More security,
More freedom

AhnLab Transaction Security Center

모바일 금융 보안 통합 매니지먼트 솔루션

표준제안서

AhnLab

목차

AhnLab
Transaction Security Center

AhnLab

01 배경

1. 금융 보안 위협의 다변화 & 고도화
2. 끊이지 않는 보이스피싱
3. 보이스피싱 대응의 현실과 도전과제

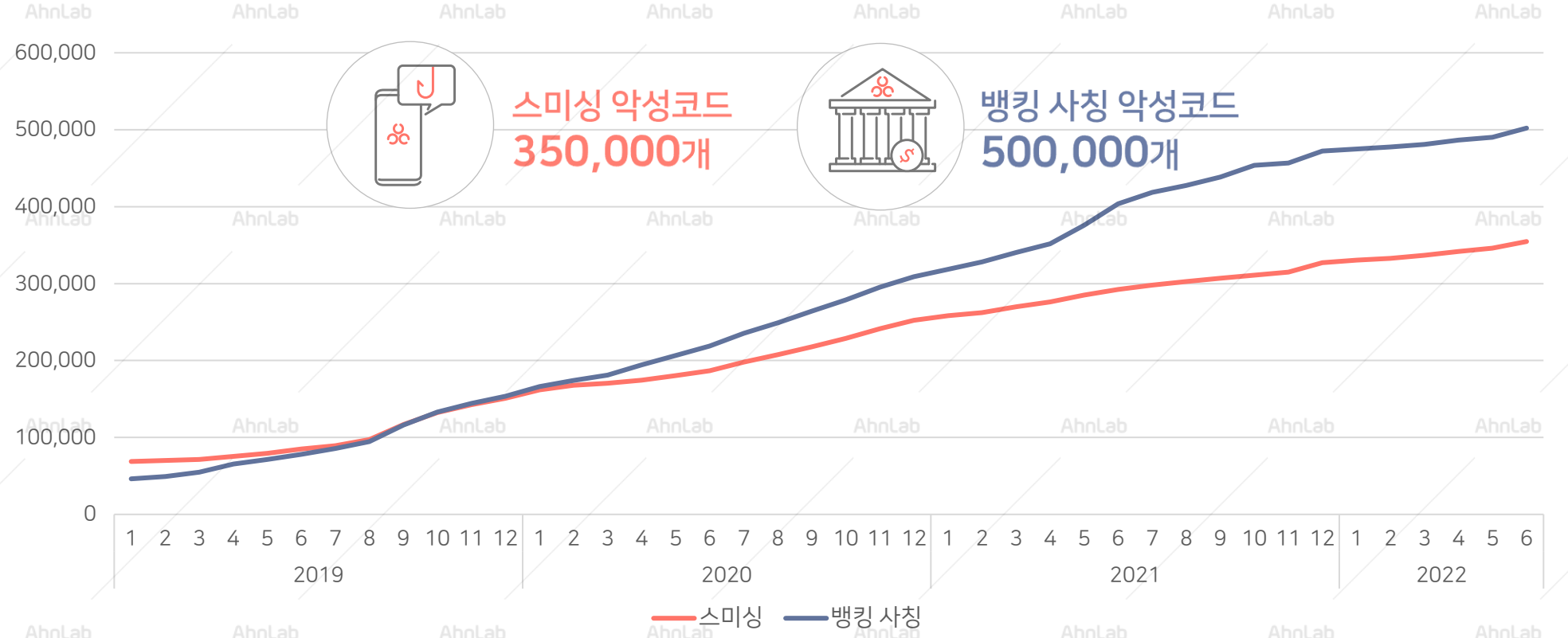
금융 보안 위협의 다변화 & 고도화

모바일 금융 거래 환경을 직접적으로 위협하는 악성코드가 증가하고 있습니다.

- 예시) 문자 메시지를 통해 악성 앱을 설치하는 스미싱 공격, 금융 서비스와 유사하게 제작된 뱅킹 사칭 앱 등

2022년 상반기 누적

스미싱 및 뱅킹 사칭 악성코드 누적 추이

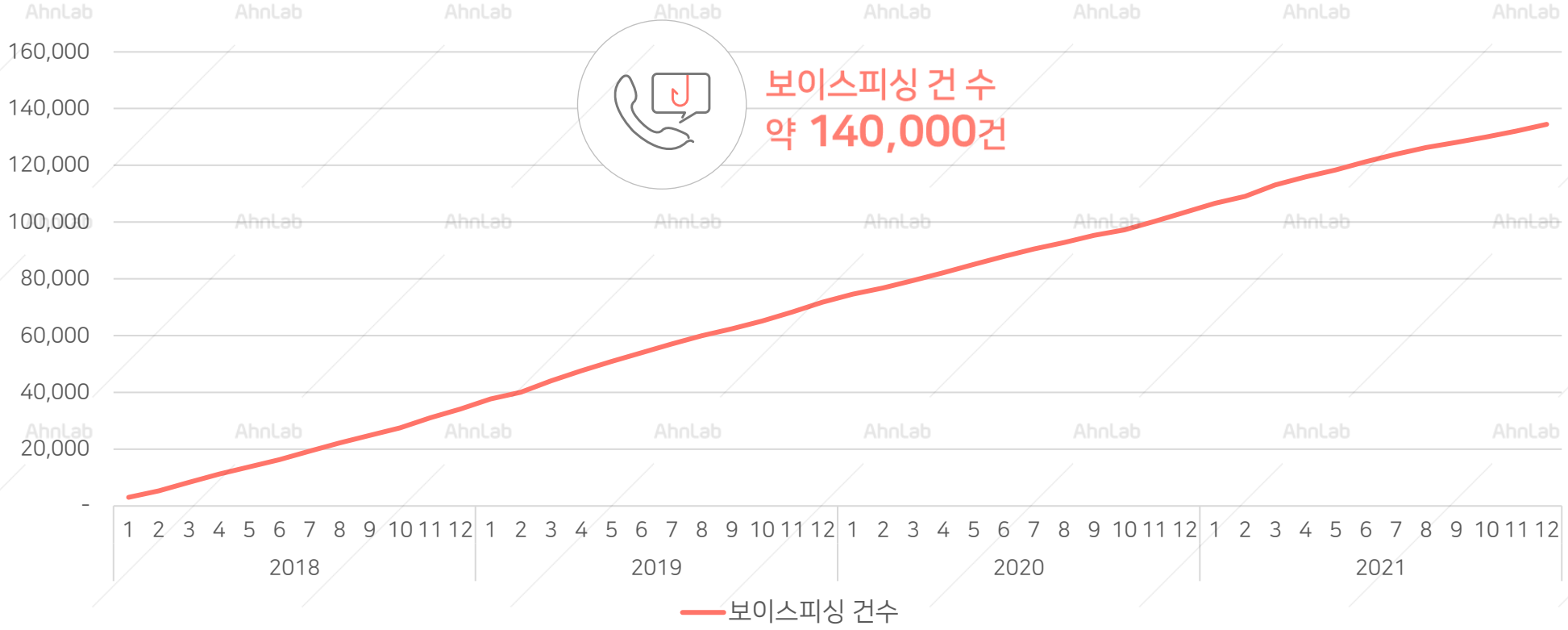


끊이지 않는 보이스피싱

모바일 금융 서비스가 확대됨에 따라 **보이스피싱도 지속적으로 증가하고, 그 피해액도 늘어나고 있습니다.**

금융 서비스 이용자 보호를 위한 **실질적인 대책 필요**

최근 4개년 보이스피싱 월별 누적 추이



보이스피싱 대응의 현실과 도전과제

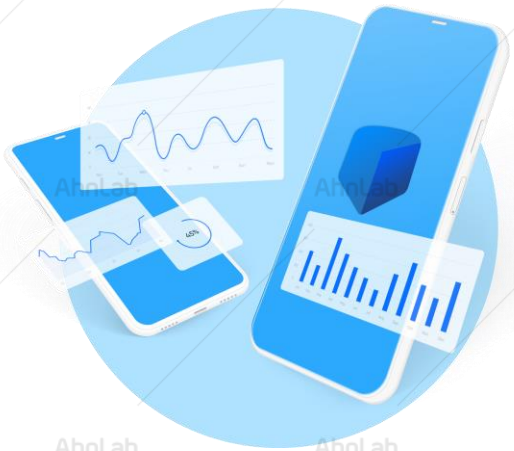
악성코드와 위협 앱을 정확하게 탐지하는 것도 중요합니다. 다만, **탐지 결과를 서비스의 보안과 운영에 실질적으로 활용할 수 있어야 합니다.**

- 수많은 탐지 결과를 중요 정보 위주로 한 눈에 확인해 손쉽게 대응하고, 업무 효율성을 제고할 수 있는 방안 필요

금융 서비스 이용 시
보안 솔루션 실행

보안 솔루션
검사 및 탐지

금융 서비스 내
탐지 결과 알림



탐지 관점

- 탐지 정보를 금융 서비스에서 알리고 있지만, 이를 보안 담당자가 상세하게 확인할 수 있는가?
- 통계 정보 기반의 그래프, 보고서를 제공해 서비스 보안 및 운영 업무에 효율성을 더하는가?

대응 관점

- 서비스 보안 및 운영 정책 변경에 따라 즉시 탐지 카테고리를 활성화/비활성화 할 수 있는가?
- 서비스 이용 제한 조치가 발동되지 않도록 특정 앱을 예외 처리 할 수 있는가?

관리 관점

- 탐지 카테고리 활성화/비활성화 및 예외 처리 조치를 제한된 인원만 설정할 수 있는가?
- 탐지 결과에 따른 보안 정책을 금융 서비스 별로 개별 적용할 수 있는가?

AhnLab
Transaction Security Center

02
솔루션 소개

1. 가치
2. 개요
3. 특장점
4. 기능 구성
5. 주요 화면

AhnLab

가치

고객사에 운영 중인 서비스의 보안 관리 효율성을 확보하고
위협 정보를 한 눈에 파악해 손쉽게 대응 가능합니다

AhnLab Transaction Security Center

운영 효율성

- 연동 서비스 개별 관리 가능
- 관리자 레벨에 따른 운영 권한 부여
- 보고서를 통한 운영 및 보안 업무 지원

쉽고 간편한 대응

- 위협 앱 카테고리 별 탐지 ON/OFF
- 탐지 앱 예외 처리

한 눈에 보는 통계 정보

- 위협 앱 탐지 현황
- 악성코드 탐지 현황
- 위협 앱 탐지 추이
- 예외 처리 등록 현황

개요

AhnLab Transaction Security Center는 **모바일 보안을 한 번에 쉽게 관리할 수 있는 통합 매니지먼트 솔루션**입니다.

솔루션 제공 방식

- 웹서비스 형태로 제공 (非 구축형)

지원 브라우저

- Chrome
- MS Edge

연동 솔루션

- AhnLab V3 Mobile Plus
- AhnLab Mobile Engine SDK
- AhnLab Mobile Engine Suite
- AhnLab Mobile 단말 위협 정보

주요 기능

- 현황 대시보드
- 탐지 내역
- 통계 정보
- 정책 설정 (탐지 정책, 예외 처리)
- 보고서
- 다양한 설정 (세션 타임아웃, 중복 로그인, 관리자 설정 등)

특장점 – 웹 기반 매니지먼트

AhnLab Transaction Security Center **웹 기반 매니지먼트를 제공하여, 서버 구축을 위한 비용과 투자가 필요하지 않습니다.**

- 언제 어디서든 웹 브라우저로 접속해 이용 가능

매니지먼트 도입 및 이용을 위해 별도 투자 불필요
Chrome과 MS Edge 브라우저 지원

주요 추이 모니터링 및
위협 앱 탐지 현황 확인

다양한 기간 별
통계와 보고서 발행

탐지 정책 설정 및
예외 처리 등록/해제

관리자 등록 및
등록 서비스 관리

관리 편의성 | **접근 용이** | **비용 절감**

특장점 – 유연한 개별 운영

조직 구조와 다양한 서비스 운영 주체를 고려한 개별 관리를 지원하며,

조직 내 역할에 따라 ▲최상위 정책 관리자 ▲정책 관리자 ▲모니터링 관리자로 서비스 이용 및 접근 권한을 설정할 수 있습니다.

최상위 정책 관리자

모든 서비스를 대상으로

- 관련 정보 확인
- 정책 설정 및 관리자 권한 설정

정책 관리자

허용된 서비스에 한해

- 관련 정보 확인
- 정책 설정 및 하위 관리자 권한 설정

모니터링 관리자

허용된 서비스에 한해

- 관련 정보 확인

특장점 – 안랩 모바일 솔루션 연동

안랩 ▲V3 Mobile Plus ▲Mobile Engine SDK ▲Mobile 단말 위협 정보를 연동합니다.

- 각 제품에서 탐지한 결과를 확인하고, 제품의 위협 앱 탐지 정책을 설정하며 탐지 예외 처리 등록 및 해제 가능.

V3 Mobile Plus 연동

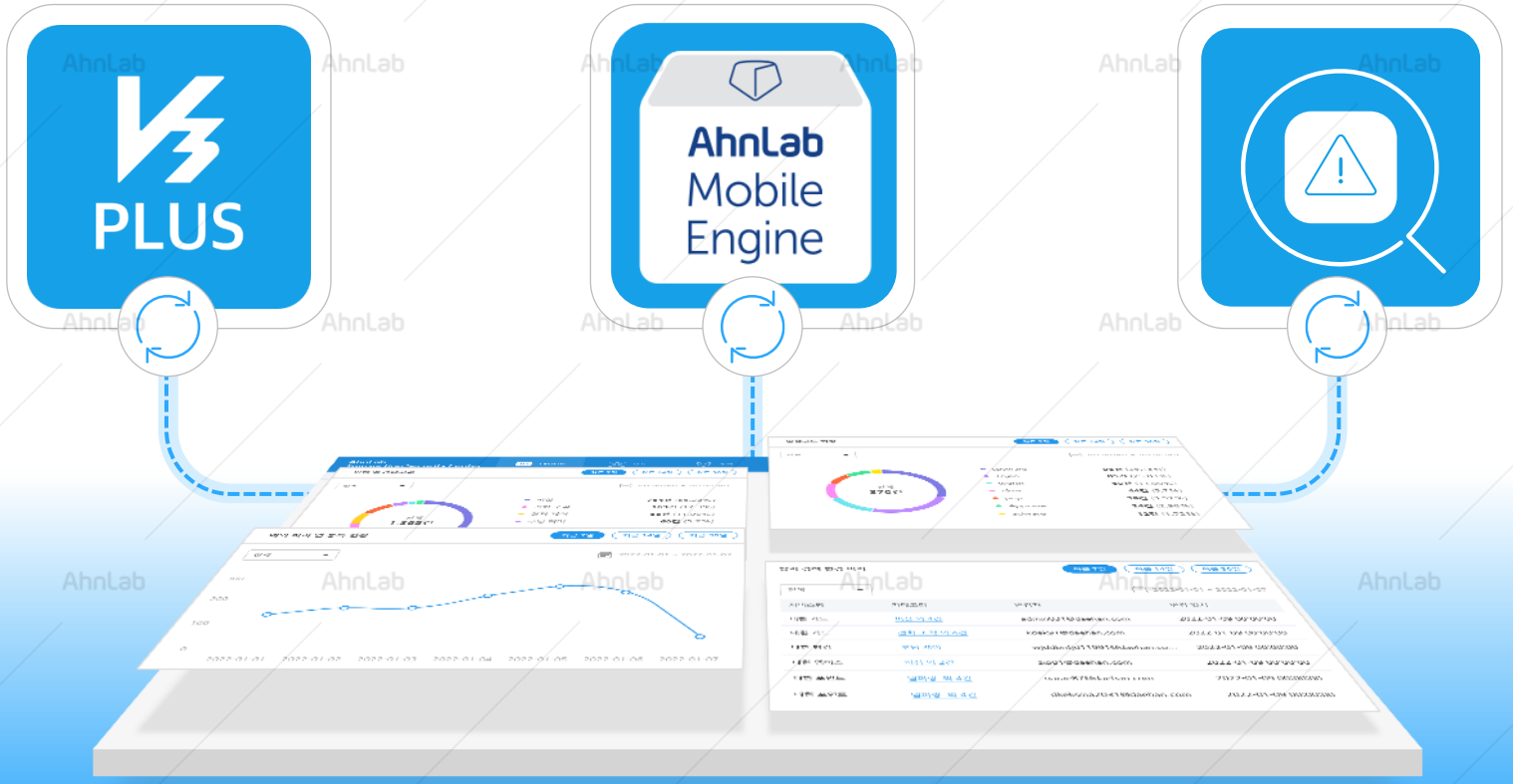
- 악성코드 탐지 결과 확인

Mobile Engine SDK 연동

- 악성코드 탐지 결과 확인

Mobile 단말 위협 정보 연동

- 위협 앱 탐지 결과 확인
- 정책 설정 및 예외 처리 등록



기능 구성

대시보드

- 위협 앱 탐지 추이 및 카테고리 비중
- 악성코드 탐지 현황
- 예외 처리 앱 등록 현황
- 탐지 정책 변경 이력

탐지

- 위협 앱 탐지 현황
- 악성코드 탐지 현황
- 위협 앱 선택 및 예외 처리
- 탐지 결과 내보내기

정책

- 탐지 카테고리 활성화/비활성화 설정
- 예외 처리 확인 및 해제
- 예외 처리 로그

통계

- 위협 앱 통계
- 악성코드 통계
- 사용 환경 통계

보고서

- 위협 앱 통계 보고서
- 악성코드 통계 보고서
- 사용 환경 통계 보고서
- 보고서 발급 이력 조회 및 PDF 다운로드

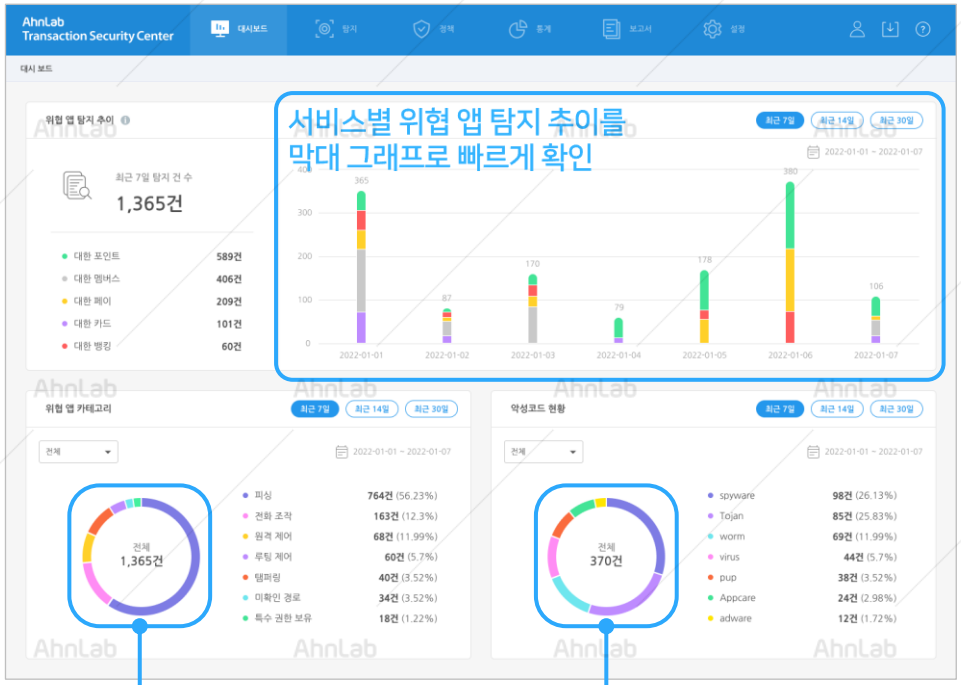
설정

- 관리자 권한 설정
- 로그인 세션 관리
- 중복 로그인 설정

주요 화면 – 대시보드

대시보드에서 최근 7일, 14일, 30일 기간에 따라 **위협 앱 탐지 추이, 카테고리, 악성코드 현황 정보를 그래프로 편리하게 파악**할 수 있습니다.
또한, 동일한 설정 기간 중, 등록된 예외 처리 앱 현황과 탐지 정책 변경 이력을 간략하게 요약하여 제공합니다.

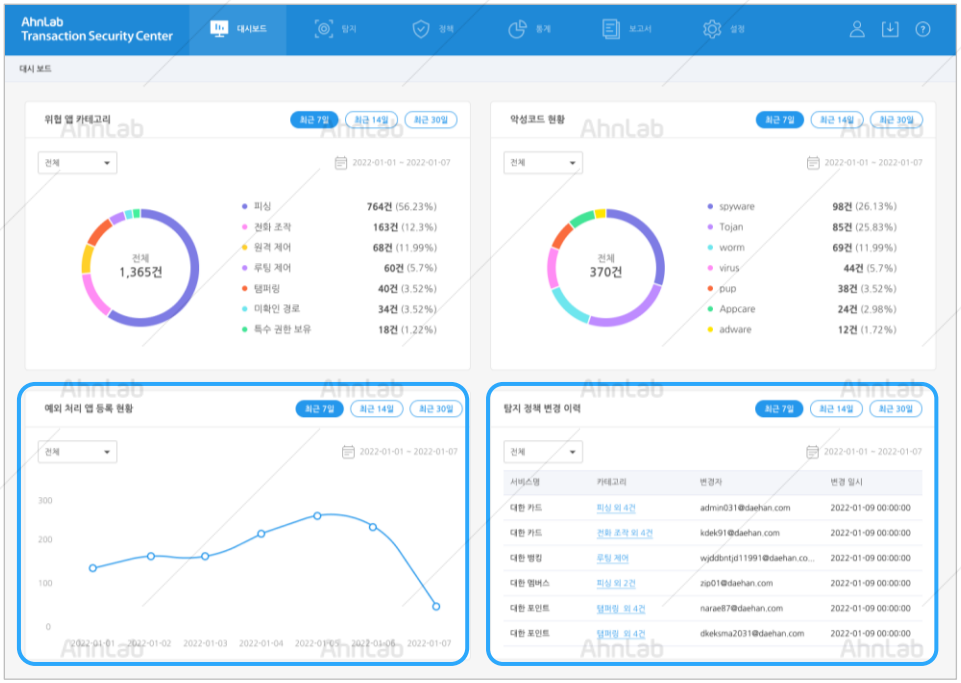
위협 앱 추이, 카테고리 및 악성코드 현황



위협 앱 카테고리
탐지 비율 확인

악성코드 진단 유형 별
탐지 비율 확인

예외 처리 앱 현황 및 탐지 정책 변경 이력



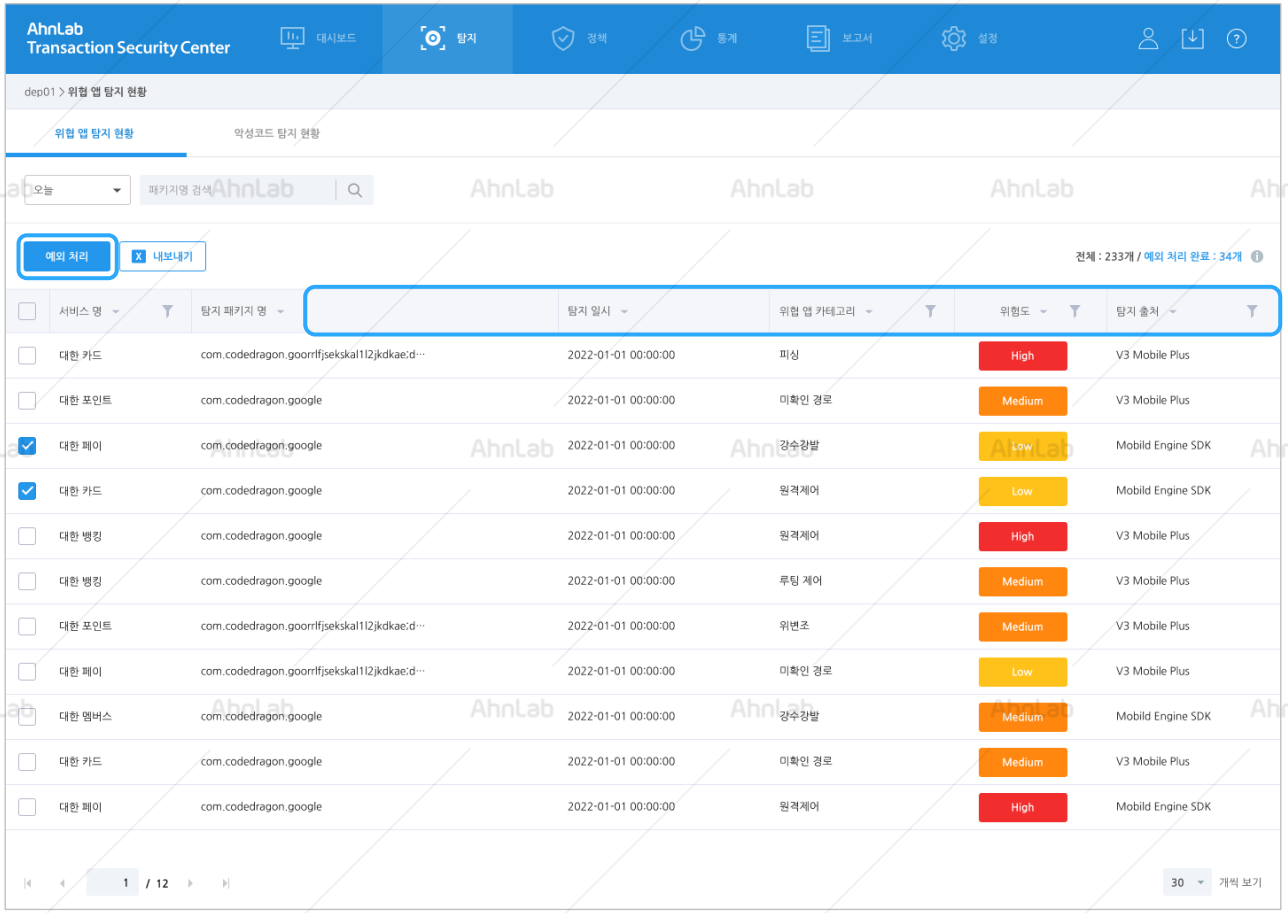
예외 처리 앱 등록 현황으로
증감 추이 확인

정책 변경 이력을 확인하여
이력 추적 가능

주요 화면 – 탐지

위협 앱의 패키지명, 탐지 일시, 카테고리 등 **모든 상세 정보를 확인할 수 있고, 예외 처리 등록도 가능**합니다.

탐지 예외 처리 가능



다양한 상세 정보 제공

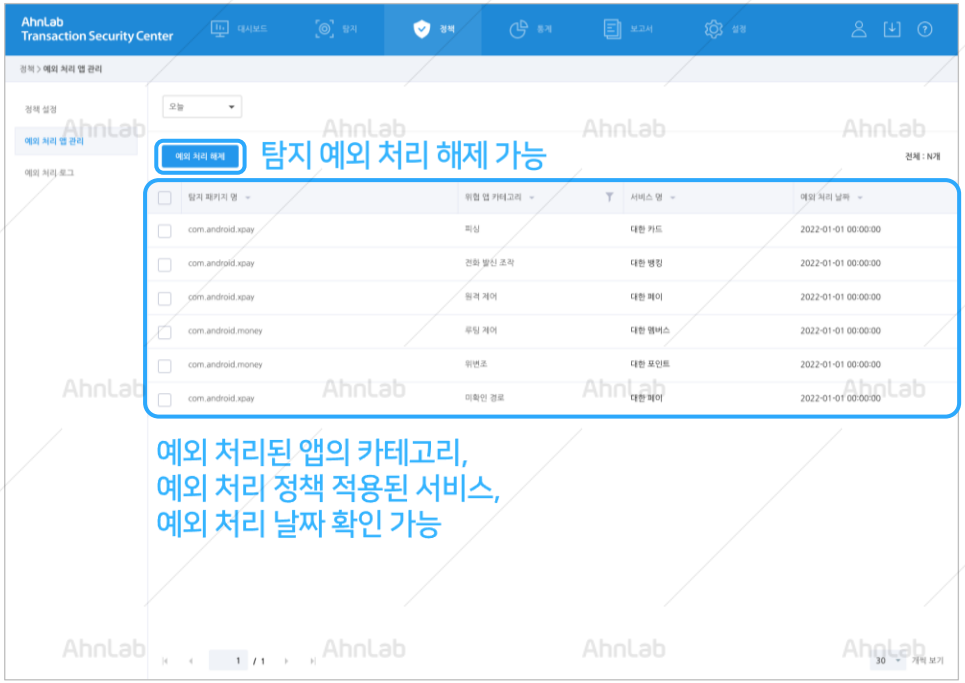
- 위협 앱 패키지명
- 탐지 일시
- 카테고리
- 위험도
- 탐지 출처
- 위협 앱 인증서 해시

주요 화면 – 정책

피싱, 전화 조작, 원격 제어 등 위협 앱 카테고리 별 탐지를 ON/OFF하여, **고객사의 상황에 맞게 보안 정책을 설정**할 수 있습니다.
탐지 예외 처리된 앱 및 카테고리, 예외 처리 날짜 등 관련 정보를 확인하여 **예외 처리된 앱을 명확하게 관리**할 수 있습니다.

정책 설정

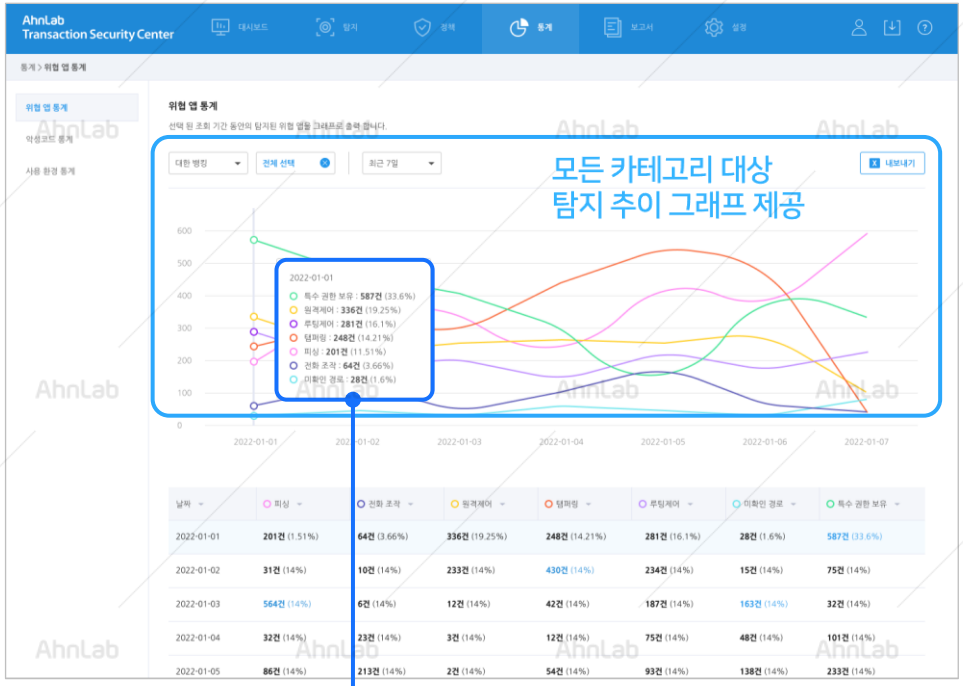
예외 처리 앱 관리



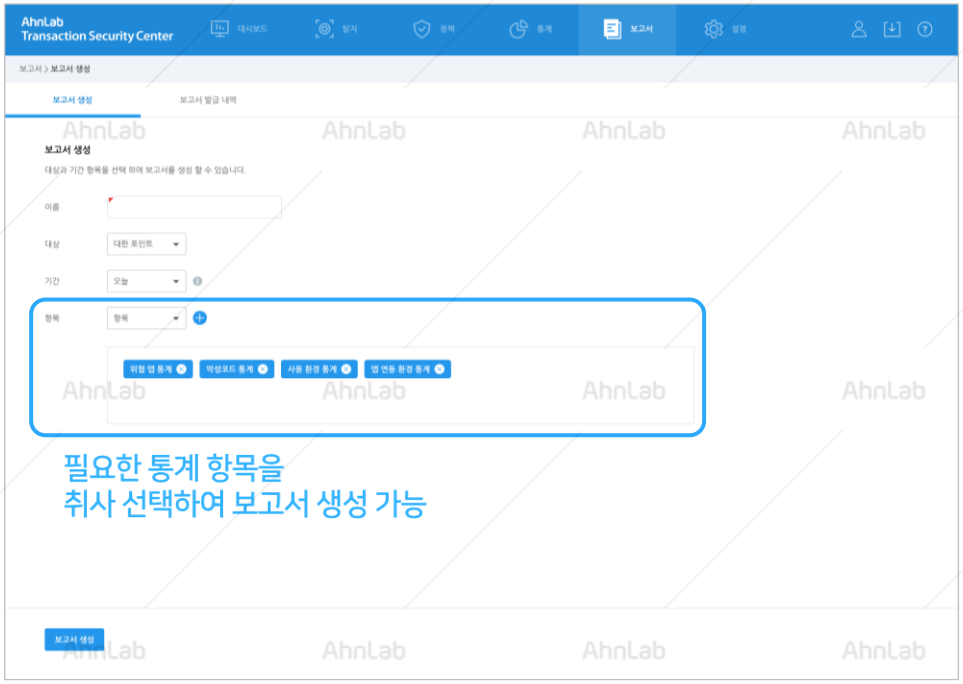
주요 화면 – 통계 & 보고서

통계 기간을 설정하여 그래프는 물론, 날짜 별 탐지 건수 및 비율 등 **다양한 통계 정보를 대시보드 대비 상세하게 확인**할 수 있습니다.
필요한 통계 항목만 취사 선택하여 보고서를 생성하고, PDF 내보내기로 공유할 수 있습니다.

통계

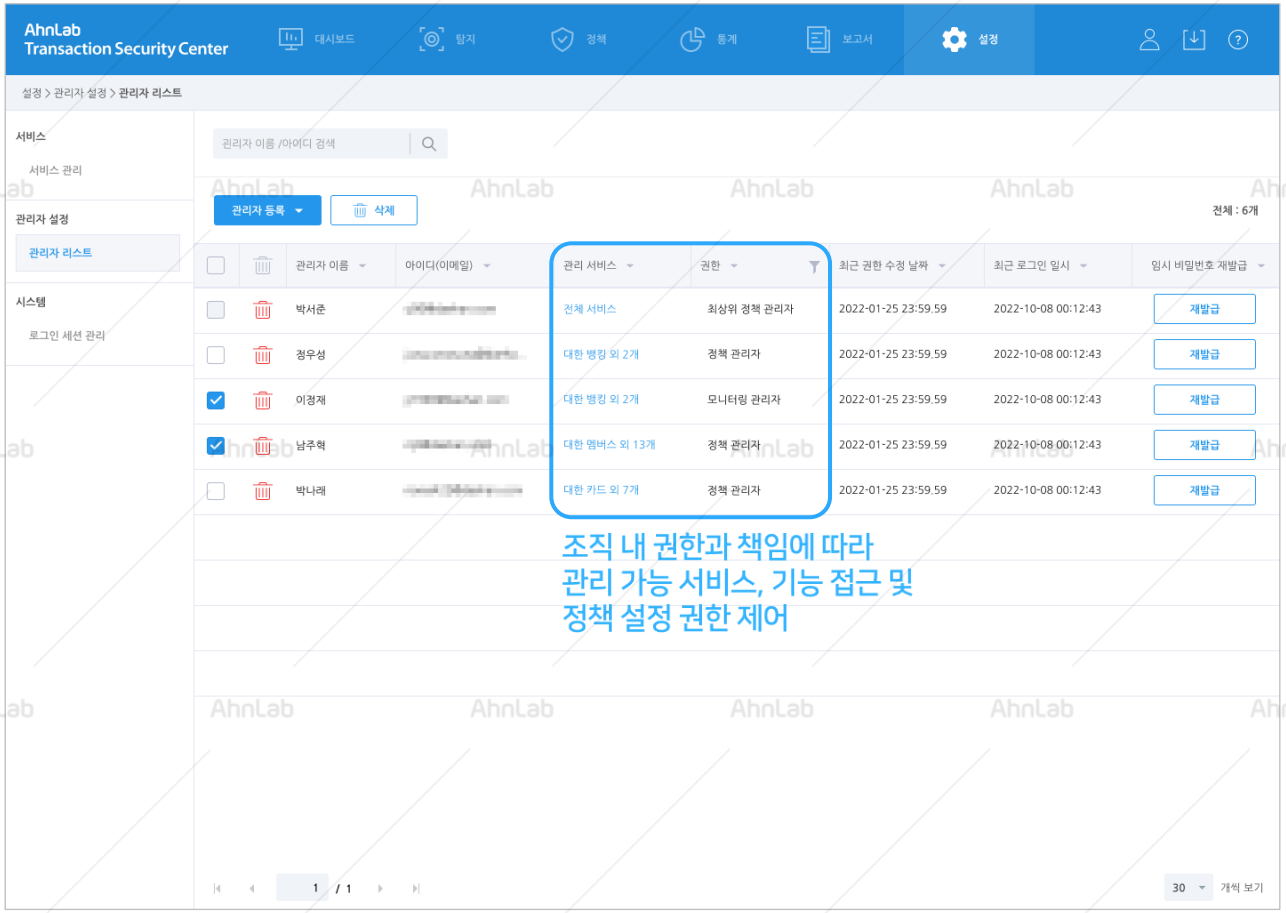


보고서



주요 화면 – 설정

모든 관리자를 확인하고 관리자 레벨을 선택하여 **기능 접근 및 정책 설정 권한을 제어**할 수 있습니다.



AhnLab
Transaction Security Center

03
도입효과

AhnLab

도입효과

AhnLab Transaction Security Center

정보 접근성 및 가시성 확보

언제 어디서든 웹 접속으로
실시간 탐지 결과 확인

막대, 추이, 파이 그래프 등을 통해
직관적인 현황을 한 눈에 파악

탐지 정보 CSV 내보내기 및
보고서 PDF 다운로드를 통해 공유

쉽고 편리한 위협 대응

위협 앱을 선택하여
손쉽게 예외 처리 등록

탐지 카테고리 별 ON/OFF 버튼을
클릭하여 탐지 정책 수립 가능

이해하기 쉬운 직관적 User Interface를 통해
정책 설정 및 위협 대응

효율적인 보안 관리

운영하는 서비스 별로
개별적 정책 설정

관리자 레벨을 설정을 통해
조직 내 권한과 책임에 따른 접근 제어 가능

탐지 현황, 위협 대응, 관리를
한 곳으로 일원화하여 보안 관리 효율성 제고

AhnLab
Transaction Security Center

※ 별첨

AhnLab

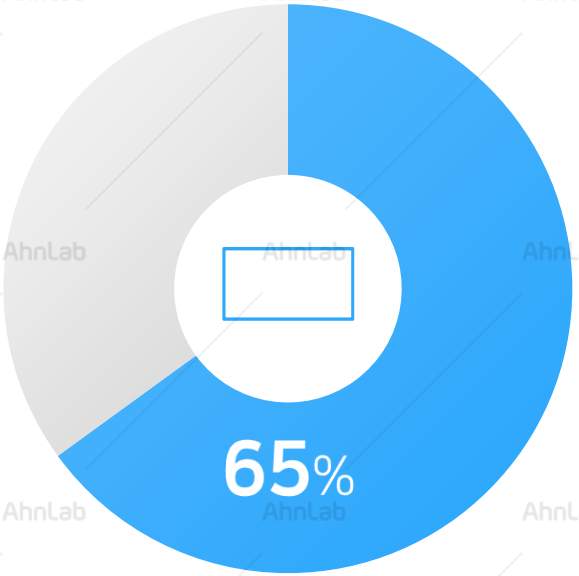
레퍼런스

※ 별첨

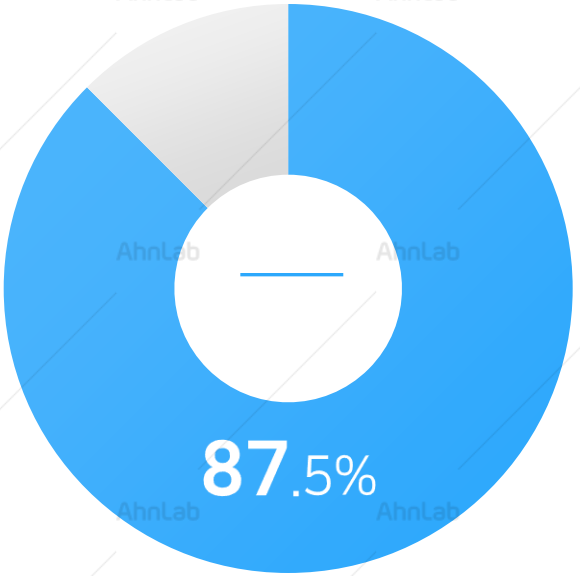
안랩의 모바일 보안 솔루션은

국내 다수 금융 고객사에 대한 레퍼런스를 갖고 있습니다.

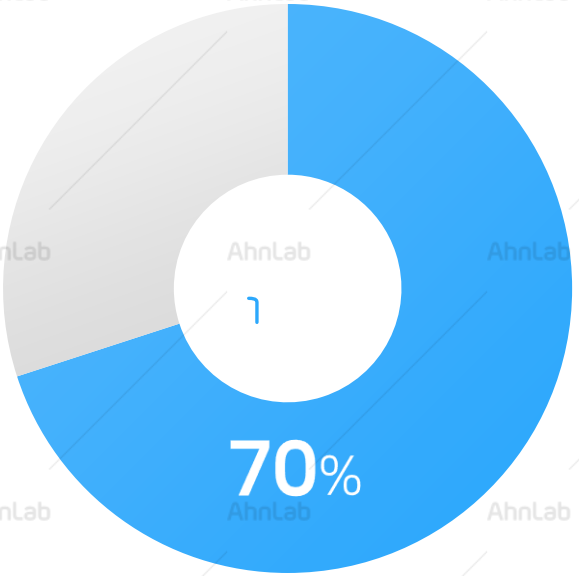
은행



카드사



증권사/금융투자회사



- 국내 제 1금융권 은행, 국책 및 특수 은행, 지방은행, 인터넷 전문 은행 중 65%
- 국내 전업 카드사 중 71% 고객사
- 국내 증권사 및 금융투자회사 중 70%
- 그 외 보험사, 금융 플랫폼 및 결제 업체 등 다수의 금융 레퍼런스 보유

글로벌 인증

※ 별첨

AhnLab 모바일 금융 솔루션은,
공신력 있는 **글로벌 인증 기관 평가를 통해 검증된 강력한 모바일 엔진**을 보유하고 있습니다.

AV-Test May 2022

100%
Protection

10년 연속 **57회** 인증 획득
(국내 유일)

AV-TEST av-test.org 05/2022 CERTIFIED ANDROID

All tested manufacturers

AhnLab, 阿里钱盾, ANTIY, ARMOR FOR ANDROID, avast, NoxSecurity, NQmobile, NSHC, MAX, panda, PLAY CASTLE
AVG, Avira, Baidu, Bitdefender, BullGuard, cheetahmobile, TOTAL AV, PSafe, 360, Quick Heal, secucloud, SECURION
COMODO, Dr. Web, eset, F-Secure, G DATA, Google, SK telecom, SOPHOS, 腾讯手机管家, ThreatTrack, TREND MICRO, WEBROOT
HAURI, Hi Security, IKARUS, NETCOP, Juniper, kaspersky, WhiteArmor, ZEMANA, Zoner AntiVirus
lookout, Malwarebytes, McAfee, eScan, NAVER Cloud, NortonLifeLock

https://www.av-test.org/en/antivirus/mobile-devices/

악성코드 대응 프로세스

※ 별첨

안랩 시큐리티 대응 센터(ASEC)의 4단계 대응 프로세스를 기반으로 강력한 악성코드 및 해킹 억제 역량을 제공합니다.

ASEC

AhnLab Security Emergency response Center

1단계 : **접수** > 2단계 : **분석** > 3단계 : **1차 대응** > 4단계 : **2차 대응**

신·변종 바이러스, 해킹 사고 접수

바이러스·해킹 툴 수집

상황 분석

1. 국내·외 피해 조사 및 예측
2. 프로그램 용도
3. 바이러스·해킹 발생 시점 및 행동 분석

샘플 분석

1. 샘플 입수·분석
2. 분석 리포트 제출
3. 대응 방식 결정
4. 대응 일정 확정

엔진 대응

1. 바이러스·해킹 툴 대응 엔진 제작
2. 엔진 업데이트

추가 공격 대응 준비

1. 변종 바이러스·해킹 툴 모니터링
2. 고객 응대 확대

모듈 변경

1. 변종 바이러스 엔진 추가 등록
2. 해킹 툴 방지 모듈 개발
3. 제품 업데이트

※ ASEC(AhnLab Security Emergency response Center)은 안랩에서 운영하는 비상 대응 조직으로, 바이러스 및 보안 위협의 24시간 감시, 신속한 대응 및 지속적인 연구를 수행하여 고객사의 중요 정보 자산 및 비즈니스 연속성을 보호하여 고객사의 대외 신뢰도 강화에 기여합니다.

More security,
More freedom

㈜안랩
경기도 성남시 분당구 판교역로 220 (우) 13493
대표전화 : 031-722-8000 | 구매문의 : 1588-3096 | 전용상담전화 : 1577-9431 | 팩스 : 031-722-8901 | www.ahnlab.com

AhnLab Transaction Security Center

AhnLab

www.ahnlab.com
www.facebook.com/AhnLabSP
www.youtube.com/user/OfficialAhnLab