IBM Security
리더십 사고의 백서

Android 과자에 만족

Android의 후식 이름으로 된 업데이트 사항은 장치와 데이터 보안을 기업에 적용할 만큼 충분히 개선시켰습니까?

IBM

Android는 기업을 위해 준비를 마쳤습니다. 여러분의 기업은 Android를 위해 준비를 마쳤습니까?

서론

Android는 오랜 기간 소비자 시장에 군림해왔습니다. 이제, Google과 장치 제조업체의 최신 보안 개선 사항 및 뛰어난 EMM 솔루션 제공업체 지원을 통해 기업 내 그 존재감을 확장하고 있습니다. 보안과 업계 표준 및 정부 규정의 준수 보장을 지원하기 위해, 기업은 광범위한 이용 가능 장치, 버전 및 세계에서 가장 유명한 모바일 운영 체제의 독특한 성격을 보호하고 관리하는 방법이 필요합니다.

"일률적으로 적용되는 (one-size-fits-all)" 솔루션은 없습니다. IT는 장치 및 애플리케이션 환경을 검사하고 사용자 지정된 엔터프라이즈 이동성 전략에 어떤 보안 및 관리 기능이 필수인지 결정해야 합니다. EMM에 대한 유연한 접근법을 제공하는 MaaS360®과 같은 플랫폼을 통해 기업에서는 기본 장치 및 OS 제어, 데이터 컨테이너화, 클라우드 기반 확장성을 활용해 자신 있게 Android를 수용할 수 있습니다.

회사에서는 직원이 자체 선호 또는 기업별 장치를 사용할 수 있게 하지만, IT는 기업 데이터 보호와 표준화된 관리 제공이라는 실질적인 문제를 해결해야 합니다.

어디에나 있는 Android: 만족한 결과 및 좋지 못한 결과

전 세계 84% 모바일 장치 시장 점유율을 확보하여[1], Android는 전 세계 190개 이상의 국가에서 업무와 즐거움을 위해 수백만 개의 모바일 장치를 구동합니다. 최대 모바일 플랫폼 기반이며 계속 성장하고 있습니다. Android 장치를 광범위하게 제공할 수 있다는 점은 종종 기업 소유 장치 프로그램에 적합하다는 의미입니다. 예를 들어 수많은 필드 기반 직원에게는 먼지, 충격, 진동, 비, 습도, 태양 방사, 고도, 극한의 온도를 견뎌내도록 구축된 견고한 Android 장치가 필요합니다. 다른 곳에서는 제고 관리와 창고 운영에 적합한 데이터 캡처 기능을 갖춘 Android 장치를 원합니다.

이러한 성장에는 의도하지 않은 결과와 IT를 위한 중요한 고려사항이 수반되기도 합니다. 회사에서는 직원이 자체 선호 또는 기업별 장치를 사용할 수 있게 하지만, IT는 기업 데이터 보호와 표준화된 관리 제공이라는 실질적인 문제를 해결해야 합니다.

세계에서 가장 유명한 모바일 플랫폼은 휘발성 보안 기록도 갖추고 있습니다.[2] 그러나 최근 과자 이름으로 명명된 Android 제품 버전 4.0 (Ice Cream Sandwich, Jelly Bean, KitKat), 5.0 (Lollipop) 및 6.0 (Marshmallow)은 과거 보안과 관련해 최대 약점을 보완했습니다. 운영 체제 측면에서 볼 때, Android 4.0은 암호화, 인증 관리를 위한 새로운 공용 키체인 프레임워크 및 메모리 착취 등 정교한 공격으로부터 보호합니다. Android 5.0에서 수많은 핵심 보안 기능이 사용자를 위해 자동 조정되며, 잠금 화면, 장치 암호화, 장치 관리자 (손실된 장치를 찾거나 원격으로 지우는 데 도움을 줄 수 있음)를 포함합니다. Google은 또한 SELinux (Security Enhanced Linux)의 실행 모드를 의무화했고, 애플리케이션 및 사용자의 특권을 필수적으로 제한해 시스템 상의 보안 위반을 방지했습니다. 기업 환경을 위한 BYOD를 지원하도록 돕기 위해, Android 5.0의 신규 관리형 프로비저닝 프로세스는 장치 상에서 보호되는 작업 프로필을 생성합니다. 설치 관리자에서 앱은 IT 관리자가 작업 프로필 내부에서 앱과 데이터를 관리하고 있음을 나타내는 작업 배지와 함께 표시됩니다.

개인 및 작업 프로필 알림이 통합 보기로 표시됩니다. 각 프로필의 데이터는 동일한 앱이 두 프로필에서 사용될 때를 포함해 서로 분리된 채로 있습니다.

Android 5.0은 또한 휴대폰 및 태블릿을 위한 게스트 모드를 제공하며, 앱을 고정 (또는 잠금) 시켜 사용자가 장치의 다른 부분으로 액세스할 수 없습니다. 이는 또한 소매점에서 디스플레이된 장치의 키오스크 모드에서도 앱을 이용할 수 있는 탁월한 방법이기도 합니다.

업무용 Android

Google이 기업의 목소리, 그리고 요구사항에 귀 기울여 왔다는 점은 명백합니다. 업무용 Android 출시를 준비하면서, Google은 IT에 컨테이너화 및 기업 대비 보안 제어를 위한 옵션을 제공합니다. 신규 기업 관리 플랫폼을 통해, 업무용 Android는 IT에 다음 사항을 지원합니다.

- Android 스마트폰에서 업무용과 개인 데이터 분리
- 무료 및 유료 Google Play 앱을 쉽게 관리 및 배포

업무용 Android는 Lollipop으로 자동 통합되어 Android 4.0+를 실행하는 모든 장치의 앱으로서 사용 가능합니다.

제조업체: 내장형 보안 및 EMM 통합

삼성, HTC, LG 및 Amazon 등 수많은 최고의 Anroid 장치 제조업체 또한 최신 장치에서 기업 수준의 보호를 구현했습니다. SD 카드 원격 지우기 및 파일 암호화, 기업급 WLAN 보안, VPN 액세스 및 단일 장치에서 개방형 및 암호화 정보를 동시 지원하는 기능 등의 내장형 기능을 활용하는 수많은 Android 장치는 기업 용도 사용에 보다 적합합니다.

- 삼성 KNOX는 기업 인텔리전스를 관리, 유지관리 및 보호가 가능한 보호 컨테이너를 제공합니다.
- HTCpro 인증 장치는 정부 등급 데이터 암호화는 물론 VPN 및 기타 고급 보안 기능을 제공합니다.
- Amazon Fire 장치는 등록, VPN, 단일 사인온 (SSO) 및 인증서 등록 기능을 갖추고 있습니다.
- LG GATE 지원 모바일 장치는 Microsoft Exchange ActiveSync, 데이터 암호화 및 VPN 지원이 가능한 고급 보안 관리성을 제공합니다.

이러한 네 곳과 기타 Android 장치 제조업체는 핵심 보안 기능을 지원했을뿐만 아니라, 업계 최고의 엔터프라이즈 이동성 관리 (EMM) 솔루션 제공업체와의 파트너십을 개발했습니다. EMM 통합 및 API는 기업이 단일 포털을 통해 견고한 관리와 보안 기능을 경험할 수 있게 합니다.

모범 사례 및 기능

Android 버전 4 및 5의 광범위한 보안 개선 사항을 고려한다면, IT는 모든 장치가 Android 4.0 이상 버전에서 실행되고 비밀번호 보호를 설정하도록 해야 합니다. 이는 단편화와 암호화 부족으로 인한 "기존의 Android 위험"을 줄입니다. Android의 유연성이 일부 "목적에 맞는" 장치를 통해 기업 (및 사용자) 을 만족시키는 반면, 이는 또한 노출을 일으켜 IT로 하여금 기업 데이터를 보호하고 루팅 및 모바일 악성 프로그램으로부터 보호하도록 구현할 것을 요구합니다.

위험한 루팅: 기업 금기사항

사용자는 UNIX 코어에 액세스함으로써 Android 장치를 "루팅"할 수 있으며, 이를 통해 악성 프로그램 등 거의 모든 애플리케이션을 설치하게 하고, 애플리케이션급 제어를 뒤엎을 수 있습니다. "루팅된" 장치는 기업 네트워크를 장치에 있는 동일한 악성 프로그램에 노출시키고 데이터 손실 보호를 무효화시킬 수 있습니다.

데이터 손실: 주머니 안 비즈니스

좋았던 시절을 기억하십니까? 데스크탑은 자체적으로 노출되기가 어렵습니다! 오늘날, 데이터는 장치끼리 이동할 때 취약합니다. 이동식 SD 카드와 USB 연결부가 있는 장치는 데이터가 암호화되어 있어도 데이터를 쉽게 손실할 수 있습니다. 불안정한 Wi-Fi 존으로 전송되는 데이터 또한 위험하며, 기업 데이터 손실 또는 피해는 막대한 벌금과 고객 신뢰 및 충성도 손실로 이어질 수 있습니다.

모바일 악성 프로그램: 우연적이든 고의적이든 관계없이 위험

모바일 앱 보안 상태 보고서에서[3], Arxan Technologies, Inc.는 최고 유료 Android 앱의 97%와 무료 유명 Android 앱의 80%가 일부 지점에서 해킹을 당했다고 발표했습니다. Android 사용자는 모든 앱스토어에서 앱을 설치할 수 있기 때문에 (Google Play로 국한되지 않음) 악성 프로그램, 악성 프로그램에 연결하도록 구성된 소셜 엔지니어링을 포함한 앱의 비율이 기타 모바일 운영 체제의 앱 대비 매우 높습니다. Arxan은 또한 점점 더 많은 회사에서 앱 중심 혁신으로 전환하고 더 많은 직원이 모바일 기술을 활용하면서 "파손된" 모바일 앱이 점차 퍼지고 있다는 점을 발견했습니다.

Google Play Store에서 무해한 것으로 간주되는 앱도 네트워크와 브랜드를 손상시켜 잠재적 수익 손실과 핵심 데이터에 대한 무단 액세스, 지적재산 (IP) 도난, 사기 및 사용자 경험 변화로 이어질 수 있습니다. 예를 들어 자녀가 귀하의 장치에서 유명 게임인 템플런을 다운로드할 경우, 해당 코드가 루트 파일시스템에 액세스할 수 있고 또는 캐시나 장치에 삽입한 SD 카드도 다운로드할 수 있습니다. 또한 장치의 마이크를 통해 음성을 바로 녹음하고 위치를 추적할 수도 있습니다. IBM® MaaS360® App Risk Management 제품을 활용해 템플런에 대한 이러한 (다소 충격적인) 모든 앱 보안 세부 정보를 확인할 수 있습니다.

이러한 취약성을 방지하려면 IT는 어떤 소프트웨어를 설치해야 하는지 알아야 하고 모바일 악성 프로그램과 루팅된 장치를 감지, 일부 블랙리스트화 수준을 수행하며 필요한 경우 준수 규칙을 실행해야 합니다.

Android 환경에서 EMM에 접근하는 방법

기업 또는 직원 소유 장치 여부에 관계없이 수많은 IT 부서에서는 한 개 이상의 장치 유형, 수많은 앱, 한 개 이상의 OS까지도 관리하고 있습니다.

EMM을 위한 모범 사례: 정밀한 환경 및 보안 정책에 맞도록 사용자 지정합니다.

IT는 여러 등급의 사용자, 부서, 지역, 장치 및 애플리케이션에 대한 이동성 관리 투자의 "올바른 범위"를 조정해야 하며 해당 사용 사례의 요구사항에 가장 적합한 기술 접근법을 적용해야 합니다. 예를 들어 영업사원은 고객 연락처에 액세스하고 데이터를 생산해야 하며, 인사부 (HR) 는 위반 시 책임져야 할 수도 있는 매우 민감한 데이터, 정보에 액세스해야 합니다. EMM은 일률적으로 적용되지 (one-size-fits-all) 않으며, 평등하지도 않습니다.

MaaS360은 Android 과자에 만족하도록 도움을 줄 수 있습니다

기술 미리 보기 파트너로서 IBM은 Google 및 삼성 등 제조업체와 긴밀하게 협력하여 고객이 Android를 최대한 활용할 수 있도록 도움을 줍니다. MaaS360은 삼성 KNOX 및 업무용 Android와 직접 통합합니다. MaaS360을 함께 사용하면 여러 플랫폼 전반에 걸쳐 다양한 장치를 관리하는 강력하고 결합된 경험을 할 수 있습니다.

Google, 장치 제조업체 및 MaaS360 기능을 함께 사용함으로써 IT는 계층화된 보안 프로그램을 구축, 관리 및 확장하는 광범위한 모바일 보안 옵션과 통합 플랫폼에 액세스합니다. MaaS360을 활용해 필요한 것을 바로 배치하고, 환경에서 원하는 특정 제어를 통해 모바일 세계를 보호하도록 도움을 주는 개별 솔루션을 선택합니다.

MaaS360	이것으로 무엇을 할 수 있습니까
IBM® MaaS360® Mobile Device Management 필요한 것을 지원하는 장치 수명 주기	• 요청 시 액세스 제어 및 특정 장치 또는 Android OS 버전 격리 • 지오펜싱（geofencing） 규칙 및 상황별 관리로 전송 중인 데이터 보호 • 루팅된 장치 감지 및 제한 • 잃어버리거나 도난 당한 장치의 원격 위치찾기, 잠금 및 지우기
IBM® MaaS360® Mobile Application Management 스마트한 모바일 엔터프라이즈 제공 방법	• 컨테이너화로 엔터프라이즈 앱 보호 • 웹 기반 콘솔로 모바일 앱을 중앙에서 관리 • 블랙리스트, 화이트리스트 및 필수 앱 설정으로 데이터 유출 및 네트워크 공격 중단
IBM® MaaS360® Productivity Suite 개인 수준에서 세계적 수준의 보호 제공	• 개인 및 기업 데이터 분리 • 사용자 수준에서 페르소나 정책 설정 • 온라인 및 오프라인 규정 준수 점검 가능 • 제품군 컨테이너, 앱 컨테이너, 엔터프라이즈 프로필 또는 전체 장치 지우기
IBM® MaaS360® Content Suite 통제와의 협업	• 문서 중앙 배포 또는 SharePoint, Windows File Share, IBM Connections, Box, Google Drive, CMIS 소스 등 기존 기업 파일 스토어에 대한 보호 액세스 제공 • 사용자가 Android 장치에서 모두 암호화된 컨테이너에서 안전하게 문서 보기, 생성, 편집 및 저장하도록 지원 • iOS, Android 및 Windows 장치 등 장치 유형 전반에 걸쳐 컨텐츠 동기화
IBM® MaaS360® Gateway Suite 입구 보호	• 장치 VPN 없이 회사 데이터 모바일 접속 보호 • SharePoint, Windows File Share, 귀사의 인트라넷 사이트 동원 • 엔터프라이즈 시스템에 앱 안의 VPN 터널 사용

MaaS360	이것으로 무엇을 할 수 있습니까
IBM® MaaS360® Mobile Threat Management 일어나기 전 공격 방지	• 지속적으로 업데이트되는 데이터베이스를 활용하여 악성 프로그램 서명이 있는 앱 감지 • 거의 실시간에 가까운 규정 준수 규칙 엔진으로 개선 자동화 • 루팅 장치 감지를 숨기는 은폐 기술 발견
MasS360 App Risk Management 앱에서 위험한 비즈니스 제거 지원	• 심층적인 자동 분석을 통해 수백 개의 코드 취약성 및 위험한 앱 동작 식별 • 사업 단위, 지역 또는 작업 그룹에 따라 배치되기 전 앱 규칙 설계 및 테스트 • 사용자 장치 및 기업 앱 스토어에서 앱 보안 정책 실행

Android는 공식적으로 기업을 위해 제공되므로 당사에 문의해 MaaS360으로 귀사가 Android에 대비할 수 있는 방법에 대해 알아보십시오. 기업 데이터를 보호하는 동시에 사용자에게 장치 상의 작업 정보에 대한 원활한 액세스를 제공하십시오. 광범위한 Android 장치 전반에 걸친 일관적인 경험을 위해 통합 정책, 위협 관리, 앱 배포, 장치 관리 및 표준 프레임워크를 활용하십시오. IBM MaaS360 30일 시험판의 즉각적인 무료 액세스는 다음 웹페이지를 방문하십시오. **ibm.com**/maas360.

IBM MaaS360 정보

IBM MaaS360은 엔터프라이즈 이동성 관리 플랫폼으로서 사람들의 업무 방식과 관련된 생산성 및 데이터 보호 기능을 제공합니다. MaaS360은 수천여 개의 조직들로부터 이동성 이니셔티브의 기반으로 인정받고 있습니다. MaaS360은 어떤 모바일 배포 과정이든 지원할 수 있도록 사용자, 장치, 앱 및 컨텐츠 측면에서 모두 강력한 보안 제어를 가능케 함으로써 종합적인 관리를 도와줍니다. IBM MaaS360에 대한 자세한 정보를 보고, 무료 30일 시험판을 시작하려면, 다음 웹페이지를 방문하십시오. www.ibm.com/maas360

IBM Security 정보

IBM의 보안 플랫폼은 조직에서 직원, 데이터, 애플리케이션 및 인프라를 총체적으로 보호할 수 있도록 도와주는 보안 인텔리전스를 제공합니다. IBM은 ID 및 액세스 관리, 보안 정보 및 이벤트 관리, 데이터베이스 보안, 애플리케이션 개발, 위험 관리, 엔드포인트 관리, 차세대 침입 보호 등을 위한 솔루션을 제시합니다. IBM은 전 세계 가장 광범위한 보안 연구 개발 및 인도 성과를 자랑하는 조직 중 하나입니다. 자세한 정보는 다음 웹사이트를 참조하십시오. www.ibm.com/security

1 "Worldwide Smartphone Shipments Edge Past 300 Million Units in the Second Quarter; Android and iOS Devices Account for 96% of the Global Market, According to IDC", IDC Worldwide Mobile Phone Tracker, August 14, 2014 (paywall,) http://www.businesswire.com/news/home/20140814005599/en Worldwide-Smartphone-Shipments-Edge-300-Million-Units

2 Ibid, 2014.

3 "State of Mobile App Security (Research), Apps Under Attack, Vol. 3 (previously titled: State of Security in the App Economy)", November 17, 2014, Arxan Technologies, Inc., https://www.arxan.com/wp-content/uploads/assets1/pdf/State_of_Mobile_App_Security_2014_final.pdf

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
2016년 3월

WGW03108-KRKO-01