Management)
- 보안 USB
- 키관리시스템 (KMS, HSM)
- 개인정보 비식별화 솔루션

백업 및 복구

- 백업/복구 관리 시스템
- 완전삭제 솔루션

위협 탐지 및 대응

- APT 대응
- 악성코드/랜섬웨어 대응
- 엔드포인트 위협 탐지 및 대응 (EDR)
- 확장형 위협 탐지 및 대응 (XDR)

로그 및 위협 분석

- 로그 관리/분석 시스템
- SIEM (보안 정보 이벤트 관리)
- 위협 관리 시스템

(※ 법규/인증 요건에서는 구체적으로 보안 솔루션을 언급하지 않습니다. 내용 설명을 위해 대표적인 보안 솔루션을 임의로 분류한 내용입니다.)

보안 인증 표준 관점

보안 인증을 취득하려면 어떤 보안 솔루션이 필요한가?
ISO 27001/27701, ISMS-P, PCI-DSS

PCI-DSS

계정 및 접근제어
통합계정관리 (IM/IAM)
통합전근관리 (EAM)
사용자 인증
싱글사인온 (SSO)
차세대 인증 (FIDO, DID, IDoT 등)
서버 접근 통제
공개키 기반 구조(PKI)

어플리케이션 및 운영 보안
패치관리시스템 (PMS)
어플리케이션 보안 테스트

네트워크 및 인프라 보안
방화벽 (UTM, NGFW 등)
침입방지시스템 (IPS)
Anti DDoS
웹 방화벽
VPN
NAC
무선 네트워크 보안 (WIPS)

데이터 보호 및 암호화
DB 보안/암호화
DLP (Data Loss Prevention)
보안 USB
키관리시스템 (KMS, HSM)

백업 및 복구
백업/복구 관리 시스템
완전삭제 솔루션

위협 탐지 및 대응
APT 대응
악성코드/랜섬웨어 대응
엔드포인트 위협 탐지 및 대응 (EDR)
확장형 위협 탐지 및 대응 (XDR)
컨텐츠 무해화 (CDR)
메일 보안 솔루션

로그 및 위협 분석
로그 관리/분석 시스템
SIEM (보안 정보 이벤트 관리)
위협 관리 시스템

(※ 법규/인증 요건에서는 구체적으로 보안 솔루션을 언급하지 않습니다. 내용 설명을 위해 대표적인 보안 솔루션을 임의로 분류한 내용입니다.)

어떤 보안 솔루션이 필요한가?

의무적으로 도입이 필요한 보안 솔루션은 무엇인가?

관련법규 + 보안인증 (약 40여종)

계정 및 접근제어
통합계정관리 (IM/IAM)
통합전근관리 (EAM)
사용자 인증
싱글사인온 (SSO)
차세대 인증 (FIDO, DID, IDoT 등)
서버 접근 통제
공개키 기반 구조(PKI)

어플리케이션 및 운영 보안
패치관리시스템 (PMS)
어플리케이션 보안 테스트

네트워크 및 인프라 보안
방화벽 (UTM, NGFW 등)
침입방지시스템 (IPS)
Anti DDoS
웹 방화벽
VPN
SASE (SD_WAN 포함)
SSL 복호화
NAC
망분리 (일방향 게이트웨이 포함)
데스크톱 가상화 (VDI, DaaS 등)
무선 네트워크 보안 (WIPS)

데이터 보호 및 암호화
DB 보안/암호화
DLP (Data Loss Prevention)
DRM (Digital Rights Management)
보안 USB
인쇄물 보안
키관리시스템 (KMS, HSM)
개인정보 비식별화 솔루션

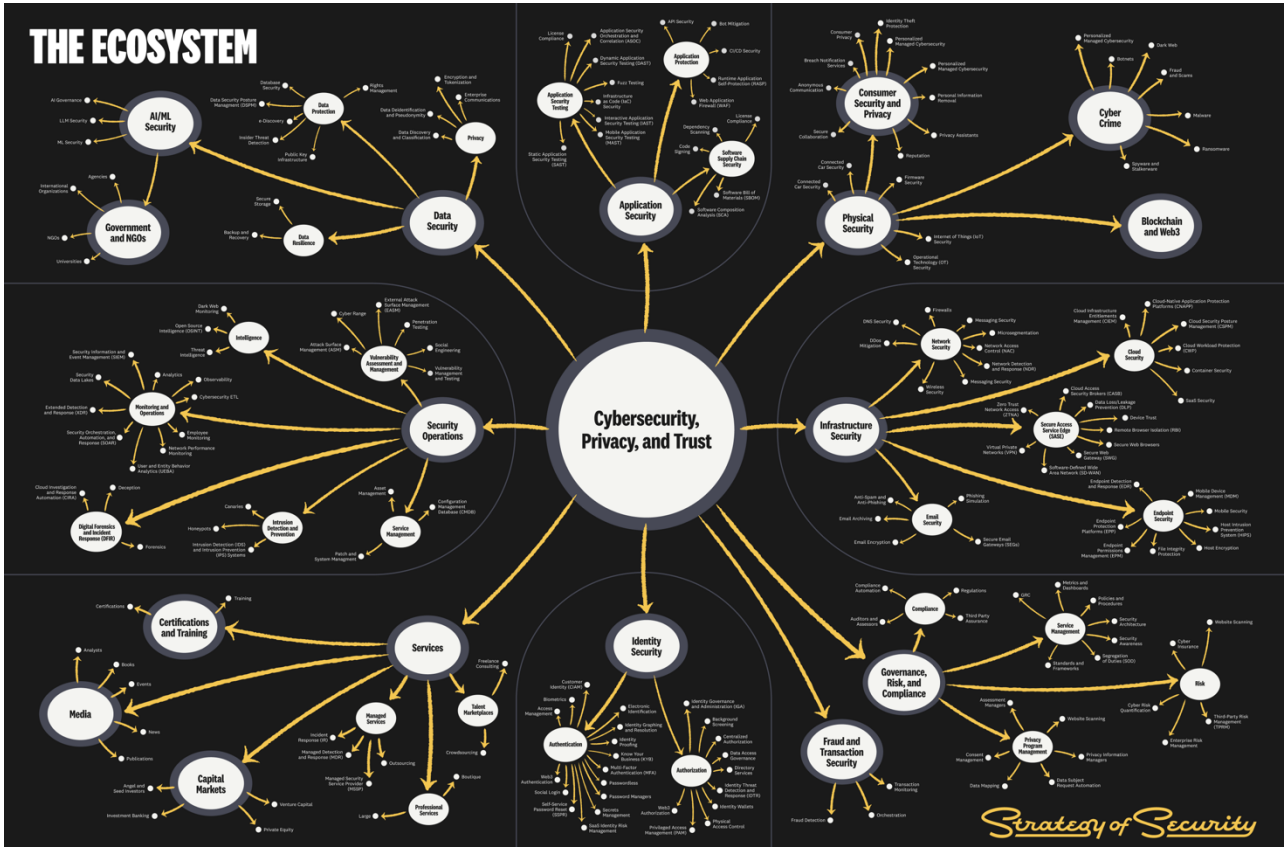
백업 및 복구
백업/복구 관리 시스템
완전삭제 솔루션

위협 탐지 및 대응
APT 대응
악성코드/랜섬웨어 대응
엔드포인트 위협 탐지 및 대응 (EDR)
확장형 위협 탐지 및 대응 (XDR)
컨텐츠 무해화 (CDR)
메일 보안 솔루션

로그 및 위협 분석
로그 관리/분석 시스템
SIEM (보안 정보 이벤트 관리)
위협 관리 시스템

(※ 법규/인증 요건에서는 구체적으로 보안 솔루션을 언급하지 않습니다. 내용 설명을 위해 대표적인 보안 솔루션을 임의로 분류한 내용입니다.)

어떤 보안 솔루션이 필요한가?



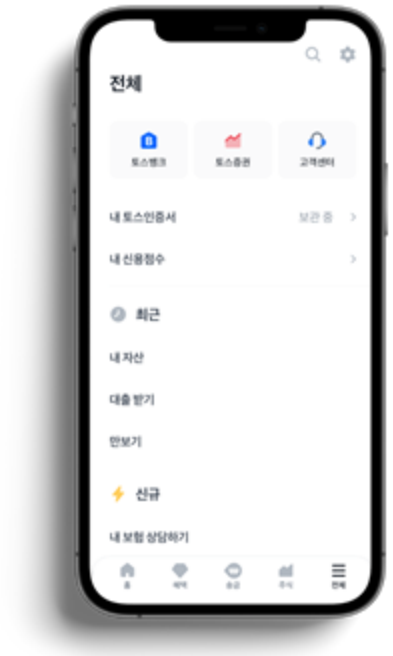
(출처 : https://strategyofsecurity.com/ecosystem)

토스의
주요 보안 솔루션

토스의 보안조직은 고객의 자산과 데이터, 서비스 환경을 보호하여 안전하게 토스를 이용할 수 있도록 하며,
임직원이 혁신적인 서비스를 개발하고 운영하는 업무에 몰입 할 수 있도록 업무환경을 보호합니다.

서비스 이용 고객
보안 솔루션

모바일 앱 보안 위협



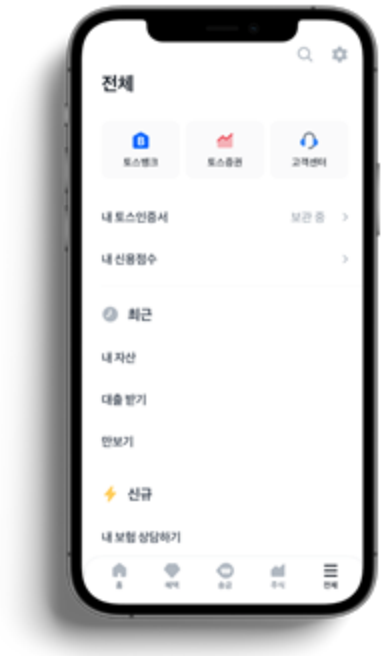
1. 앱 위/변조

- 앱 위/변조를 통한 가짜 앱
- 악성코드가 포함 된 가짜 앱 설치 유도
  - 앱 설치 ➔ 개인정보입력 ➔ 정보탈취
  - 송금 시 해커의 계좌로 금액을 송금
  - 이용자가 가지고 있는 자산, 개인정보 탈취

2. 소스코드 분석 및 데이터 조작

- 서비스 이용자의 어뷰징
- 소스 분석 후 임의의 패킷을 전송하여 금전적 이득을 취함
- 리워드 서비스등 다양한 영역에 어뷰징 시도

모바일 보안 솔루션



1. 앱 난독화

- 앱 디컴파일 대응
- 디컴파일 시 소스코드 분석을 어렵게 함

2. 토스가드 (자체 보안 모듈)

- 앱 분석 등 악성 행위 탐지
- 앱 위변조 탐지, 운영체제 무결성 체크 등

3. 동적 위/변조 방지 모듈

- API replay attack 방어
- 내부용 API 호출 방어
- App Signature 위/변조 검사

4. ADS (Abusing Detection System)

- 악성 행위 시나리오에 따라
  사용자 디바이스/계정 탐지 및 차단
  API Path 차단, IP차단

모바일 사용자 보안 위협 – 보이스 피싱

Voice Phishing

보이스 피싱 유래

1997년 대만에서 시작, 2000대 초반 대만에서 급격히 발생이 증가하자
범정부 차원에서 강력한 대응책 시행, 단속을 피해 중국대륙으로 본거지 이동

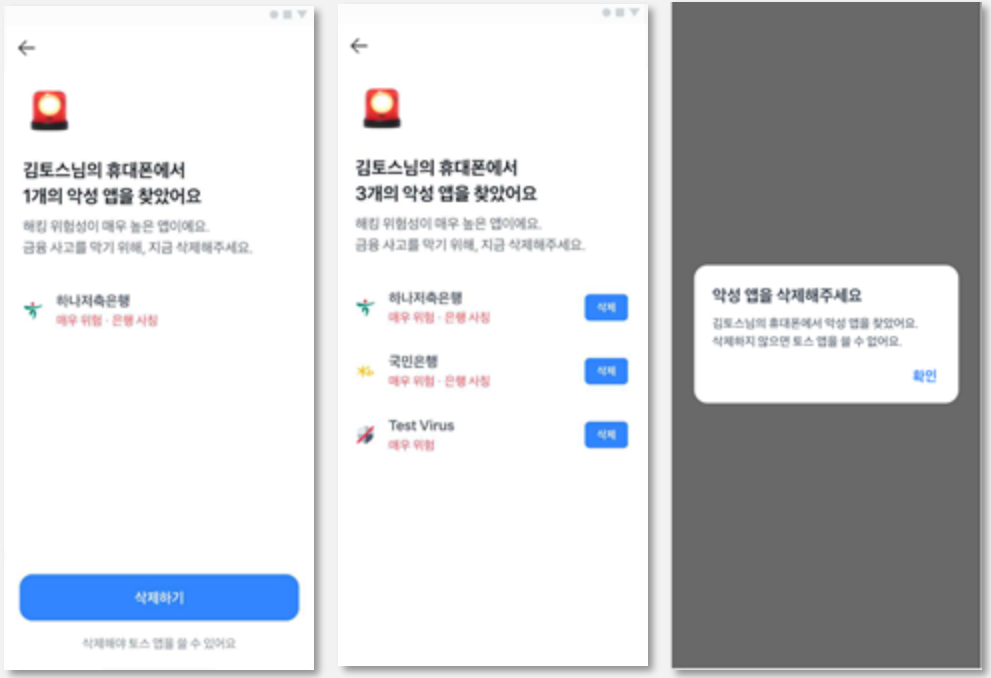
국내 최초 보이스 피싱 사건

‘2006년 5월 18일 국세청 직원 사칭 환급금 사기 사건’

‘모바일 기기에 악성 앱 설치를 유도하고
개인정보의 취득/탈취 및 휴대폰 단말기에 대한 제어권한 획득’
하는 방식은 대표적인 보이스 피싱 수법 중 하나

모바일 보안 솔루션 – '피싱제로'

악성앱 탐지 ('피싱제로') 기능



Security Tech Alert APP 11:02 AM

토스앱 2025:02:28 24시간 탐지 통계

- 추가된 악성앱 : **46**
- 탐지된 악성앱 : **622**
  - LOW : **2**
  - SUSPICIOUS : **366**
  - CRITICAL : **254**
- 악성앱 탐지 유저수 : **119**
- 가장 많이 탐지된 악성앱 순위
  - [**com.yc.openskipapp**] - 10번
  - [**com.fakevi.tisland**] - 6번
  - [**zvhp3.cyo88.km4dx**] - 5번

모바일 보안 솔루션 – '피싱제로'

피싱제로 운영 현황

추가 악성앱

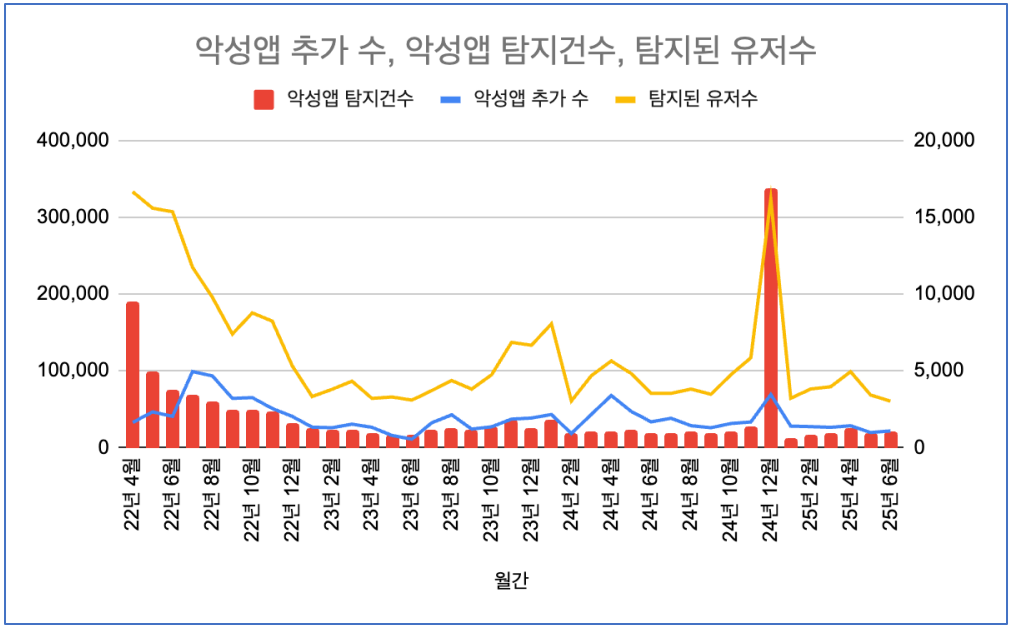
7만4천+

탐지 건수

165만+

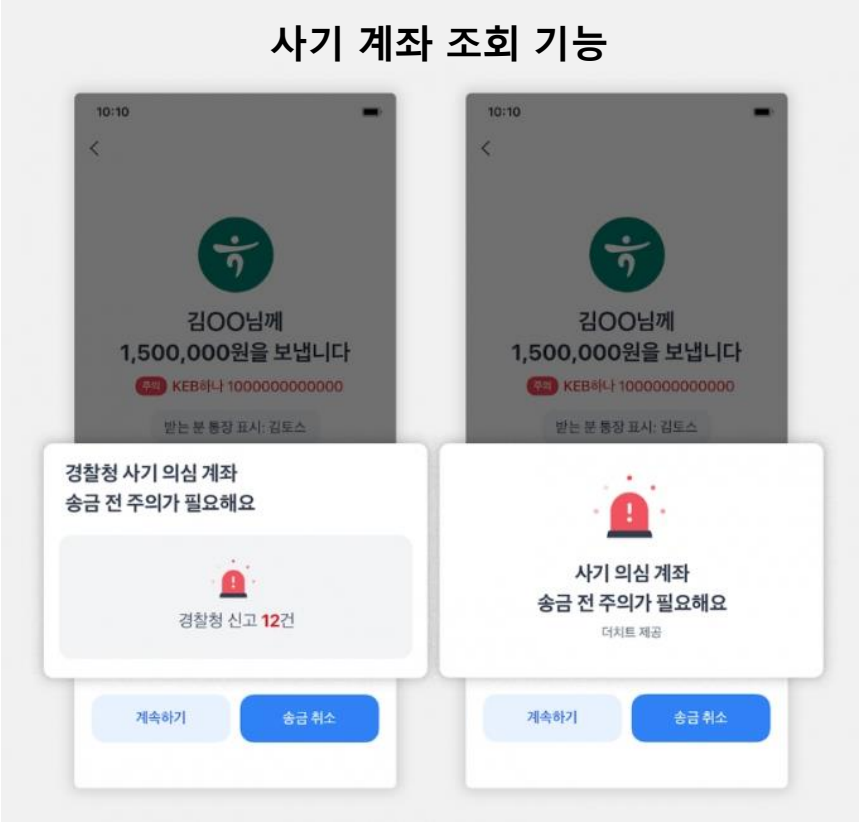
탐지 사용자

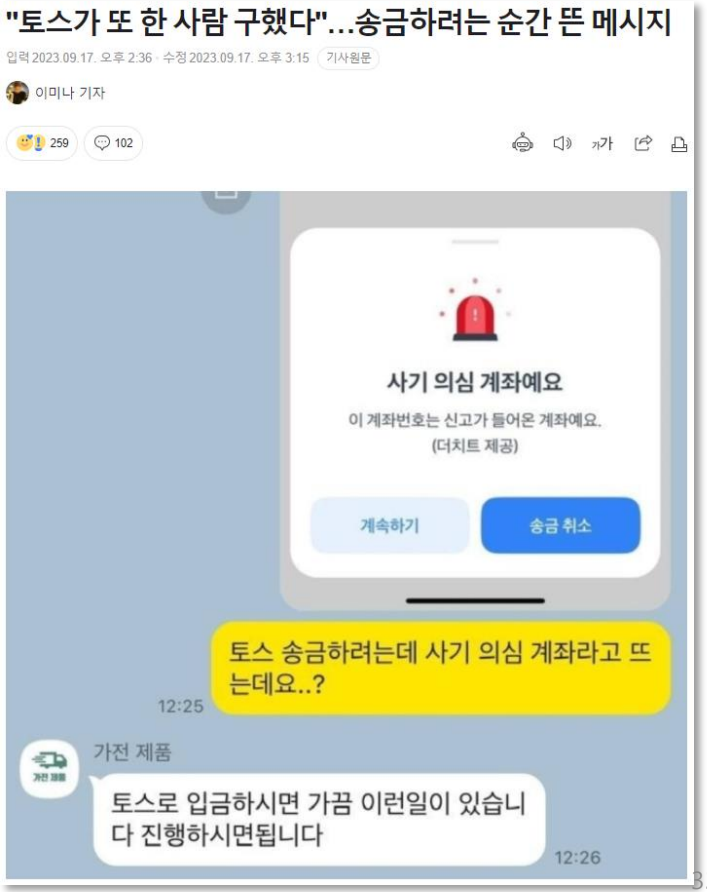
23만+



** 다른 금융권 앱에 무료로 피싱제로 기능 제공 중

모바일 보안 솔루션 – ‘사기 계좌 조회’





서비스 사칭 대응 솔루션

toss

Case1) 토스 로고 / 서비스명 사칭 도박 사이트

1. 사칭 사이트 탐지

- Text : 회사 / 서비스명
- Image : 회사 / 서비스 로고
- Domain : 회사 / 서비스명 유사 도메인

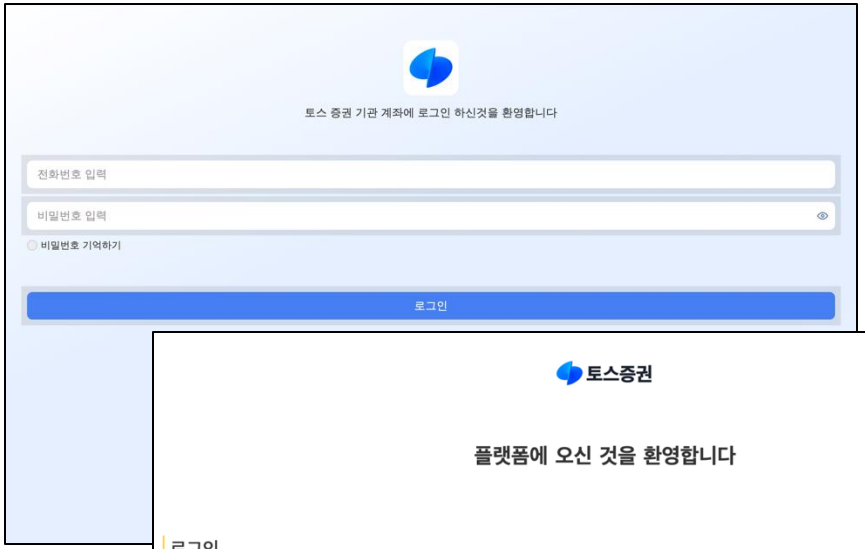
2. 사칭 사이트 대응

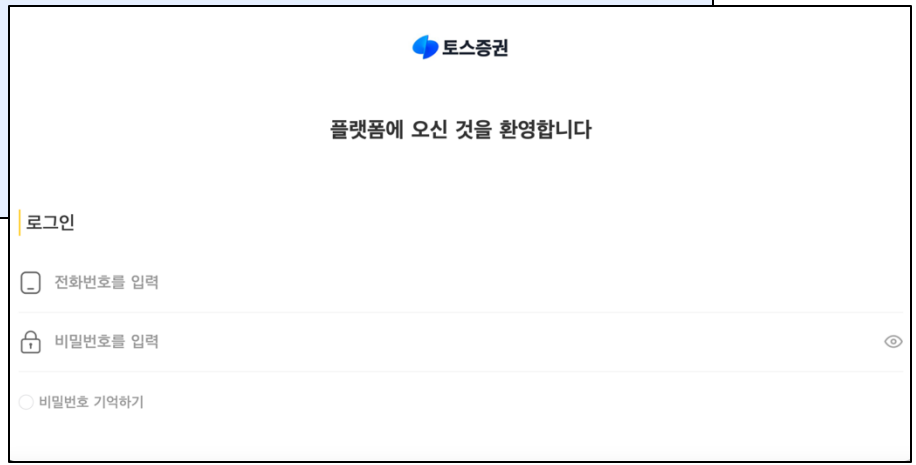
- Google delisting request
- Soft Notice to Registrant
- Report Abuse to Registrar
- Report Abuse to ICANN
- Report Abuse to Hosting Provider
- Report Abuse to Registry
- Report Abuse to Payment Service
- Report Abuse to KISA
- UDRP (Uniform Domain-Name Dispute-Resolution Poilcy)

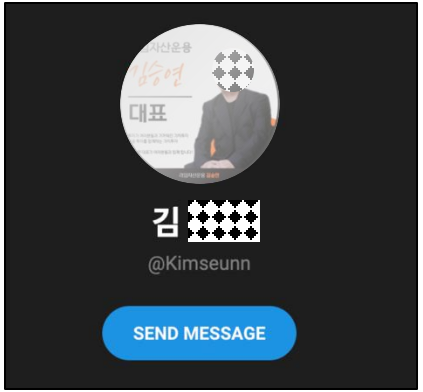
MARQVISION

서비스 사칭 대응 솔루션

Case2) 토스증권 사칭 사이트 / SNS / 메신저

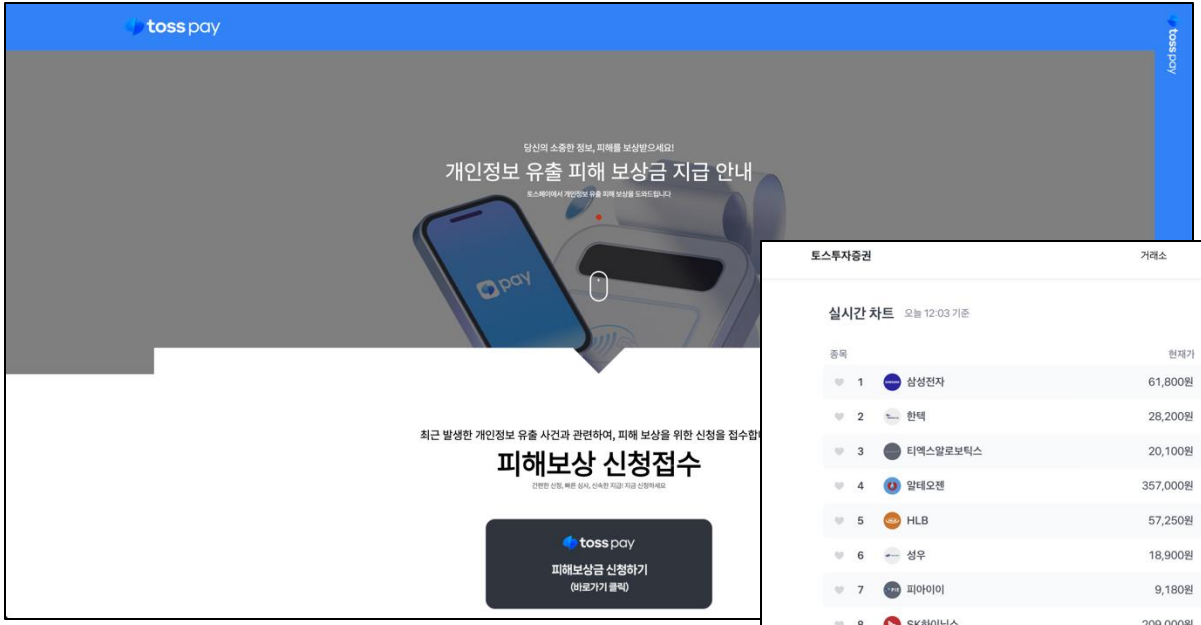


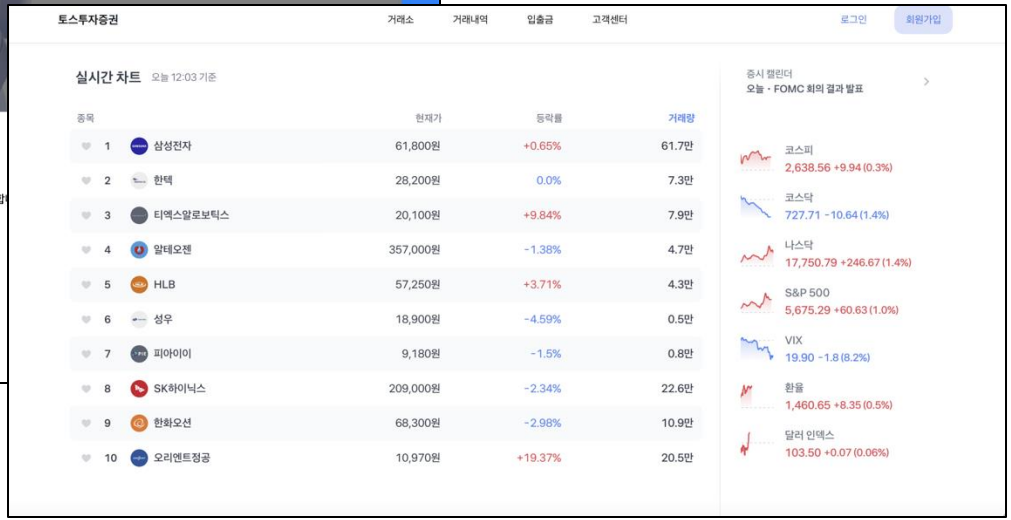




서비스 사칭 대응 솔루션

Case3) 정교한 사칭 사이트

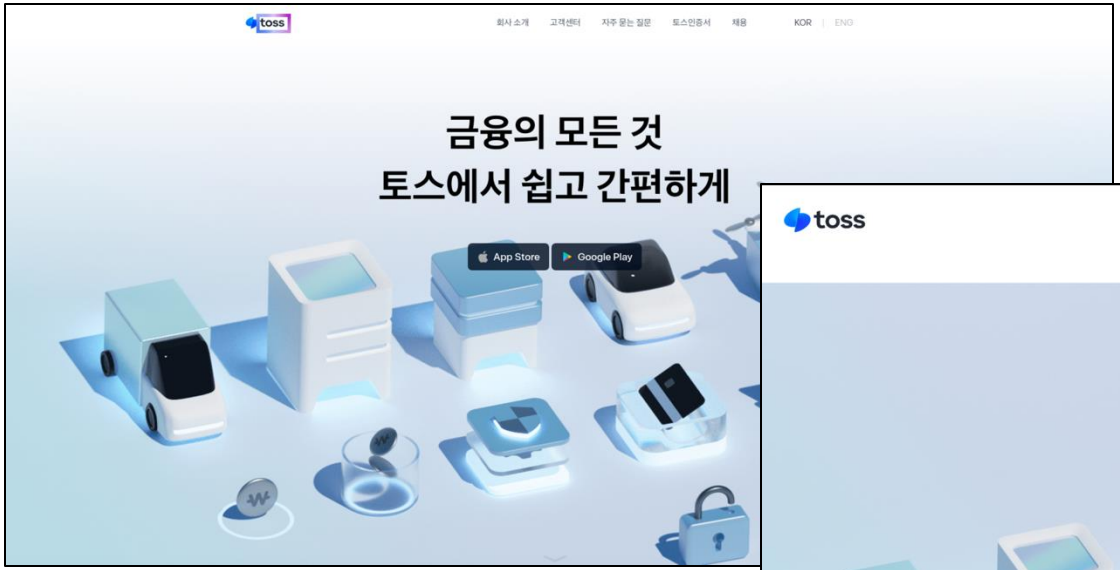




서비스 사칭 대응 솔루션

toss

Case4) 홈페이지 복제



출입 통제
보안 솔루션

토스 Face Pass

얼굴 인증을 통해 토스 임직원만 출입 가능

- 위변조 방지 (Liveness) 적용
- 얼굴 데이터 암호화, 악의적 행위 모니터링 (CCTV, FDS 운영)

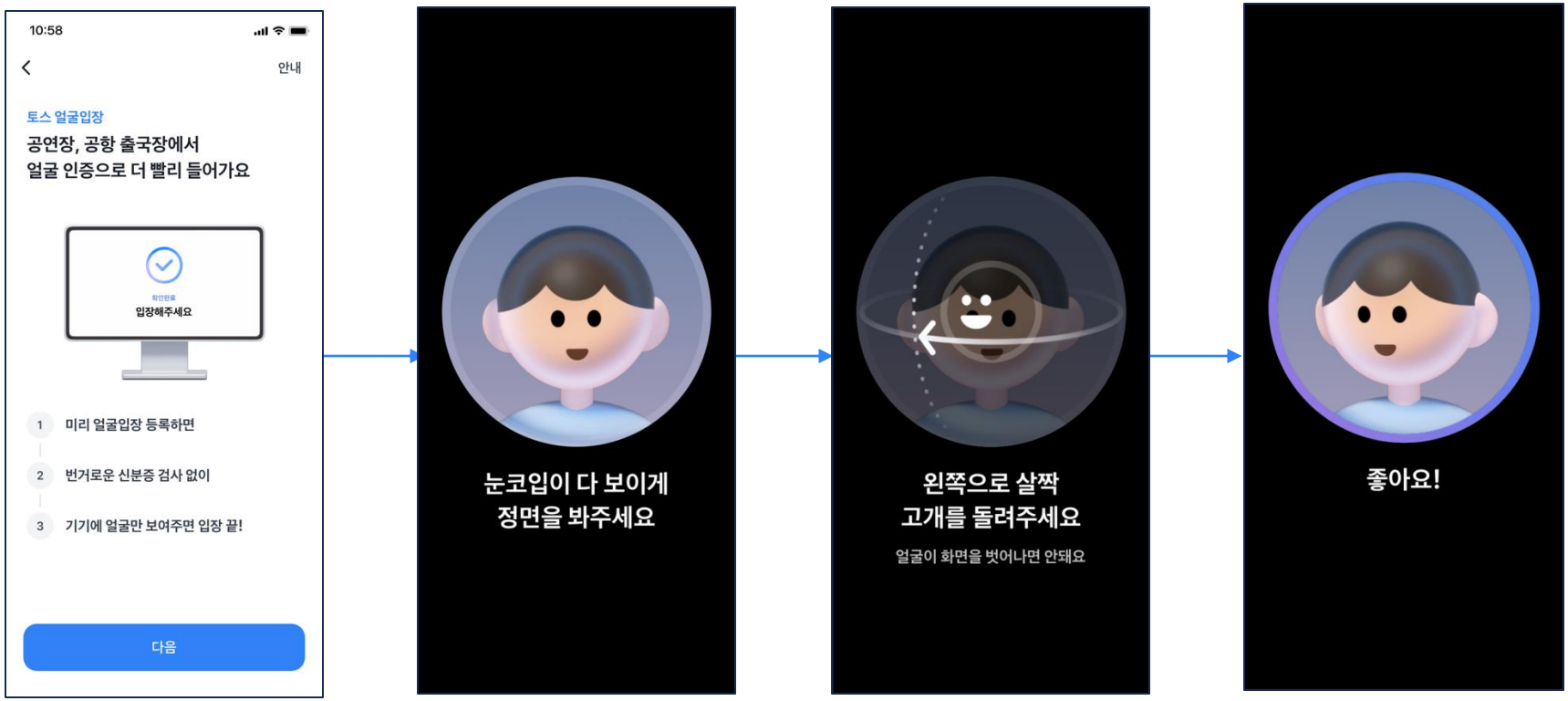
얼굴 인식&인증

인증 성공

인증 실패

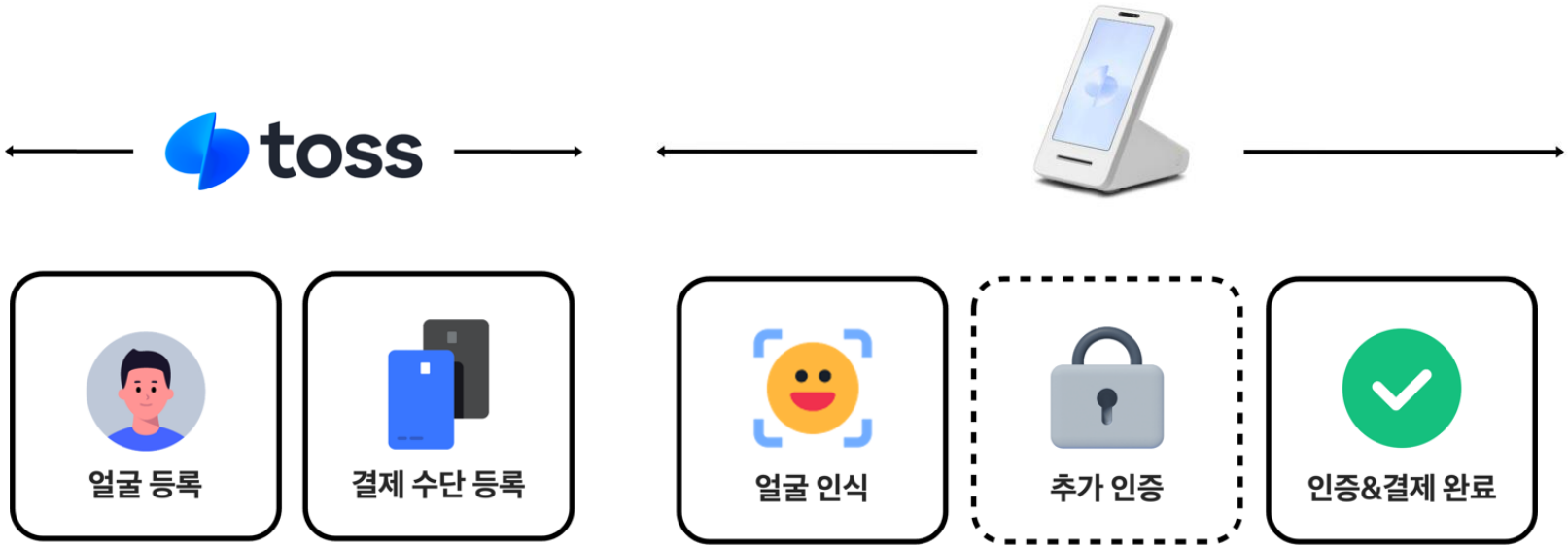
토스 Face Pass

얼굴 정보 등록 절차



토스 Face Pay

서비스 활용 사례 (Face Pay)



[토스 앱에서 얼굴등록]

[매장에 설치된 토스 단말기에서 인증 & 결제]

토스 Face Pay

서비스 활용 사례 (Face Pay)

CU

GS25

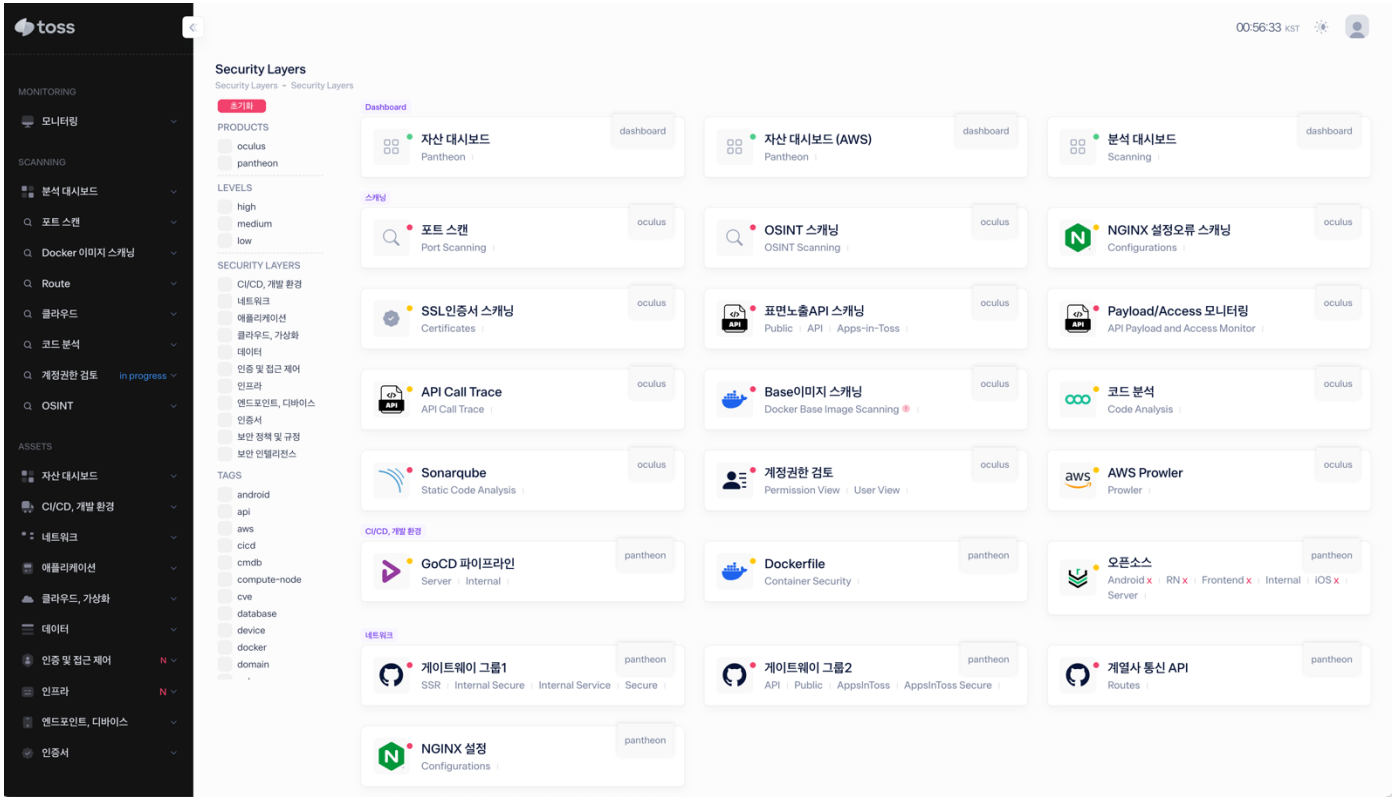
세븐일레븐

(출처 : 각 사 보도자료)

자산관리
보안 솔루션

자산관리 보안 솔루션

보호대상 자산을 수집 / 관리



자산관리 보안 솔루션

보호대상 자산을 수집 / 관리

toss

Pantheon

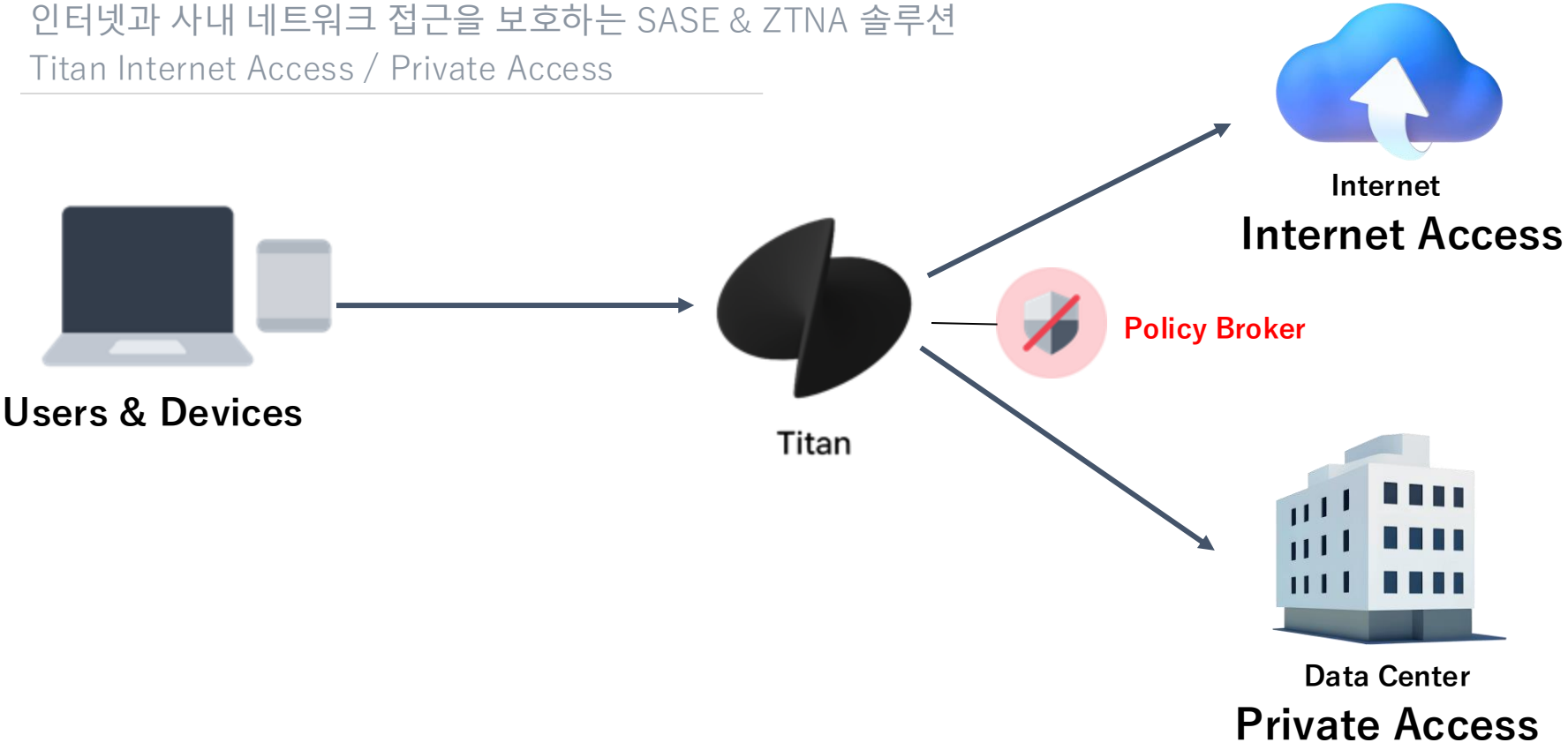
- CI/CD, 개발 환경
- 데이터
- 엔드포인트, 디바이스
- 네트워크
- 인증 및 접근 제어
- 인증서
- 애플리케이션
- 인프라
- 앱 서비스
- 클라우드, 가상화

업무 네트워크
보안 솔루션

업무 네트워크 보안 솔루션 – Titan

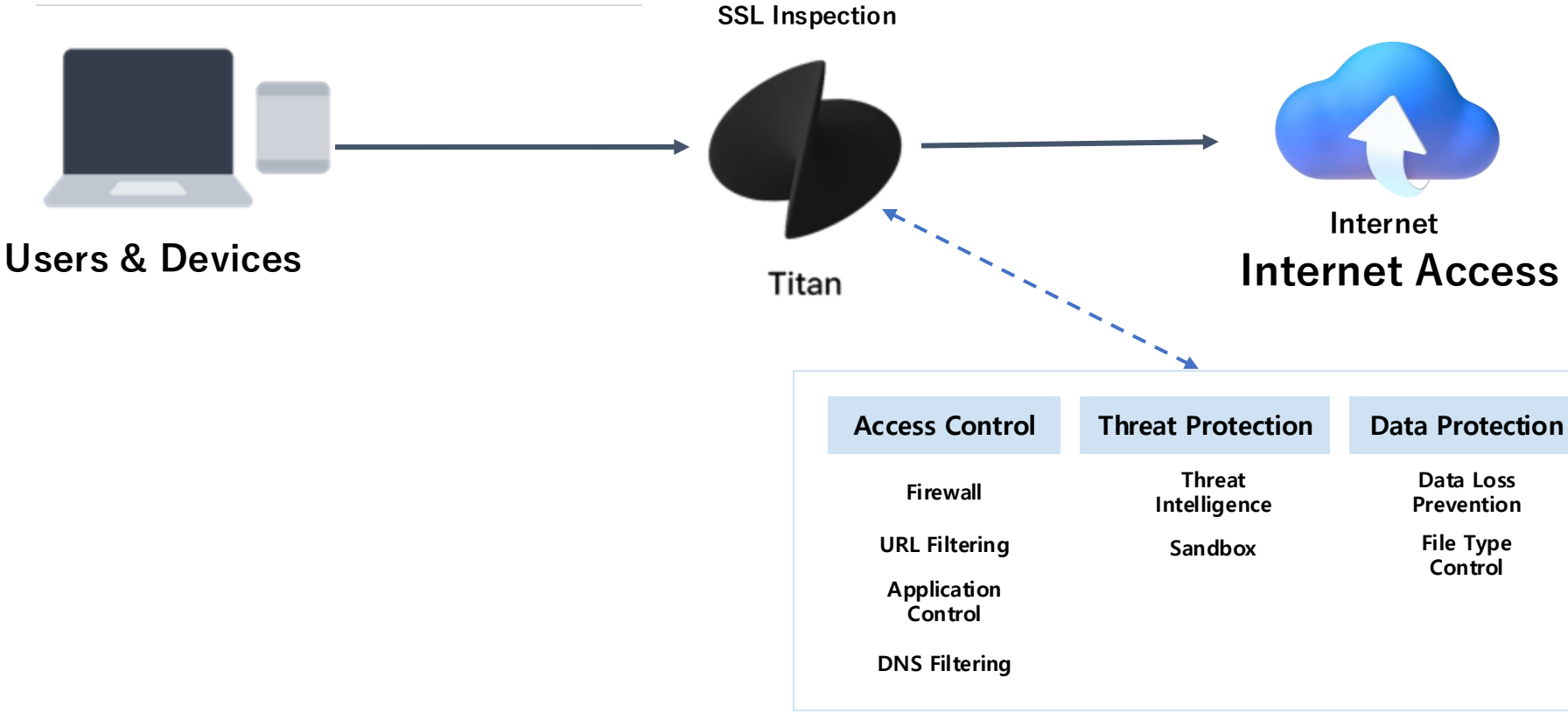
인터넷과 사내 네트워크 접근을 보호하는 SASE & ZTNA 솔루션

Titan Internet Access / Private Access



업무 네트워크 보안 솔루션 – Titan

Titan Internet Access



업무 네트워크 보안 솔루션 – Titan

Titan Private Access

Users & Devices

Titan

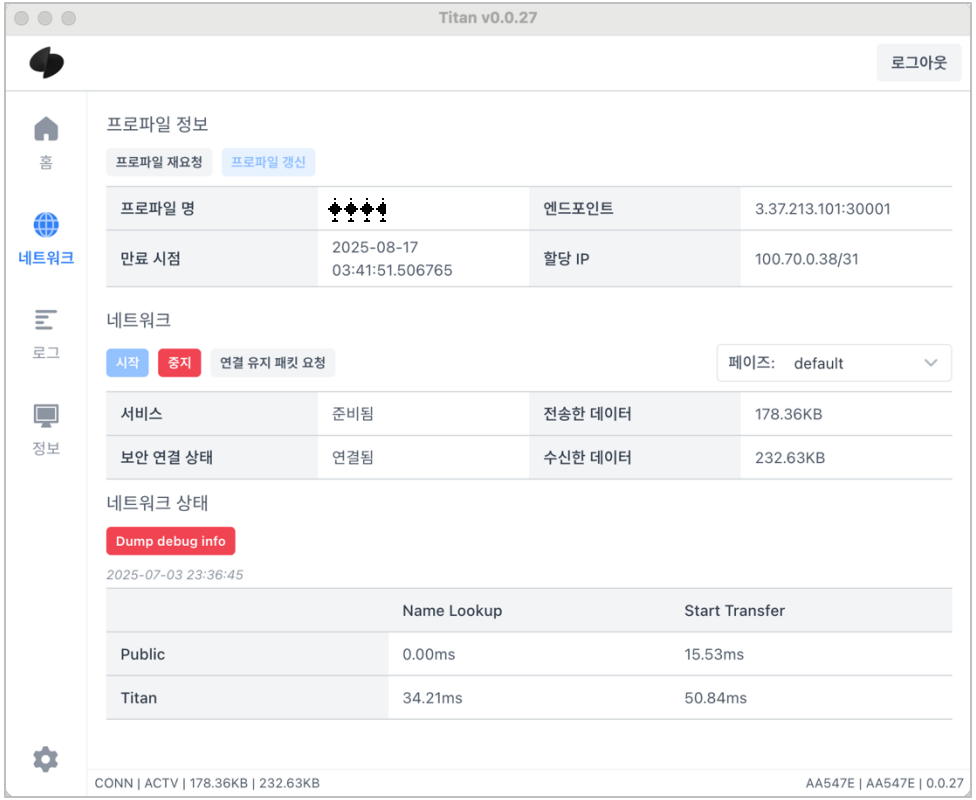
Data Center

Private Access

Access Control	Device Posture	Etc.
Firewall	OS	Multi Profile
	Application Process	
	File Path	
	IP Address	

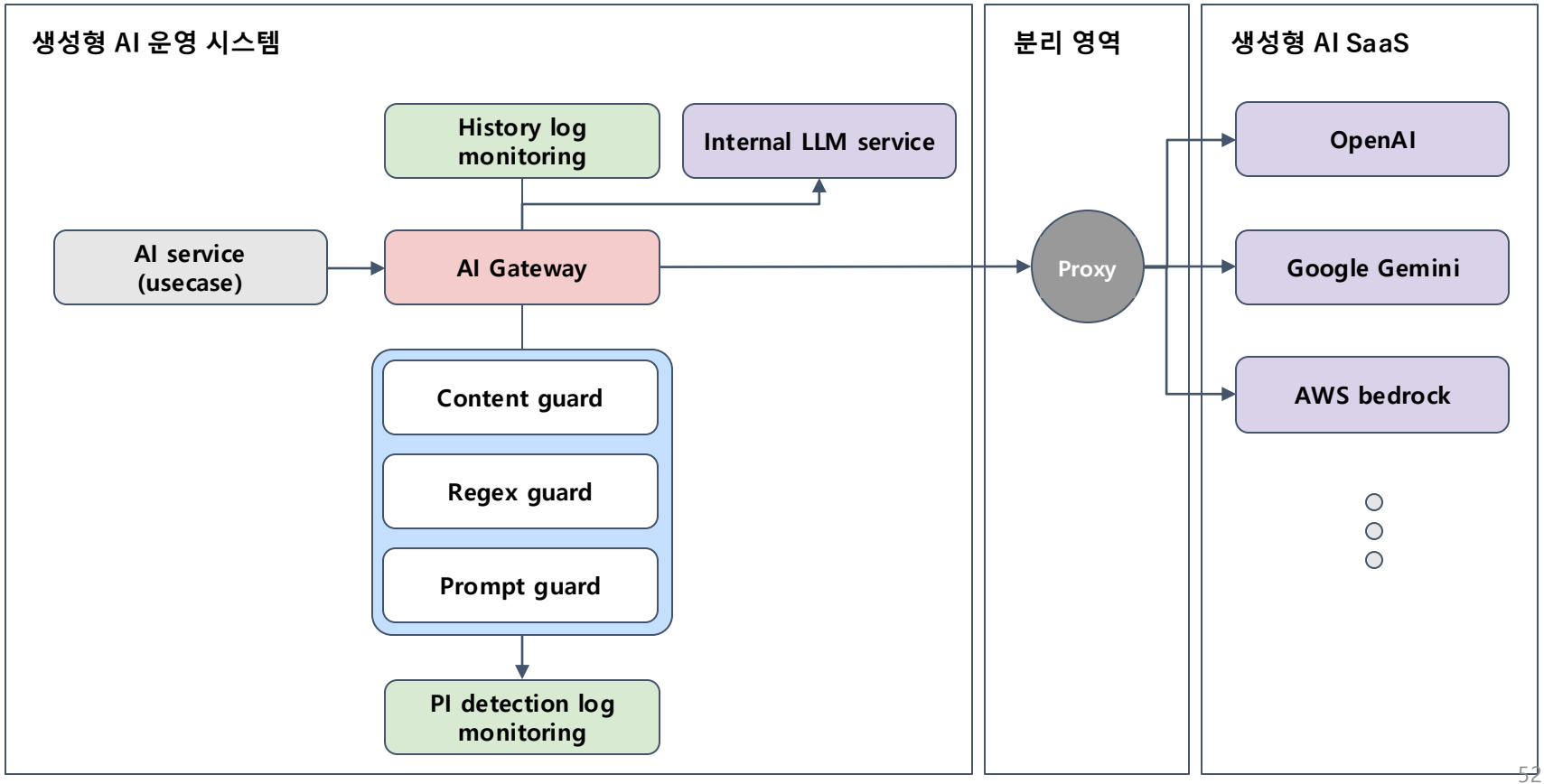
업무 네트워크 보안 솔루션 – Titan

Titan Agent



생성형 AI
보안 솔루션

생성형 AI 보안 솔루션


생성형 AI 운영 시스템
분리 영역
생성형 AI SaaS
History log monitoring
Internal LLM service
AI service (usecase)
AI Gateway
Proxy
OpenAI
Google Gemini
AWS bedrock
Content guard
Regex guard
Prompt guard
PI detection log monitoring

어떤 보안 솔루션이 필요한가?

어떤 보안 솔루션이 필요한가?

- 규제 요건, 인증 요건 분석
  - 기업이 속한 산업군, 사업 영역, 처리 정보 유형에 따라 준수해야 하는 요건 파악
- 조직의 IT 인프라 및 운영환경 파악
  - 온프레미스/클라우드, 원격근무 여부, 업무용 단말 종류 등 고려
- 보호대상 자산 및 데이터 파악
  - 보호대상 자산 및 데이터에 따라 보안 수준, 보안 수단 결정
- 위협 시나리오 기반 위험도 평가
  - 위협 시나리오 기반 위험도 평가 결과에 따라 보안 수준, 우선순위 결정
- 보안 성숙도, 운영 역량 고려
  - 운영이 간단한 보안 솔루션, 전문 인력이 필요한 보안 솔루션, 자체 개발 보안 솔루션

조직에 맞는 보안 솔루션을 갖춰야

보안 위협에 맞설 수 있습니다

감사합니다