Battle Card – Check Point 모바일 위협 방어

개요

MTP는 기업이 BYOD(Bring Your Own Device)의 위협을 관리하고 완화하며 모바일 사이버 위협으로부터 직원과 기업 자산을 보호하도록 지원하는 최고의 모바일 보안 솔루션입니다. 조직은 기존의 보안 및 모빌리티 인프라로 연장되는 즉각적인 위협 제거와 실시간 인텔리전스 및 가시성을 통해 모바일 장치를 확실하게 보호할 수 있습니다.

엘리베이터 피치 – 4대 판매 요점

- 최고의 위협 탐지율
- 장치, 어플리케이션 및 네트워크 내(in-network) 모바일 위협을 탐지하는 유일한 솔루션
- 투명한 사용자 경험. 장치 성능 훼손 없는 즉각적 위협 탐지와 제거
- 최고의 MDM 및 SIEM과 통합할 수 있는 실시간 가시성 및 위협 인텔리전스

현장의 중요 포지셔닝 팁

팁 1: 업계 최고의 위협 탐지율과 가장 광범위한 탐지 기능을 통해 진보된 모바일 위협을 방지하는 최고의 보안 벤더

팁 2: 투명한 사용자 경험과 MDM/EMM, Check Point SmartEvent, Check Point ThreatCloud 및 SIEM 솔루션과의 원활한 통합으로 더욱 간편해진 배포

팁 3: Check Point는 22년 동안 기업을 보호해온 입증된 실적을 가지고 있습니다.

팁 4: 주요 가전 제품 제조사는 핵심 직원 장치의 4 ~ 5%가 여러 종류의 맬웨어(mRATs, Credential Stealer, 중간자 공격)에 감염되어 있다는 것을 알게 되었습니다. CISO는 이제 모든 장치를 MTP로 보호하도록 지시합니다.

대상 시장/구매자

대상 시장

- COD 및 BYOD가 있는 기업

대상 구매자

- 고위 보안: 최고정보보호책임자(CISO), 보안/IT 부사장, 보안/IT 전무/이사
  - 참고: 전체 보안 전략을 책임지고 있는 고위 보안 담당자를 만날 수 있어야 합니다.
- 모빌리티/최종 사용자 컴퓨팅 책임자
  - 참고: MDM/EMM 전략/정책의 책임자.

가장 포괄적인 솔루션: 다음 모두에 대하여 모바일 위협 탐지를 제공하는 유일한 솔루션입니다.

장치(OS)
공격, 취약점, 구성 변경 탐지

어플리케이션
악성 앱 탐지

네트워크
중간자 공격 탐지

영업 지원 리소스

성공 사례
미국에 본사를 둔 가전 제품 제조사
금융 서비스 회사

관련 비디오
작동 중인 모바일 보안 – 기업이 위협을 앞지를 수 있는 방법
(Samsung Research America의 사례 연구 포함)
설명자 비디오

제품 페이지
내부
외부

기타 리소스
백서, 데이터시트 등

Battle Card – Check Point 모바일 위협 방어

경쟁 방법...

FireEye

- **애플리케이션에만 주력** – 이 솔루션은 네트워크 및 모바일 OS 우회 공격과 같은 다른 공격 형태를 예방할 수 없기 때문에 장치를 취약한 상태로 방치합니다.
- **예방적 보호 기능 없음** – 이 솔루션은 이미 감염된 장치에서 위협을 완화하기 위해 추가 비용이 드는 제3자 솔루션(MDM)이 필요합니다.

Lookout

- **애플리케이션에만 주력** – 이 솔루션은 네트워크 및 모바일 OS 우회 공격과 같은 다른 공격 벡터를 예방할 수 없기 때문에 장치를 취약한 상태로 방치합니다.
- **예방적 보호 기능 없음** – 이 솔루션은 이미 감염된 장치에서 위협을 완화하기 위해 추가 비용이 드는 제3자 솔루션(MDM)이 필요합니다.
- 기업 MDM과의 **제한적 통합**(MobileIron & Airwatch만)

Zimperium

- **제한적 탐지법** – 이 솔루션은 장치에서 악성 활동을 탐지하기 위해 행태 분석만 사용하기 때문에 장치를 보다 정교한 공격 벡터에 노출된 상태로 방치합니다.
- **예방적 보호 기능 없음** – 이 솔루션은 이미 감염된 장치에서 위협을 완화하기 위해 추가 비용이 드는 제3자 솔루션(MDM)이 필요합니다.
- 기업 MDM과의 **제한적 통합**(MobileIron & Airwatch만)

Skycure

- **부분적 보호** – 이 솔루션은 네트워크 우회 공격(MiTM)에 대한 보호에 주력하고 있으며, 악성 어플리케이션과 OS 우회 공격과 같은 다른 공격 벡터에 대해서는 장치를 취약한 상태로 방치합니다.

Palo Alto Networks

- **사내 솔루션만** – 모든 모바일 트래픽은 사내 PAN 하드웨어에서 경로가 재설정되어야 합니다(관리 및 게이트웨이에 추가 비용 발생). 모바일 트래픽의 경로 재설정은 모바일 트래픽에 대역폭과 지연 문제를 초래할 수 있습니다.
- **부분적 보호** – Palo Alto Wildfire는 Android 어플리케이션만을 분석할 수 있으며, iOS 기반 공격과 우회 공격에 대비한 보호 능력이 제한적입니다.

핵심 기능 비교

비교 대상	Check Point	FireEye	Lookout	Zimperium	Skycure	Palo Alto Networks
알려지지 않은 악성 앱 탐지	●	●	●	◓ 1	●	◓ 2
OS 변경 및 장치 우회 공격 탐지	●	◔ 3	◔ 3	◓ 4	◔	◔ 4
악성 네트워크 연결 탐지(MiTM)	●	○	○	●	●	○
완전한 장치 위험 평가(장치, 앱 및 네트워크 활동 연관)	●	◔ 5	◔ 5	◓ 6	●	◓ 7
적응형 완화 및 교정	◔	◓ 8	◓ 8	◓ 8	◔	◓
클라우드 기반 모바일 위협 프레젠테이션	●	○	○	○	○	◓ 9
모바일 장치를 위한 보안 컨테이너	●	◔ 10	◔ 10	◔ 10	◔ 10	◔ 10
요약						
완전한 모바일 위협 방어 솔루션	●	◔	◔	◓	◔	◓

WEAK — STRONG

1) B행태 분석만
2) Android 앱만
3) 장치 루팅/탈옥
4) 장치 모니터링
5) 앱만
6) 네트워크 및 앱
7) HIP만
8) MDM 필요
9) 사내 어플라이언스 포함
10) 제3자 MDM 경유

[기밀]—Check Point 사용자 및 승인된 제3자용.

Battle Card – Check Point 모바일 위협 방어

고객 스크립트/질문

모바일에 대한 사이버 위협이 증가하고 있습니다! 어떤 대형 가전 제품 기업은 최근에 자사 모바일 장치의 4~5%가 회사의 데이터 및 보안을 위험에 빠뜨리는 고급 맬웨어에 감염되었다는 것을 알게 되었습니다.

- 귀하의 모바일 장치에 어떤 위협이 있는지 알 수 있습니까?
- 사용자가 다운로드했던 앱의 악성 여부를 알고 계십니까?
- 장치가 감염되면 어떻게 알 수 있습니까?
- 귀하의 MDM은 고급 위협/맬웨어를 차단할 수 있습니까?

이의 처리

MDM/EMM 솔루션이 이미 있습니다.
MDM은 모바일 액세스를 지원하고 정적 정책 제어를 제공하지만 APT, 스파이웨어, 중간자 공격(Man-In-The-Middle Attack, MiTM) 등과 같은 고급 모바일 위협에 대한 보호는 제공하지 않습니다. MTP가 위협을 탐지하면 사용자가 이를 즉시 제거하여 생산성을 유지할 수 있습니다.

필요한 모든 보안을 제공하는 보안 컨테이너가 이미 있습니다.
보안 컨테이너는 무단 액세스나 데이터 유출을 예방하도록 설계되었지만 모든 모바일 위협으로부터 보호하지는 않습니다. Check Point는 맬웨어가 보안 컨테이너의 암호화를 바이패스하고 데이터를 유출할 수 있는 방법을 시연할 수 있습니다.

저의 iOS는 안전하다고 생각합니다.
iOS 장치는 기본적으로 Android보다 안전합니다. 하지만 장치에 탈옥이 발생하지 않은 경우에도 iOS를 훼손할 수 있는 다양한 위협이 상당 부분 존재합니다. Check Point는 라이브 데모로 이를 시연할 수 있습니다.

우리의 모바일 보안에 문제가 있다고 생각하지 않습니다.
모바일 위협의 수량과 정교함이 증가하면서 고객의 감염률이 높아지고 있음을 확인하고 있습니다. 문제가 아니라는 것을 알 수 있는 완전한 가시성을 보유하고 있다고 확신하십니까?

요약 - 승리 보장

MTP는 기업을 위한 가장 높은 수준의 모바일 보안을 제공합니다.

- 장치, 어플리케이션 및 네트워크 내(in-network) 모바일 위협을 탐지하고 교정하는 유일한 솔루션
- 완전한 모바일 위협 가시성과 인텔리전스를 제공합니다.
- 단순한 배포와 투명한 사용자 경험을 제공합니다.

고객의 업무에 따른 접근방법

최고정보보호책임자(CISO), 보안/IT 부사장, 보안/IT 전무/이사

사이버 보안 관심사:

- 브랜드 평판
- 고객 및 시장 신뢰
- 규정 준수 및 비즈니스 위험(사이버 보안 관련)
- IT의 운영 효율성

모바일 보안 관심사

- 모바일은 새로운 공격 벡터. 모바일 위협에 대한 가시성 없음
- 위협이 정말로 존재한다는 것이 납득이 되지 않을 수 있음
- 그들이 제어하지 않는 것을 보호하는 방법을 이해(Bring Your Own Device, BYOD)
- 사용자 경험이나 장치 성능에 영향을 주지 않고 강력한 보안을 제공할 수 있는 능력

우리의 가치:

- 모바일을 위한 최고 수준의 보안 제공
- 위협에 대한 즉각적 교정 제공
- 위협에 대한 완전한 가시성 제공
- 보안 훼손 없이 BYOD를 배포하도록 지원
- 모빌리티와 보안 통합을 통한 배포 단순화

모빌리티/최종 사용자 컴퓨팅 책임자

모바일 사이버 보안의 관심사:

- IT의 운영 효율성
- 제어 정책과 규정 준수
- 사용자 경험이나 장치 성능에 영향을 주지 않고 강력한 보안을 제공할 수 있는 능력
- 보안팀의 신뢰와 예산 필요

우리의 가치:

- 기존의 MDM/EMM에 추가적인 보안 계층 추가
- MDM/EMM을 통해 손쉬운 배포 지원
- Check Point Capsule을 통해 MDM 없이 고객 지원
- 위협에 대한 즉각적 교정 제공
- 위협에 대한 완전한 가시성 제공
- 보안 훼손 없이 BYOD를 배포하도록 지원