CHECK POINT
MOBILE THREAT PREVENTION

특장점

- 조직의 네트워크에 적합한 iOS 또는 Android 모바일 장치 설치
- 모바일 장치안에 있는 민감한 정보를 사이버 스파이로부터 보호
- 기존의 모빌리티와 보안 인프라(MDM, MAM, NAC, SIEM 등)에 쉽게 통합할 수 있는 모바일 보안 기능을 통해 최신 모바일 위협에 대한 가시성 및 보호 기능 개선
- Microsoft Exchange와 컨테이너/랩퍼 (container/wrapper) 솔루션의 보안 수단 증가
- 여러 플래폼에 걸친 APT공격에 대한 신속한 대응 지원
- 허가된 사용자들은 관리되지 않는 장치에서 기업 데이터에 안전하게 액세스하도록 지원
- 조직 또는 규제기관의 지시에 따라 필요한 보호 기능을 추가하는 동시에 사용자 경험과 프라이버시 보호

공격이 시작되기 전에 탐지하고 차단

오늘날에는 스마트폰과 태블릿을 이용해서 중대한 비즈니스 정보에 그 어느 때보다 쉽게 접근하여 보다 빠르고 정확하게 업무를 처리할 수 있게 되었습니다. 직원들이 원하는 모바일 장치에서 이러한 정보에 액세스할 수 있도록 허용하는 것은 많은 장점이 있지만 기업을 위험에 노출시키기는 단점도 있습니다.

iOS와 Android 장치의 모바일 보안에 대한 혁신적 접근방식인 Check Point 모바일 위협 방어(Mobile Threat Prevention)는 모바일 위협이 시작되기도 전에 이를 탐지하고 중단시킵니다. 데이터가 장치에 머물러 있거나 클라우드를 통해 이동 중이거나, 모바일 위협 방어(Mobile Threat Prevention)는 데이터를 위험에 처하게 하는 취약점과 공격으로부터 보호합니다.

기업을 위한 가장 높은 수준의 모바일 보안

오직 Check Point만이 OS, 어플리케이션, 네트워크 상에서의 위협으로부터 장치를 보호하고 iOS와 Android를 위한 업계 최고의 위협 탐지율을 제공하는 완전한 모바일 보안 솔루션을 제공합니다. 모바일 위협 방어(Mobile Threat Prevention)는 악성 앱 탐지 기능을 통해 위협 에뮬레이션, 진보된 정적 코드 분석, 앱 평판 및 머신 학습을 적용하여 알려진 위협과 알려지지 않은 위협을 찾습니다. 또한 보호되지 않은 Wi-Fi® 네트워크 액세스와 중간자 공격으로부터 장치를 보호하고 위협이 탐지되었을 때 기업 네트워크에 대한 액세스를 중지시킵니다.

공격면을 줄이기 위해 공격, 취약성, 구성 변경 및 진보된 루팅과 탈옥을 탐지하여 디바이스의 OS수준에서 실시간 위험 평가를 사용하며, 동적인 위협 대응을 통해 손상된 장치가 조직의 네트워크에 액세스하는 것을 예방하고, 조직이 장치에서의 위협 완화 및 제거를 위해 고유의 한계점을 기반으로 적응 정책 제어를 설정하도록 지원합니다.

진보된 어플리케이션 분석

민감한 기업 자산에 액세스하는 직원을 신뢰할 수 있겠지만 그들의 어플리케이션도 신뢰할 수 있습니까? Check Point의 솔루션은 앱이 장치에 다운로드 되면 이 앱이 승인되거나 악성으로 플래그 표시되기 전에 캡처하여 가상의 클라우드 기반 환경에서 실행시키고 행위를 분석합니다. 이해하기 쉽고 생성하기 쉬운 Check Point의 분석 보고서는 보안팀이 직원이 사용하는 앱이 안전한지 확인하는 것을 돕습니다.

네트워크 기반 공격

공공 장소는 개방형 Wi-Fi 네트워크로 가득하기 때문에 어떤 네트워크가 안전하거나 안전하지 않은지 알기가 어렵습니다. 사이버 범죄자는 스마트폰과 태블릿을 가로채기 위해서 안전하지 않은 네트워크를 사용하고, 메시지, 파일, 네트워크 기밀정보와 같은 중요 데이터를 조정합니다. Check Point의 솔루션은 악성 네트워크의 행위와 상태를 탐지하고 의심스러운 네트워크를 자동으로 비활성화시켜 장치와 데이터를 안전하게 지킵니다.

August 6, 2015

디바이스 취약성 평가

사이버 범죄자는 디바이스 보안의 약한 고리를 먼저 발견하려고 하며, 이러한 약한 고리에는 다른 보안 솔루션이 탐지하지 못하는 운영 체제와 앱의 약점이 포함되어 있습니다. Check Point의 솔루션은 사이버 범죄자가 장치를 공격하고 정보를 훔치기 위해 이용하는 취약성과 행위를 알아내기 위해 지속적으로 장치를 분석합니다. 또한 모바일 장치가 직면하는 위협에 대한 가시성을 개선하면 전체적인 공격면과 위험을 줄일 수 있습니다.

완전한 모바일 위협 가시성과 인텔리전스

모바일 위협 방어의 클라우드 기반 대시보드는 지원되는 장치의 관리와 모바일 위협 제어를 빠르고 간편하게 합니다. 이는 보안팀과 모빌리티팀에게 비즈니스 또는 사용자에게 영향을 줄 수 있는 모바일 위협의 수량과 유형에 대한 실시간 위협 인텔리전스와 가시성을 제공합니다.

인텔리전스와 기존 시스템의 통합

모바일 위협 방어의 실시간 위협 인텔리전스 스트림은 보안 이벤트 모니터링과 내부 네트워크에 대한 공격과의 상관 관계에 대해 자동으로 Check Point SmartEven에서 분석해줍니다. 이 정보는 사이버 공격 발생을 예방하기 위해 네트워크 환경 내에서 사용할 수 있는 광범위한 일체의 위협 인텔리전스를 제공하면서 Check Point의 위협 클라우드에서 공유되고 상관관계가 있습니다. 위협 인텔리전스는 또한 보안 정보 및 이벤트 관리(Security Information and Event Management, SIEM) 플랫폼과 같은 기존의 기업 시스템에 제공될 수도 있습니다. 여기에는 상세한 로그와 다른 훼손 지표가 포함되며, 이는 보안팀이 위험을 통제하고 제거하기 위한 조치를 신속하게 취하는 데 도움이 되는 대응 조치를 트리거하도록 필터링할 수 있습니다.

가장 간편한 모바일 보안 배포

보안팀과 모빌리티팀은 신경을 써야 할 일이 많기 때문에 이들이 MDM 또는 EMM 솔루션과의 통합 및 협력을 통해 모바일 장치를 신속하고 확실하게 지킬 수 있도록 돕기 위해 모바일 위협 방어(Mobile Threat Prevention)가 고안되었습니다. 모바일 위협 방어는 솔루션의 확장성을 크게 개선하며, 광범위한 보안 인프라 내에서 모바일 보안을 관리할 수 있도록 강력한 운영 및 배포 효율성을 제공합니다.

간편하게 진보된 모바일 보안 배포

지원하는 장치가 300개이건 30만 개이건 관계 없이 Check Point의 솔루션은 기존 MDM과 쉽고 빠르게 통합할 수 있습니다. 기존 MDM을 통해 자동으로 배포하고 관리할 수 있기 때문에 채택이 신속하고 전체적 운영 비용이 감소합니다. Check Point의 솔루션은 기존의 MDM과 함께 확장할 수 있으며 등록한 모바일 장치를 완벽하게 보호하고 기능들을 제거 할 수 있습니다. 그 결과 고도로 역동적인 환경에서도 모바일 장치를 관리하고 보호하기 위해 필요한 보안 계층을 유지하기 때문에 안심할 수 있습니다.

장치에서 직접 위협 완화 및 제거

위협이 식별되면 Check Point 솔루션은 위협이 제거될 때까지 자동으로 위험을 완화시킵니다. 장치에서 즉시 위협을 제거할 수 있는 경우 이에 대해 사용자에게 알림을 제공하고 악성 앱 삭제 또는 즉각적으로 네트워크 분리 등과 같은 조치를 취하도록 메시지가 표시됩니다. 기존 MDM과의 통합은 보안 컨테이너 액세스를 제한하거나, 손상된 장치에서의 실시간 위험 기반 정책 조정을 수행하도록 솔루션을 지원하는데 이는 MDM이 자체적으로 수행할 수 없는 기능입니다. 또한 Check Point 솔루션은 사용자 연결 상태는 계속 유지하면서도 데이터 트래픽을 사이버 범죄자로부터 멀리 유지하고 데이터 유출을 피하기 위해 요구사항에 맞는 VPN을 활성화할 수도 있습니다.

사용자 프라이버시 존중 및 장치 성능

최종 사용자의 프라이버시는 매우 중요하기 때문에 Check Point는 절대로 파일, 브라우저 이력, 또는 어플리케이션 데이터를 분석하지 않습니다. Check Point의 솔루션은 장치가 손상되었는지 여부를 결정하기 위해 운영 체제, 앱, 네트워크의 상태 및 콘텍스트 메타데이터를 사용하며 분석에 사용하는 데이터를 익명화하여 보존하고 보안 인텔리전스 정보는 별도로 보관합니다. Check Point는 장치 성능에 영향을 주지 않기 위해 클라우드에서 분석을 수행하며 보호 기능은 백그라운드에서 실행되기 때문에 사용자는 새로운 것을 알아야 할 필요 없이 계속 보호를 받습니다.

자세한 내용은 checkpoint.com/mobilesecurity에서 확인하십시오.

연락처

본사 | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | 전화: 972-3-753-4555 | 팩스: 972-3-624-1100 | 이메일: info@checkpoint.com
한국지사 | 서울특별시 영등포구 국회대로62길 21 동성빌딩 7층 | 전화: 02-786-3303 | 팩스 02-761-9391 | krissl@checkpoint.com

August 6, 2015