데이터시트

Symantec Endpoint Protection Mobile 이전의 Skycure Mobile Threat Defense

스마트 디바이스를 위한 스마트 보안

SEP Mobile을 선택해야 하는 이유

통합 모바일 보안
다계층 모바일 방어 체계를 통해 모든 공격 경로에서 알려진 공격, 알려지지 않은 공격, 표적 공격을 차단합니다.

예측 기술
의심스러운 네트워크, 악의적 개발자, 악성 앱이 피해를 일으키기 전에 식별하여 차단합니다.

생산성 및 비침해성
모바일 경험 또는 배터리 수명 저하 없이 공용 모바일 앱을 통해 개인 정보를 보호하고 생산성을 유지합니다.

손쉬운 구축
관리와 유지 보수가 용이한 iOS 및 Android 기본 앱을 통해 신속하게 온보딩합니다.

엔터프라이즈급 솔루션
기존 엔터프라이즈 EMM/MDM, 이메일 서버, VPN과 통합하여 자동으로 IT 정책을 적용합니다. SEP Mobile은 수분 내로 수천 대의 디바이스에 구축할 수 있습니다.[1]

유효성 및 가시성
모바일 취약점, 보안 위협, 공격을 효과적으로 모니터링할 뿐 아니라 자동으로 탐지하고 제거합니다.

대규모의 크라우드 소싱 기반 인텔리전스
매우 통합적이고 효과적인 모바일 보안 인텔리전스 커뮤니티를 활용하여 제로데이 공격으로부터 보호합니다.

우수한 사이버 보안 전문성
SEP Mobile Research Labs는 전문적으로 수많은 새로운 취약점 및 보안 위협을 찾아내 리포팅합니다. 지난 4차례의 iOS 주요 릴리스 출시에는 SEP Mobile Research Labs가 리포팅한 하나 이상의 취약점에 대한 패치가 포함되었습니다.

솔루션 개요

Symantec Endpoint Protection Mobile(SEP Mobile)은 심층적인 보안 위협 인텔리전스를 통해 광범위한 기존의 보안 위협 및 알려지지 않은 보안 위협을 예측하고 탐지하면서 최고의 정확성 및 실효성으로 모바일 보안 위협을 차단하는 통합 솔루션입니다. SEP Mobile의 예측 기술은 디바이스 및 서버 기반 분석뿐 아니라 대규모의 크라우드 소싱 기반 보안 위협 인텔리전스를 활용하는 다계층 접근 방식을 통해 인터넷에 연결되었거나 연결되지 않은 상태에서 사전 예방적으로 각종 악성 코드, 네트워크 보안 위협, 앱/OS 취약점 익스플로잇을 차단하여 모바일 디바이스를 보호합니다.

솔루션 구성 요소

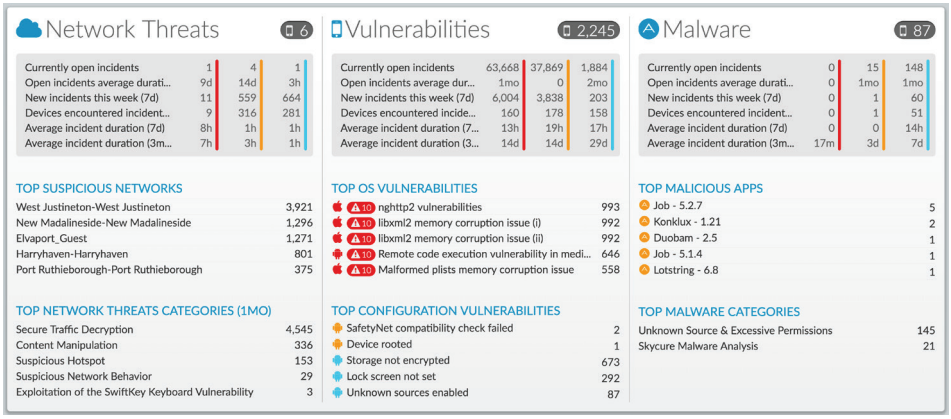
SEP Mobile의 엔터프라이즈급 모바일 보안 위협 차단 플랫폼은 아래 요소로 구성됩니다.

공용 모바일 앱

- 손쉬운 구축, 도입, 유지 보수, 업데이트
- 생산성, 경험, 개인 정보 보호에 영향을 미치지 않음[2]
- 의심스러운 특정 앱 및 네트워크를 실시간으로 차단
- 공격을 받는 경우 자동으로 회사 자산 보호
- SEP Mobile의 크라우드 소싱 기반 보안 위협 인텔리전스 데이터베이스에 데이터 제공

클라우드 서버

- 의심스러운 앱에 대해 2차 심층 분석 실시
- 앱, 네트워크, OS에 대한 머신 러닝 기반의 평판 엔진
- 대규모의 크라우드 소싱 기반 보안 위협 인텔리전스 데이터베이스
- EMM, VPN, Exchange, 기타 통합 기능으로 정책 적용
- 모든 SIEM 솔루션과 통합할 수 있도록 통합적인 활동 로그 관리



[1] 실제 고객 구축 사례 기반

[2] 고객 사례 기반

광범위한 보호

악성 코드 차단

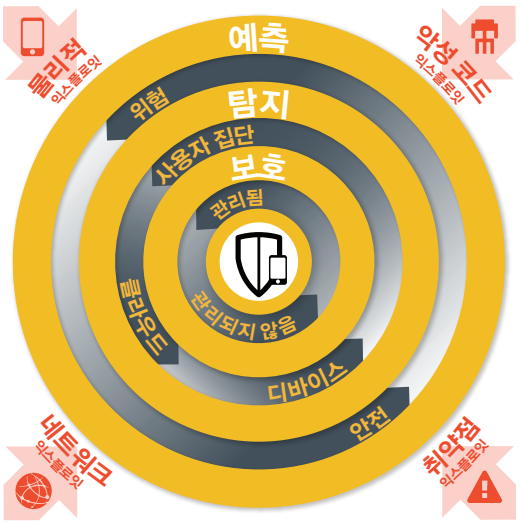
- 사전 예방적으로 제로데이 악성 리패키징 앱 차단
- 시그니처, 정적/동적 분석, 행위, 구조, 권한, 소스 등을 기반으로 한 추가 앱 분석
- 알려졌거나 알려지지 않은 각종 악성 코드 공격 및 표적 악성 코드 공격에 대해 실시간으로 대응 및 차단

네트워크 방어

- 악성 Wi-Fi 네트워크를 효과적으로 차단
- 악성 iOS 프로필 탐지, 차단, 제거
- Active Honeypot 특허 기술을 사용하여 개인 정보를 보호하면서 MITM(Man-in-the-Middle), SSL 다운그레이드, 컨텐트 조작 공격 탐지

취약점 차단

- 디바이스에서 알려진 취약점에 대한 패치 적용 여부 모니터링
- 사용자 교육, IT 보안 팀에 통지
- 앱 및 운영 체제에서 제로데이 취약점을 탐지하는 동시에 벤더에 정보 제공
- Stagefright, Accessibility Clickjacking과 같이 알려졌거나 알려지지 않은 취약점 탐지



물리적 방어

- 유일하게 MDM 기능이 통합된 MTD 솔루션 또는 기존 EMM/MDM 솔루션과의 통합을 지원하는 MTD 솔루션
- 디바이스 분실 또는 감염 시 원격 지우기 수행
- 패스코드 잠금 기능으로 기업의 정보 보호
- SEP Mobile 앱 및 프로필로 자동 업그레이드/업데이트
- 디바이스, 사용자, 그룹에 대한 통합 리포팅

심층 인텔리전스

클라우드 서버

- SEP Mobile Research Labs는 해커처럼 생각하면서 실제 해킹 공격에 대비
- 정적/동적 심층 분석에 머신 러닝을 기반으로 하는 행위 분석도 포함
- 지속적으로 미결 상태의 취약점 모니터링 및 심각도 평가
- 다른 엔터프라이즈 시스템(EMM, SIEM 등)으로부터 인텔리전스 피드 수신

사용자 집단

- 전 세계의 모든 SEP Mobile 앱이 센서 겸 데이터 수집기의 역할 수행
- 정상 및 악성 앱/네트워크의 특성 카탈로그화
- OS 버전 및 디바이스 유형을 평가하여 업그레이드 가능 여부 확인
- 리패키징 앱 및 기타 악성 코드 유형의 제로데이 탐지에 중요

디바이스

- 의심스러운 앱 및 네트워크를 식별하는 일차 방어선 역할 수행
- 다양한 특성을 기반으로 앱 추가 분석
- 정상 네트워크와 의심스러운 네트워크 모두 즉시 인식
- 리스크 데이터베이스를 대상으로 디바이스 유형, OS 버전 등의 상관관계 분석

무료 평가판*

평가판 및 리스크 평가 서비스를 통해 현재 직면한 모든 보안 위협에 대해 꼭 필요한 가시성을 확보하십시오. 5분 내로 가동하고 실행할 수 있습니다. **무료 평가판 사용 ❯**

* 해당 약관이 적용됩니다.

Symantec™ + Skycure®

시만텍코리아 | 서울시 강남구 테헤란로 152강남파이낸스센터 28층 |
TEL: 02-3468-2000 | FAX: 02-3468-2001 | **www.symantec.com/ko/kr**

SYMC-DS-Skycure-v5a_KR