IBM Global Technology Services
Thought Leadership 백서

2012년 11월

더 효과적인 모바일 엔터프라이즈 프로그램 개발

파트너와 함께 모바일 엔터프라이즈 프로그램을 개발하는 "방법(how-to)"을 소개하는 실용 가이드

IBM

모바일 디바이스가 빠르게 보급되고 회사 자원에 대한 즉각적인 액세스를 필요로 하는 글로벌 및 원격 인력이 늘어나면서 모바일 엔터프라이즈 프로그램이 절실히 필요해졌습니다. 이러한 프로그램은 직원과 다른 이해 관계자가 스마트폰, 태블릿과 같은 모바일 디바이스에서 엔터프라이즈 애플리케이션을 구현하고 회사 리소스에 액세스하도록 지원하는 인프라, 기술, 정책을 포괄합니다. 회사 소유 모바일 디바이스만 업무에 사용하도록 규정한 곳도 있지만, 직원이 개인 소유의 모바일 디바이스를 선택하여 구매하고 업무에 사용하는 것을 허용하는 "BYOD(bring-your-own-device)" 프로그램을 도입하는 기업이 늘고 있습니다.

모바일 엔터프라이즈 프로그램을 통해 기업의 직원, 파트너, 고객 모두를 위해 상당한 가치를 실현할 수 있습니다. 직원은 사실상 어디서든 24시간 언제라도 회사 자원에 액세스하면서 일할 수 있습니다. 회사 입장에서는 전반적인 생산성, 효율성, 경쟁 우위를 강화할 수 있는 기회가 됩니다. 그러나 모바일 엔터프라이즈 프로그램이 기업에게 중대한 과제를 부여할 수도 있습니다. 모바일 기술이 최근에 빠른 속도로 확산되었기 때문에 이렇다 할 베스트 프랙티스가 드문 편입니다. 따라서 모바일 엔터프라이즈 프로그램을 개발하려는 기업 중 상당수는 어떻게 또는 어디서 시작해야 하는지 모르고 있습니다. 자체적으로 프로그램을 개발하기로 결정한 경우 시간, 비용, 복잡성, 리스크의 측면에서 쉽지 않은 일임을 깨닫곤 합니다.

이 글은 전략에 기초하여 더 효과적인 모바일 엔터프라이즈 프로그램을 구현하는 "방법(how-to)"을 소개하는 실용 가이드로서 모바일 엔터프라이즈 파트너가 회사 소유 디바이스 또는 BYOD 모바일 엔터프라이즈 프로그램의 개발과 지원을 위해 어떤 강력한 기능을 제공할 수 있는지 자세히 살펴봅니다. 고객이 아닌 직원을 위한 모바일 엔터프라이즈 프로그램에 초점을 두고 있습니다.

소비자 주도의 IT

업무 환경에서 모바일 디바이스에 대한 수요가 확산되고 업무 환경 자체도 더욱 분산화됨에 따라 각 기업의 업무 환경에서 모바일 기술 사용의 지원은 필수 과제가 되었습니다. 최근 IBM이 전 세계 대기업의 CIO(chief information officer) 및 IT 관리자 675명을 대상으로 실시한 설문 조사에서 응답자의 74%는 향후 12개월간 유연한 워크플레이스 개발에 최우선적으로 투자할 것이라고 밝혔습니다.[1] 또한 응답자 대다수는 유연한 워크플레이스를 통해 생산성을 높일 수 있다고 확신하며, 절반 가량은 수익 향상으로 연결될 수 있다고 생각합니다.[2]

산업 분석 기관인 Gartner는 2014년이면 두 가지 이상의 모바일 디바이스를 사용하여 기업 시스템 및 데이터에 액세스하는 모바일 전문가가 (현재의 40%에서) 80%로 늘어날 것으로 예상합니다.[3] 업무 환경에서 모바일 디바이스를 사용하는 것이 하나의 트렌드에 머무르지 않고 기업이 받아들여야 할 새로운 현실로 자리 잡았습니다.

"'BYOD(bring your own device)' 프로그램이 부상하면서 PC[4]가 업무 환경에 등장한 이래 기업의 클라이언트 컴퓨팅에서 가장 큰 경제적 변화가 일어나고 있습니다. 어떤 기업이든 설령 BYOD를 허용하지 않더라도 그에 관한 명확한 입장을 정립해야 합니다."[5]

기업의 모바일 과제

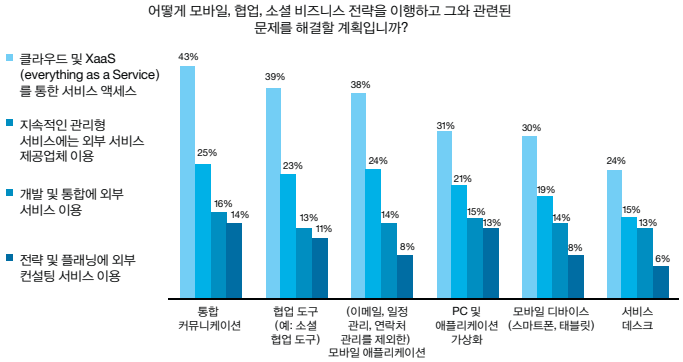
모바일 기술은 새롭고 끊임없이 변화하고 있으므로 기업에서 효과적인 모바일 전략을 구현하는 데 로드맵이 될 만한 베스트 프랙티스가 드문 편입니다. 따라서 어떻게 또는 어디서 시작해야 하는지 모르는 기업이 많습니다.

보안, 개인정보 보호, 사용 거버넌스 역시 중대한 문제입니다. 많은 모바일 디바이스에서 개인 데이터와 업무 데이터가 혼재하기 때문입니다. 실제로 설문에 참여한 CEO(chief executive officer)와 IT 관리자의 71%는 가장 중요한 모바일 엔터프라이즈 과제로 보안을 꼽았습니다.[6] 사실 이러한 우려에는

타당성이 있습니다. Ponemon Institute는 Symantec의 의뢰로 실시한 7차 연례 연구 조사의 결과 보고서에서 기업이 데이터 유출로 인해 부담하는 평균 비용이 550만 달러, 레코드당 194달러에 달한다고 밝혔습니다.[7]

같은 보고서에 따르면, 직원 또는 계약직의 모바일 디바이스를 분실하거나 도난당해 데이터 유출 사고가 일어난 적이 있는 기업이 39%에 달합니다. 여기에는 기밀 정보 및 중요 정보가 저장된 랩탑, 스마트폰, 태블릿, USB 드라이브도 포함됩니다. 또한 응답자의 37%는 악의적 또는 범죄 목적을 지닌 공격에 대해 우려하고, 24%는 IT 및 비즈니스 프로세스상의 오류가 복합적으로 작용한 것을 비롯한 시스템 차원의 문제를 지적했습니다.[8]

빠르게 발전하며 더욱 복잡해지는 모바일 세상을 무작정 탐색하다가 겪게 될지도 모르는, 심각한 상황을 감당할 수 있는 곳은 없습니다. 이런 이유로 많은 기업에서 고도의 기술력을 가진 전문가의 도움을 구하곤 합니다. 즉 리스크를 완화하고 지속 가능한 모바일 엔터프라이즈 프로그램을 구현하는 데 필요한 자원과 기술을 제공할 수 있는 파트너를 찾습니다. 모바일 엔터프라이즈 파트너는 다양한 업종의 여러 기업이 성공적인 모바일 엔터프라이즈 전략을 수립하도록 지원하면서 축적한 베스트 프랙티스에 관한 지식을 전수할 수도 있습니다.



기준: 전 세계의 IT 의사결정권자 80명
출처: IBM이 Forrester Consulting에 의뢰하여 실시한 조사, 2012년 5월

모바일 엔터프라이즈의 개발, 관리, 지원 "방법(How-to)"에 관한 지침

다음 4단계를 통해 효과적이고 지속 가능한 모바일 엔터프라이즈 프로그램을 구현할 수 있습니다.

1. **모바일 전략 정의:** 모바일 목표를 명확히 하고 지원할 프로그램 유형(BYOD 또는 회사 소유 디바이스)을 결정하고 비용과 관련하여 고려할 사항을 평가합니다.

2. **모바일 엔터프라이즈 프로그램 구현:** 모바일 엔터프라이즈 프로그램을 구축하고 이를 지원하도록 엔터프라이즈 네트워크를 준비하는 데 어떤 도구를 활용할지 결정합니다.

3. **모바일 디바이스 보호 및 관리:** 네트워크에 연결된 모바일 디바이스를 보호하는 데 도움이 될 기술을 선택하고 모바일 보안 정책을 수립합니다.

4. **지원:** 지속적으로 모바일 디바이스의 장애 해결을 지원합니다.

아래에서 각 단계를 자세히 살펴보겠습니다.

1단계: 모바일 전략 개발

모바일 엔터프라이즈 프로그램을 마련하는 데 가장 중요한 단계 중 하나가 업무 환경에서 어떻게 모바일 개발 및 구현을 결정할 것인지 좌우할 모바일 전략의 수립입니다. 이와 같은 전략은 고객의 필요, 기대, 목표를 명확하게 정의하는 것에서 출발해야 합니다.

다음과 같은 질문에 답할 필요가 있습니다.

- 왜 모바일 엔터프라이즈 프로그램을 구현하려 합니까? 궁극적인 비전이 무엇입니까? 어떤 혜택을 기대합니까?

- 모바일 엔터프라이즈 프로그램의 비용과 관련하여 무엇을 고려해야 합니까? 고객의 상황에서 부담할 비용이 기대할 수 있는 혜택보다 큽니까?
- 회사가 모바일 디바이스를 소유합니까? 아니면 직원이 각자의 디바이스를 구입하여 사용하게 할 것입니까? 회사에서 비용을 보조할 경우 얼마나 지원할 것입니까?
- 맞춤형 모바일 애플리케이션을 개발하거나 모바일 애플리케이션의 개발을 아웃소싱하거나 미리 패키지화된 모바일 애플리케이션을 도입할 계획입니까?

모바일 엔터프라이즈 프로그램의 혜택: 모바일 엔터프라이즈 프로그램은 다양한 혜택을 제공하지만, 대표적인 것을 간추려 소개하면 다음과 같습니다.

- 직원 만족도 향상 - 직원들이 모바일 디바이스, 특히 자신이 선택한 디바이스와 플랫폼으로 일하는 것을 좋아합니다. 또한 어디서든 자신에게 편리한 방식으로 일할 수 있다는 유연성도 만족스러운 점입니다.
- 더 손쉽게 직원 채용 및 인재 기반 보호 – 직원들은 업무 환경에서 모바일 기술을 지원하는 기업에서 일하는 것을 선호합니다.
- 생산성 향상 - 사실상 언제 어디서든 일하는 것이 가능하므로 사무실 안팎에서 더 많은 성과를 거두게 됩니다. 뿐만 아니라 맞춤형 모바일 애플리케이션을 개발하여 더 새롭고 혁신적인 업무 방식을 도입할 수 있습니다.
- 고객 관계 향상 - 전문적인 모바일 애플리케이션(앱)을 활용하여 모바일 디바이스를 통해 제품을 판매하고 영업 팀에게는 실시간으로 고객 데이터를 제공할 수 있습니다. 이와 같이 강력한 기능은 고객의 "감정"을 모니터링하고 더욱 신속하게 고객의 필요와 요구에 대응하고 더 우수한 서비스를 제공하는 데 큰 도움이 됩니다.

비용과 관련된 일반적인 고려 사항: 고객들은 매우 다양한 차원에서 비용 절감 효과를 거뒀다고 밝힙니다. 여기에는 소프트웨어, 인프라(회사 소유 디바이스 모델을 선택한 경우 모바일 디바이스도 포함), 인력 또는 관련 지원 서비스, 애플리케이션 개발, 만일의 네트워크 업그레이드에 대한 투자의 측면이 포함됩니다. 소프트웨어 라이센스 요금, 회사의 모바일 디바이스 요금 지원, 해외 사용 요금, 세금, 보험, 기타 소프트 비용 등 잘 드러나지 않는 요소도 고려해야 합니다. 물론 모바일 엔터프라이즈 프로그램의 혜택 중 상당수, 이를테면 생산성 향상, 워크플레이스 혁신, 시간 절약, 직원 만족도 등은 측정 불가한 지표입니다. 그리고 모바일 엔터프라이즈 서비스를 외주하는 기업이 상당한 절감 효과를 거두는 경우도 많습니다.

CIO들은 유연한 워크플레이스 서비스를 아웃소싱함으로써 20%의 생산성 향상 및 비용 절감 효과를 거뒀다고 밝힙니다.[9]

BYOD 아니면 회사 소유 디바이스: 모바일 엔터프라이즈 프로그램의 비용은 구현하려는 프로그램의 유형과도 관련됩니다.

예를 들어, BYOD 프로그램의 비용 및 복잡성 부담이 더 클 수 있는데, 모바일 디바이스에 업무 데이터와 개인 데이터가 섞여 있고 개인용 디바이스를 안전하게 지키는 데 더 복잡한 기능이 필요하기 때문입니다. Aberdeen Group의 분석을 따르면, BYOD 모바일 디바이스 1,000대를 보유한 기업은 중앙에서 구매하고 회사에서 디바이스를 소유하는 정책을 선택한 기업보다 연평균 17만 달러를 더 지출합니다. 추적하기 쉽지 않은, BYOD에서 추가로 부담할 비용에는 다음 항목이 포함됩니다.

- 할부 통신 요금
- 직원 요금 지원을 위해 제출된 추가 비용 보고서
- IT 팀에서 직원 소유 디바이스의 업무 데이터를 관리하고 보호해야 하는 추가적인 부담
- 일반적으로 모바일 지원을 맡지 않는 다른 운영 그룹의 업무량 증가
- 궁극적으로 모바일 환경의 복잡성 심화 및 그에 따른 지원 비용 증가[10]

관리 통제 및 편의성 역시 고려할 점입니다. 회사에서 모바일 디바이스를 선택, 소유, 관리한다면 더 수월하게 보호하고 회사의 정책 준수를 관리할 수 있습니다. 업무용 데이터 및 애플리케이션을 제공할 인프라를 회사에서 구축할 수 있기 때문입니다. 하지만 이와 같은 통제로 인해 사용자의 만족도가 저하될 수 있습니다. 많은 직원들이 자신이 소유한 디바이스로 일하는 것을 확실히 선호하기 때문입니다. 회사 소유 디바이스 모델이 폭넓은 지지를 받으려면 직원들로부터 사용하고 싶은 디바이스 및 애플리케이션 유형에 대한 의견을 수렴해야 합니다. 직원들은 자신이 프로그램 개발에 일조했다면 그 프로그램의 한계를 더 기꺼이 수용할 것입니다. 또한 회사에서 모바일 디바이스를 지급할 경우 직원들은 회사에서 높은 수준의 일반 사용자 지원을 제공할 것으로 기대합니다. 따라서 이 새로운 요구사항을 해결할 적정 인력과 사내 전문성을 확보해야 합니다.

전략적 고려사항 - 모바일 엔터프라이즈 파트너의 역할: 모바일 엔터프라이즈 파트너는 모바일 기술이 해당 기업의 직원, 고객, 비즈니스 전반에 어떤 이점을 제공할 것인지 평가하도록 지원합니다. 요구사항과 목표를 명확히 하고 우선순위를 정하며 유무형의 ROI(투자 수익률)를 평가하고 프로그램 구현을 위한 단계별 로드맵을 개발할 수 있도록 전략과 컨설팅을 제공하기도 합니다. 통신 비용 관리 서비스를 통해 모바일 지출을 최적화하고 더 효과적으로 관리하도록 도울 수도 있습니다. 또한 파트너를 이용하면 독자적으로 시작하는 것과 달리 연구조사 및 물류의 부담이 사라지므로 더 일찍 프로그램을 가동할 수 있습니다.

2단계: 모바일 프로그램 구현

프로그램 목표를 명확히 세웠으면 이를 기술적으로 구현할 방법을 평가할 차례입니다.

다음과 같은 질문에 답할 필요가 있습니다.

- 어떤 디바이스를 지원합니까(전화, 태블릿, 랩탑)? 각종 디바이스와 운영 체제를 지원하면 어떤 장단점이 있습니까? 이 분석 결과와 일반 사용자의 선호도에 따르면 어떤 디바이스와 모바일 운영 체제를 지원할 것입니까?
- 일반 사용자에게 어떤 데이터 및 애플리케이션에 대한 액세스를 허용해야 합니까? 그리고 전체 액세스 권한 또는 제한적인 액세스 권한을 부여합니까?
- 어떤 서비스를 지원합니까?
- 가장 우선적인 모바일 요구사항을 가진 직원과 이해 당사자는 누구입니까? 이 사용자에 한해 모바일 엔터프라이즈를 도입합니까? 아니면 모든 사용자가 액세스할 수 있도록 확장합니까?

- 어떤 모바일 디바이스 사용 시나리오에서 특별 모바일 애플리케이션의 개발이 가능합니까?
- 전략적 사업장에 한하여 모바일 엔터프라이즈 프로그램을 도입합니까? 아니면 전 세계의 여러 사업장을 지원할 수 있도록 전사적 차원의 프로그램으로 실시합니까?
- 엔터프라이즈 시스템과 모바일 시스템은 어느 정도까지 통합해야 합니까?
- 성공적인 모바일 엔터프라이즈 프로그램을 위해 네트워크에서 최적의 성능을 지원하려면 어떻게 합니까?

지원할 디바이스 결정: 새로 출시되는 모든 태블릿과 스마트폰을 안전하게, 물류 차원에서 지원하는 것은 거의 불가능합니다. 특정 디바이스와 운영 체제를 지원하고 모바일 정책에서 이 디바이스를 (지원하는 이유에 대한 설명과 함께) 정의하는 것이 더 효과적인 방법입니다. 이 주제는 이 글에서 다시 자세히 살펴보겠습니다. 원칙적으로는 모바일 디바이스의 현재 용도와 원하는 용도, 직원의 선호 사항에 대한 인식에 기초하여 결정해야 합니다.

그러나 대체로 더 많은 플랫폼을 지원하면 복잡성이 가중됩니다. 따라서 복잡성을 줄이는 가장 쉬운 방법은 지원하는 디바이스 및 플랫폼의 수를 제한하는 것입니다. 그러나 RIM(Research in Motion) BlackBerry, Apple iOS, Android, Windows 등 다양한 플랫폼의 장단점을 반드시 고려해야 합니다. 그리고 장점을 살펴볼 때 보안의 관점에서 가장 합당한 것과 그렇지 않은 것을 식별하여 우선순위를 정하십시오. BlackBerry 전화기는 강력한 보안이 구현된 설계 때문에 많은 기업에서 이 기종의 사용을 지원합니다. 그리고 iOS 및 Android 플랫폼은 상대적으로 높은 수준의 보안을 지원할 수 있으나 구 버전의 Microsoft Windows와 Android는 지원하지 않을 수도 있습니다. 보안, 앱 호환성, 서비스 데스크의 부담을 고려할 때 운영 체제(OS) 플랫폼 및 버전의 수를 제한하는 것이 좋습니다. 그리고 프로그램 및 보안 인프라도 시간이 흐르면서 계속 발전하므로 점차적으로 디바이스 및 플랫폼 지원을 확대할 수 있습니다.

모바일 액세스를 지원할 데이터 및 애플리케이션 선택: 지원할 디바이스와 운영 체제의 범위를 한정했다면 특정 직원이 액세스할 수 있는 데이터와 애플리케이션을 결정해야 합니다. 이를테면 의료 기관에서는 간호사 및 의사의 모바일 액세스 권한과 관리자의 액세스 권한을 다르게 지정해야 할 수 있습니다. 전담 팀을 두고 직원들로부터 정보를 수집하여 업무 환경에서 실제로 필요한 모바일 기술과 사용자가 필요하다고 여기는 기술을 통찰력 있게 파악하는 일을 맡기는 것이 좋습니다. 이렇게 수집한 정보를 참조하여 전사적 범위에서 특정 비즈니스 프로세스에 대한 브레인스토밍을 효과적으로 진행할 수 있습니다. 즉 모바일 디바이스에서 특정 데이터, 기존 또는 맞춤형 애플리케이션에 액세스하는 방법으로 활성화할 수 있습니다. 그리고 복잡성을 줄이기 위해 어떤 사용자가 모바일을 통해 이 기업 자원에 액세스할지 결정하는 우선순위를 정합니다. 물론 액세스 범위를 (전 직원이 아니라) 우선순위가 높은 사용자로 제한하는 "시험 단계"를 거쳐 상황을 파악해야 합니다.

이메일 및 일정 관리 애플리케이션부터 시작하는 것이 일반적이고 더 편리합니다. 직원들이 이미 모바일 디바이스에서 이메일과 일정 관리에 액세스하고 있다면 사용되는 디바이스 및 플랫폼을 인벤토리화함으로써 모바일 엔터프라이즈 프로그램을 업데이트하거나 확장하기 전에 보안 컴플라이언스를 점검할 수 있게 하는 것이 좋습니다. BYOD 프로그램을 시작하고 있다면 모바일 메시징 미들웨어에 제한적인 기능이 있음을 염두에 두십시오(8-9페이지의 "디바이스 지우기 및 잠금" 참조).

직원 서비스 활성화: 모바일 디바이스에서 애플리케이션뿐 아니라 특정 서비스도 사용 가능하게 선택할 수 있습니다. 여기에는 소셜 비즈니스 기능, 이를테면 인스턴트 메시징, ERM(enterprise-risk management), CRM(customer-relationship management), 영업, 재무, 인사(HR) 데이터 액세스 시스템 등이

포함될 수 있습니다. 이와 같은 서비스에 대한 액세스를 허용하는 순서, 즉 우선순위를 정하십시오. 업무 환경에서 모바일 기술을 지원하기 시작하면 직원들이 다양한 기능을 원하게 될 것입니다.

네트워크 준비: 모바일 엔터프라이즈 프로그램을 계획할 때 효율적인 네트워크 관리를 간과하기 쉽지만, 이는 모바일 이니셔티브의 성패를 좌우할 수도 있습니다. 일반적으로 더 많은 디바이스와 방대한 데이터를 지원하는 확장형 네트워크에서는 대역폭을 늘리고 보다 강력한 네트워크 관리 기능을 갖춰야 합니다. 따라서 구성 변경을 자동화하고 성능을 분석하고 보안을 관리하고 그 밖의 다양한 관리 기능을 제공하고 대규모의 확장성을 지원하는 솔루션(예: 클라우드 기반 또는 가상화된 네트워크 도구)이 필요합니다.

가동 시간도 중요한 문제입니다. 네트워크가 확장되면 오류 및 보안 리스크가 발생할 가능성도 높아집니다. 이와 같이 리스크가 증가하면 안정적이고 효과적으로 이벤트를 관리하고 근본 원인을 분석하고 변경 및 구성을 관리하고 성능을 보고하고 엔드포인트를 관리하는 기능이 절실히 필요해집니다.

관리 가능한 단계별 모바일 전략 구현 방식

모바일 엔터프라이즈 프로그램을 개발할 때, 모바일 엔터프라이즈 파트너와 함께하더라도 한꺼번에 모든 것을 해결하려 하지 마십시오. 더 폭넓은 관점을 유지하면서 목표를 향해 각각의 작은 단계를 점진적으로 수행하십시오. 그러면 더 복잡한 이니셔티브로 진행하기에 앞서 문제에 직면하더라도 이를 다루고 해결할 수 있습니다.
몇 개월 또는 그보다 오랜 기간에 구현할 수 있는 모바일 엔터프라이즈 프로그램의 예를 소개합니다.

1. 이메일, 일정 관리, 기타 모바일 애플리케이션에 액세스하는 기존 디바이스 관리: 인프라 관리 도구 또는 MDM 소프트웨어를 사용하여 네트워크에 액세스하는 모바일 디바이스의 숫자를 인벤토리화합니다. 그리고 각 디바이스에서 네트워크에 액세스하는 방식(예: VPN, Wi-Fi)과 이 디바이스에서 액세스할 수 있는 데이터 및 애플리케이션에 특히 주의를 기울입니다. 가능하다면 디바이스의 보안 상태(인증 절차, 애플리케이션 보안 포함)도 확인해야 합니다. MDM 또는 보고 도구가 없어 이러한 정보를 얻을 수 없다면 기한을 정해 기존의 모바일 액세스 사용을 일시 중단하고 더 새롭고 엄격한 정책과 절차를 지원할 기술적 기능을 갖춘 다음 직원들에게 이 정책과 절차를 발표하는 방법도 있습니다.
2. 모든 직원을 대상으로 관리형 액세스 확대: 직원 대부분은 적어도 회사 이메일 및 일정 관리 애플리케이션에 대한 액세스를 원할 것입니다. 이 기능을 확장하여 모든 직원에게 제공한다면 만족도를 높일 뿐 아니라 전사적 차원의 모바일 기능 구현과 관련된 물류적 측면을 더 명확하게 이해할 수 있습니다. 이러한 통찰을 통해 다른 데이터와 애플리케이션에도 전사적 범위의 모바일 액세스를 지원할지 여부를 결정할 수 있습니다.
3. 디바이스의 컨텐츠 저장 및 동기화 보호: 네트워크 기반 데이터 스토리지만 허용함으로써 디바이스 분실 또는 도난 시 위험을 야기할 로컬 복사본 저장을 차단할 수 있습니다. 저장된 컨텐츠를 확실하게 보호하기 위해 암호화, 컨테이너화와 같은 방법을 선택할 수도 있습니다.
4. 회사에서 사용하는 기존 소프트웨어용 COTS(commercial off-the-shelf) 모바일 앱 인벤토리화 및 우선순위 지정: 그러면 모바일 액세스로 직원의 업무 생산성을 높이는 데 필요한 기능을 제공할 수 있습니다.
5. 필요에 따라 맞춤형 앱 개발 또는 외주 제작: 어떤 서비스 및 프로세스에서 맞춤형 애플리케이션의 개발이 필요할지 고려하고 모바일 우선순위에 따라 개발합니다.
6. 보안 인프라가 제대로 갖춰진 상태에서 모바일 애플리케이션 구축: 모바일 액세스를 허용하는 업무용 애플리케이션은 적어도 모바일 액세스가 허용되지 않은 애플리케이션의 보안 수준에 부합해야 합니다. 이 보안 기준에 부합하는 애플리케이션을 구축할 수 없다면 더 신뢰할 수 있는 모바일 애플리케이션으로 구축 범위를 한정하십시오.

3단계: 보안 관리

모바일 엔터프라이즈 프로그램의 개발 및 관리에 사용할 기술을 결정했다면 네트워크에 연결된 모든 모바일 디바이스를 보호하기 위한 계획을 마련해야 합니다.

다음과 같은 질문에 답할 필요가 있습니다.

- 어떻게 하면 디바이스, 애플리케이션, 데이터 액세스의 보안을 더 효과적으로 관리할 수 있습니까?
- 직원이 퇴사할 때 또는 디바이스를 분실하거나 도난 당했을 때 어떻게 데이터를 관리합니까?
- 어떻게 하면 일반적인 위협 요소(바이러스, 맬웨어, 공격 등)로부터 모바일 디바이스를 더 안전하게 지킬 수 있습니까?
- 최소한 유지해야 할 보안 수준은 무엇이며, 현재 기업 문화의 조건에서 어떻게 이를 구현할 수 있습니까?
- 어떻게 하면 더 안전하게 모바일 디바이스와 기업 애플리케이션을 배포하고 온보딩 및 도입 프로세스를 관리할 수 있습니까?
- 모바일 보안 정책에 무엇을 포함해야 하며, 어떻게 하면 더 효과적으로 개인정보 보호법을 준수할 수 있습니까?

모바일 보안이 여전히 기업의 최우선 관심사이지만 모바일 디바이스에서 데이터를 보호할 여러 가지 방법이 있습니다. 회사에서 지원할 모바일 디바이스 및 최소한 지켜야 할 보안 수준을 결정했다면, 더 안전하게 모바일 엔터프라이즈를 지원하는 데 사용할 도구를 훨씬 수월하게 선택할 수 있습니다.

다음을 비롯하여 다양한 자원 및 보안 방식 중에서 선택할 수 있습니다.

모바일 디바이스 관리(mobile device management, MDM): 사내에서 또는 클라우드 기반 서비스를 통해 운영하는 디바이스와 서버에 소프트웨어 에이전트를 설치하고 이를 통해 디바이스를 모니터링하는 기존의 IT 방식입니다. MDM은 보고하거나 확인해야 하는 모든 디바이스에 효과적입니다. 뿐만 아니라 전사적 범위에서 OTA(over the air) 방식으로 기업 애플리케이션을 구축, 관리하고 배포하는 것도 지원할 수 있습니다. MDM에서는 사용자가 설치한 애플리케이션을 확인하고 제한된 애플리케이션에 대한 액세스를 차단하고 새로운 애플리케이션 또는 업데이트를 제안하는 것도 가능합니다. 다양한 셀프 서비스 사용자 포털을 제공하여 직원이 패스코드를 재설정하고 디바이스를 잠그고 분실했거나 도난 당한 디바이스의 전체 또는 일부를 원격으로 지우는 것을 지원하는 경우도 있습니다. 자체적으로 MDM을 구현할 경우 설비 투자의 부담이 커질 수 있습니다. 하지만 SaaS(software as a service) 클라우드 기반 시스템은 더 신속하게 설정하고 편리하게 업데이트할 수 있으며 더 경제적입니다.

그러나 MDM 솔루션을 구성할 때 기업 문화의 관점에서 특히 개인용 디바이스와 관련하여 무엇이 허용되는지 고려하십시오. 예를 들어, Android 전화기에 에이전트를 설치하여 상세한 소프트웨어 인벤토리를 관리하고 카메라 기능을 끄고 GPS(global positioning system) 위치를 추적하고 전화기의 부분 또는 전체 지우기를 수행하는 것이 가능할 수 있습니다. 하지만 기업 문화가 이를 지원합니까? 아니면 사생활 침해로 간주합니까?

컨테이너화: 일부 MDM 프로그램에 포함된 컨테이너화(containerization) 기능은 암호화 및 기타 방법을 통해 모바일 디바이스에서 업무용 데이터와 개인 데이터를 구분합니다. 이는 BYOD 프로그램에 적합하고 효과적인 방법입니다. 비용 절감 및 벤더 관리 차원에서 MDM과 컨테이너화 기능을 결합하는 곳도 있겠지만, 복잡성을 줄이려면 컨테이너화와 MDM을 분리하는 것이 좋습니다.

디바이스 지우기 및 잠금: 모바일 디바이스 보안의 최대 장애물 중 하나는 디바이스 자체의 모바일 속성입니다. 휴대 가능한 크기 때문에 분실하기 쉽습니다. 그리고 이동하면서 사용하기 때문에 중요한 업무용 데이터를 보호하기 위한 추적 및 관리 메커니즘이 꼭 필요합니다. 비밀번호 입력 오류가 일정 횟수를 초과하면 모바일 디바이스의 모든 데이터를 지우거나 삭제하는 기능을

통해 brute-force 공격의 위험을 줄일 수 있습니다. 또한 디바이스를 분실했거나 도난당한 경우 또는 직원의 퇴사 또는 인사이동이 있을 경우 일반 사용자나 관리자가 "로컬 지우기"를 수행하는 것이 바람직합니다. 일정 기간 사용되지 않은 디바이스를 잠그는 것도 보안 위험을 줄이는 데 도움이 됩니다.

BYOD 프로그램을 시작한 지 얼마 되지 않았고 개인 소유 디바이스에 MDM 에이전트를 설치하는 것을 원치 않는 경우, 모바일 메시징 미들웨어가 부분 지우기 또는 데이터 분리를 지원하지 않는다는 점을 기억할 필요가 있습니다.

암호화 및 데이터 스토리지 대안: 모바일 디바이스의 데이터를 암호화함으로써 보안 수준을 한층 더 강화할 수 있습니다. 가장 보편적인 방법 중 하나인 하드웨어 기반 암호화는 장치에 기본적으로 구현되고 성능 향상의 이점을 제공할 수도 있으므로 소프트웨어 암호화보다 유리합니다.

브라우저 및 가상화된 애플리케이션은 모바일 장치에 데이터를 저장하는 것의 대안이 될 수 있습니다. 즉 실제로 장치에 저장되는 데이터는 거의 없으며, 필요에 따라 요청 받아 표시되므로 데이터 손실의 위험이 줄어듭니다. 그러나 네트워크 액세스가 필요하기 때문에 오프라인 상태 또는 연결이 끊어진 상태에서는 사용자가 데이터에 액세스할 수 없습니다. 그리고 리치 클라이언트에서 모바일 디바이스의 로컬 데이터에 액세스하는 경우에 비해 성능이 낮거나 일반 사용자의 응답 시간이 길어질 수 있습니다.

사용자 기반 인증 및 사기 방지: 디바이스에 로그온한 다음 회사 네트워크에 로그온하는 2단계 사용자 기반 인증을 최소 기본 요구사항으로 설정하여 누가 업무용 데이터 및 애플리케이션에 액세스하는지 모니터링하고 제어할 수 있습니다.

디바이스에 로그인하는 데 표준 숫자 또는 영숫자 패스코드를 입력하고 네트워크 액세스에는 고급 인증 방식(예: 스마트 카드, 디지털 인증서, 토큰)을 사용하는 것이 가능합니다.

일부 디바이스에서는 패스코드만 지원하지만 BlackBerry는 스마트 카드도 지원합니다. 고급 보안 기능을 모바일 애플리케이션에 통합하는 방법도 있습니다. 예를 들어, 특히 민감한 데이터 및 애플리케이션에 대한 액세스에는 추가적인 인증 절차를 적용할 수 있습니다. 이를테면 성문 분석과 같은 생체 인식 표시 장치를 사용하여 등록된 정보와 비교합니다. 다층적 인증 방식은 보안 사고를 줄일 수 있는 효과적인 방법 중 하나입니다.

회사 인트라넷에 대한 가상 사설망(VPN) 액세스를 허용할 계획이라면 액세스 가능한 IP(Internet Protocol) 주소를 제어하는 기능도 포함하십시오.

그러나 이 모든 방식은 구현하는 데 상당한 비용이 들고 복잡합니다. 따라서 적용할 인증 및 사기 방지 방식을 결정할 때 비용과 사용 편의성을 균형적으로 고려하는 것이 중요합니다.

모바일 위협 관리: 어떤 모바일 디바이스도 맬웨어에 감염될 가능성이 있습니다. 이와 같은 맬웨어를 줄이려면 데스크탑 및 랩탑 환경과 비슷한 수준의 보호 기능을 구현해야 합니다. 그러기 위해서는 모든 고객이 맬웨어 방지 소프트웨어를 설치하고 자동으로 실행하며 정기적으로 실시간 검사를 실시할 필요가 있습니다. 사전 예방 차원에서 직원에게 신뢰할 수 있는 애플리케이션만 다운로드하여 설치하고 의심스러운

애플리케이션이 발견되면 바이러스 검사와 같은 알맞은 조치를 취하도록 조언해야 합니다. 또한 맞춤형 앱 스토어를 구축하여 공식적으로 검증되고 지원되는 업무용 및 비업무용 애플리케이션만 다운로드할 수 있게 하면 네트워크의 맬웨어를 줄이는 데 효과적입니다.

모바일 보안 정책: 법적 책임 및 보안 위협으로부터 회사를 보호하기 위해 정책을 마련하고 시행하는 것도 중요합니다. 회사 법률 고문 및 모바일 보안 조치의 기술적 세부 사항을 잘 아는 IT 팀이나 모바일 엔터프라이즈 파트너의 도움을 받아 모바일 보안 정책을 수립합니다. 모바일 보안 정책은 다음과 같은 핵심 사항을 포함해야 합니다.

- 지원할 모바일 디바이스(회사 소유 디바이스 및 개인용 디바이스 포함), 제공할 일반 사용자 지원의 수준, 지원을 이용하는 방법. 특정 플랫폼을 지원하는 이유를 밝힐 수도 있습니다. 예를 들어, 암호화가 가능한 플랫폼만 지원하기로 선택하면 일부 디바이스는 제외될 것입니다.
- 모든 주요 용어의 정의 - 모바일 디바이스, 모바일 디바이스 관리와 같은 기본 용어 포함
- 특정 데이터 및 애플리케이션에 대한 액세스 권한을 갖는 사용자
- 회사에서 모니터링하고 추적할 데이터 및 활동 - 회사 소유 디바이스와 개인용 디바이스를 구분합니다. 여기에는 문자 메시지, 이메일, 인터넷 탐색, 다운로드, GPS 추적, 인스턴트 메시징, 멀티미디어 파일 저장 등이 포함될 수 있습니다.
- 회사 소유 디바이스와 개인 소유 디바이스에서 모니터링하고 추적한 정보를 어떻게 사용하거나 사용하지 않을 것인지 상세히 밝히는 개인정보 보호정책
- 일반 사용자가 회사의 사용 정책을 위반할 경우 회사 차원에서 취할 구체적 조치
- 디바이스 분실 또는 도난 시 또는 직원의 퇴사 또는 인사이동 시 회사 차원에서 취할 명확한 방어 조치(예: 원격 지우기)

직원과 상사가 정책 동의서에 서명해야 합니다. 공식적인 모바일 보안 정책을 마련했으면 반드시 전사적으로 발표하고 정책 변경 시 업데이트된 내용을 배포해야 합니다. 또한 뉴스레터, 회사 소셜 네트워크, 인트라넷에 모바일 보안 정책을 공지하십시오.

Gartner의 모바일 보안 정책 스타일 가이드라인[11]

- 정책 문서는 간략하게, 몇 페이지 이하로 작성하십시오.
- "해야 한다", "할 수 있다"와 같은 지시형 표현에 알맞은 문구를 사용해야 합니다. 표준은 반드시 따라야 할 지침입니다. 가이드라인은 고려할 제안 사항입니다. 어떤 표준 또는 가이드라인이 적용 가능하거나 적용 불가할 때 질문과 결정 기준이 표시되게 설정합니다.
- 상세한 프로세스 설명 및 튜토리얼 해설은 문서의 본문보다는 부록 또는 외부 문서에 수록합니다.
- 다른 문서, 특히 다른 사람이 관리하는 문서의 내용을 그대로 싣지 마십시오. 외부 문서의 인용임을 명확히 표시합니다. 해당 문서의 저자들과 커뮤니케이션할 수 있는 채널을 확보합니다.
- "항상 이러하다. 다만..."과 같은 모호한 조건문, "이러하지 않다면 달라질 것"과 같은 부정적 시험이 중첩된 문장은 삼갑니다. 명확하게 규정되는 긍정적 조건문으로 시작합니다.
- 조건이 온전히 절대적인 경우에만 ("항상"과 같은) 절대적 문장을 사용합니다.
- 약어는 처음 나왔을 때 한 번만 풀어씁니다.
- 반복적으로 사용되는 약어를 포함한 용어 해설을 문서의 마지막에 넣습니다.

간과할 수 없는 일반 사용자의 만족도: 보안 정책을 정의할 때 사용자 경험의 품질을 염두에 두십시오. 이를테면 모바일 디바이스에서 데스크탑 디바이스와 다른 애플리케이션이 요구될 경우 프로그램의 성공에 지장을 줄 수 있습니다. 애플리케이션의 구속적 특성도 프로그램이 널리 보급되는 데 불리하게 작용합니다. 뿐만 아니라 직원들은 디바이스에서 컴플라이언스 미준수 문제가 발생할 때 자동으로 경보가 발효되고 직접 문제를 해결할 수 있도록 지침이 제공되기를 기대합니다. 정기적으로 보안 컴플라이언스 정책을 전달하면서 그러한 지침을 제공하십시오.

4단계: 일상적인 지원

정기적으로 모바일 디바이스의 보안을 관리하고 일반 사용자를 지원해야 합니다.

다음과 같은 질문에 답할 필요가 있습니다.

- 회사 소유 또는 개인 소유 디바이스에 어느 수준의 관리와 지원을 제공할 수 있습니까?
- 사내에 구현 및 지원을 위한 적정 자원을 보유하고 있습니까? 아니면 외부의 도움을 받아야 합니까?

지원 인력 확보: MDM 도구와 보안 관리 소프트웨어를 사용하여 네트워크에 연결된 모바일 디바이스의 활동을 추적하고 모니터링할 수 있습니다. 그러나 이러한 기능을 지원하고 지속적으로 모바일 기술로 인한 위협 요소로부터 네트워크를 보호할 수 있도록 도와줄 인력이 필요합니다.

또한 모바일 엔터프라이즈 프로그램은 일반 사용자를 위해서도 일정 수준의 지원을 제공해야 합니다. 모바일 엔터프라이즈 프로그램이 시작하면 디바이스-직원의 양적 비율이 순식간에 증가하기 때문에 이 새로운 수요를 뒷받침할 인력과 예산이 필요합니다. 또한 담당 팀은 일반 사용자의 새로운 지원 요청을 관리할 수 있도록 수준 높은 모바일 기술 전문성을 갖춰야 합니다.

지원-제공 방식: 지원을 제공할 방식에 관한 접근 모델을 설계해야 합니다. 어떤 기업에서는 일정 시간(대개 30분 ~ 1시간)을 할애하여 모바일 디바이스 문제를 다룹니다. 모바일 디바이스 자체가 아니라 네트워크 관련 문제만 지원하기로 결정하는 곳도 있습니다. 또는 일반 사용자가 지원 문제와 관련된 경험을 나눌 수 있도록 메일링 리스트, 웹 포털, 위키까지 제작하는 기업도 있습니다. 예를 들어, 어떤 사용자가 디바이스에서 Microsoft ActiveSync를 구성하는 것에 관한 질문을 올리면 다른 직원이 여기에 답하는 것입니다. 일반 사용자가 디바이스 분실 또는 손상 시 디바이스를 교체해주거나 보조해주는 보험에 가입하는 것을 의무화하는 방법도 있습니다. 이 경우 회사의 모바일 정책에서 이용 가능한 보험사 및 보험료를 지정해야 합니다.

구현, 보안, 지원 – 모바일 엔터프라이즈 파트너의 지원: 모바일 엔터프라이즈 파트너는 자체 제작 솔루션보다 빠르고 경제적으로 모바일 엔터프라이즈 프로그램을 구현하고 관리하도록 필요한 역량, 기술, 교육, 지원을 제공할 수 있습니다. 포인트 솔루션과 통합(end-to-end) 솔루션 모두 다음 기능을 포함할 수 있습니다.

- 모바일 디바이스 구매, 스테이징, 구성
- 모바일 전략 개발
- 모바일 디바이스 관리 및 애플리케이션 개발
- 호스팅형 및 사내 구축형(on-premise) 보안 관리
- 모바일 정책 개발
- 일반 사용자 헬프 데스크 지원
- 네트워크 최적화, 보고, 모니터링, 통합 서비스
- 컴플라이언스 추적 및 적용
- 유지보수 및 디포(depot) 서비스
- 종합적인 전략, 구현, 일상적인 지원을 제공하도록 설계된 관리형 모바일 엔터프라이즈 솔루션

IBM 모바일 솔루션과 기능

IBM Mobile Enterprise Services for managed mobility

IBM Mobile Enterprise Services for managed mobility는 RIM BlackBerry, Apple iOS, Google Android 스마트폰과 태블릿, 여러 Microsoft Windows 모바일 기반 러기다이즈 디바이스를 비롯한 각종 디바이스와 운영 체제를 지원하고 고급 MDM 기능과 전략을 제공합니다. 다양한 플랫폼의 디바이스를 구매, 설치, 구성, 실행하고 관리할 수 있습니다. 고객의 디바이스 요구사항, 사용 필요성, 서비스 옵션에 따라 유연성을 발휘할 수 있는 구독 기반 가격 모델을 제공합니다.

IBM 전략 서비스는 비즈니스 및 IT 환경의 모바일 준비 실태를 평가하고 모바일 디바이스 관리를 위한 계획을 세울 수 있도록 지원합니다. 엔터프라이즈급 보안 정책 및 거버넌스 체계를 마련하여 사내외의 컴플라이언스 문제를 다루는 것과 같은 해결책도 조언할 수 있습니다. IBM의 모바일 인프라 전략 및 플래닝 기능을 활용하면 사용자 프로파일과 비즈니스 요구사항에 따라 올바른 선택을 내릴 수 있습니다.

IBM Integrated Communications Services

Integrated Communications Services는 "언제 어디서든" 통합 비즈니스 커뮤니케이션을 실현할 수 있는 최적화된 통신 및 네트워킹 환경을 구축하기 위해 이를 설계, 구현, 관리하는 데 중점을 둡니다. 이 솔루션을 활용하여 주요 네트워킹 환경을 지원하고 비즈니스 혁신을 통한 차별화된 우위를 확보할 수 있습니다.

IBM Telecom Expense Management Services

TelecomExpense Management(TEM) Services는 통신 비용 지출 패턴을 신속하게 파악하고 장단기적 절감이 가능한 영역을 찾아낼 수 있도록 컨설팅, 소프트웨어, 관리 서비스를 제공합니다.

IBM Mobile Foundation

IBM Mobile Foundation 오퍼링은 주요 모바일 기능을 하나의 통합형 패키지에 수록한 것으로 모바일 채널에서 제시하는 모든 과제와 기회를 수용할 수 있도록 지원합니다. IBM Mobile Foundation은 다양한 애플리케이션 개발, 연결, 관리 기능을 제공하면서 각종 모바일 디바이스와 모바일 앱 유형을 지원합니다.

IBM Mobile Foundation 오퍼링은 다음 제품으로 구성됩니다. 각 제품은 독립 실행형 버전으로도 구입 가능합니다.

- IBM Worklight® 여러 플랫폼에서 운용 가능한 모바일 앱의 개발, 실행, 관리를 지원합니다.
- IBM WebSphere® Cast Iron® Hypervisor Edition 클라우드 및 백엔드 시스템에 모바일 앱을 연결할 수 있도록 지원합니다.
- IBM Endpoint Manager for Mobile Devices 일반 사용자 디바이스를 제어하고 관리할 수 있도록 지원합니다.

IBM Mobile Foundation은 두 가지 구성으로 이용할 수 있습니다.

- Enterprise Edition – 기업에서 사내 앱을 관리하는 데 사용할 수 있는 B2E(business-to-enterprise) 패키지로서 Worklight, WebSphere Cast Iron Hypervisor Edition, Endpoint Manager for Mobile Devices가 포함되어 있습니다.
- Consumer Edition – 상용 앱 및 고객용 앱에 쓰이는 B2C(business-to-consumer) 패키지로서 Worklight 및 WebSphere Cast Iron Hypervisor Edition이 포함되어 있습니다.

IBM Sametime

IBM Sametime®은 사용자가 어디서든 간편하게 엔터프라이즈 인스턴트 메시징, 실재 프레즌스, 온라인 미팅, 텔레포니, 비디오 컨퍼런싱 등 다양한 기능을 이용할 수 있게 해주는 업계 최고 수준의 소프트웨어입니다. Sametime 소프트웨어를 활용하면 더 신속하고 경제적인 방식으로 고객 참여도를 개선할 수 있을 뿐만 아니라 각 팀이 직접 이동하지 않고도 사내외의 전문가들과 연계하여 더 발 빠르게, 전문성에 기초한 결정을 내릴 수 있습니다.

IBM Connections

IBM Connections는 사내외 환경에서 고급 애널리틱스 기능, 실시간 데이터 모니터링, 고속 협업 네트워크를 통합적으로 제공합니다. 이러한 기능은 사내 구축 형태로, IBM SmartCloud™에서 또는 각종 모바일 디바이스를 통해 이용할 수 있습니다. 여러 활동 스트림, 일정, 위키, 블로그, 이메일 기능 등을 통합하고 관련 데이터를 플래그로 표시하여 실행할 수 있게 합니다. 또한 클릭 한 번으로 즉시 협업하고 사내외에서 더 안전한 소셜 커뮤니티를 조직하여 고객 충성도를 높이고 더 빨리 비즈니스 성과를 거둘 수 있도록 지원합니다.

IBM Mobile Security

IBM Mobile Security 솔루션은 맬웨어를 차단하고 강력한 보안이 구현된 연결 기능을 제공하고 엔터프라이즈 데이터 및 시스템에 안전하게 액세스하고 더 안전한 애플리케이션, 더 안정적인 모바일 앱 플랫폼을 구축할 수 있도록 지원합니다. IBM의 주요 보안 제품은 통합 모니터링(one-view) 대시보드와 기능을 갖추고 스마트폰, PC, 서버, 라우터 등 사실상 모든 유형의 엔드포인트 또는 네트워크도 확실하게 보호할 수 있도록 지원합니다. 다음과 같은 기능을 제공합니다.

- IBM Security Access Manager – 비밀번호 관리를 간소화하고 액세스 보안을 강화하고 더 효과적으로 컴플라이언스를 입증할 수 있도록 지원합니다.
- Enterprise Wireless Networks – 뛰어난 보안과 성능을 갖춘 무선 네트워크 솔루션에서 “시간과 장소의 제약 없는” 커뮤니케이션을 실현할 수 있습니다.

- WebSphere DataPower® Service Gateway XG45 어플라이언스 – 확장 가능하고 자동화된 맞춤형 서비스 모니터링 및 거버넌스 기능으로 더 안전한 웹 서비스, 애플리케이션, 데이터를 제공할 수 있습니다.
- 호스팅형 모바일 디바이스 보안 관리 - 맬웨어 및 기타 위협 요소로부터 모바일 디바이스를 보호하는 데 필요한 지식과 기술을 제공하고 지속적으로 관리하는 등 "턴키" 형태로 모바일 디바이스 보안을 지원합니다.
- IBM AppScan® – 애플리케이션 보안 테스트 및 리스크 관리 솔루션을 제공합니다.
- IBM Lotus® Mobile Connect – 대표적인 모바일 디바이스부터 엔터프라이즈 호스팅 솔루션까지 전 범위에서 더 안전한 연결 기능을 제공합니다.

IBM을 선택해야 하는 이유

IBM은 15년 이상 수백 곳의 고객에게 모바일 솔루션을 제공하고 전 세계에서 수십만 대의 모바일 디바이스를 관리해 왔습니다. IBM을 선택한 고객은 모바일 전략 개발 및 구현부터 보안 관리, 일상적인 지원까지 모바일 환경의 라이프사이클 전 범위를 포괄하는 다양한 서비스와 혁신적인 솔루션을 이용할 수 있습니다. 뿐만 아니라 5,000명 이상의 통합형 통신 및 네트워킹 전문가, 전 세계에 위치한 70개의 워크플레이스 서비스 콜 센터, 9개의 보안 운영 센터, 12개의 모바일 서비스 및 지원 센터, 모바일을 지원하는 30개의 연구소가 포함된 강력하고 방대한 글로벌 인프라도 활용 가능합니다.[12] 또한 IBM은 업계 선두 주자로서 고객의 모든 IT 요구사항을 지원하고 멀티벤더 서비스 환경의 문제를 해결하는 기능을 제공하면서 복잡성을 줄일 수 있도록 지원합니다.

직원의 모바일 디바이스 선택을 지원하는 IBM

전 세계 IBM 직원의 절반 이상이 모바일 인력입니다. IBM은 2004년에 회사에서 지급한 단일 디바이스를 대상으로 시작했던 전사적 모바일 프로그램을 확장하여 업무 환경에 새롭게 도입된 각종 모바일 플랫폼을 수용해야 했습니다. IBM은 3년간 다양한 디바이스 및 운영 체제에서 모바일 액세스를 지원하는 파일럿 프로젝트를 진행했고 새롭게 출시된 태블릿과 같은 디바이스도 추가했습니다. IBM의 협업 소프트웨어가 이 솔루션에 필수적인 역할을 했습니다. 2011년에는 프로덕션 환경에서 대규모의 배치가 진행되었고 모바일은 핵심적인 인프라 서비스로 자리 잡았습니다. 현재 이 프로그램은 8만여 대의 개인 소유 디바이스를 포함하여 12만여 명의 모바일 사용자를 지원하며 계속 확장되고 있습니다.[13]

"IBM의 BYOD 프로그램은 사실상 직원이 원하는 방식으로 일할 수 있게 지원하는 것입니다. 직원 스스로 업무 수행에 가장 적합한 도구를 찾아냅니다. 그 도구를 사용할 수 있게 하되 회사의 무결성을 지키는 방식으로 허용하려 합니다."

—IBM CIO, Jeanette Horan

추가 정보

IBM의 모바일 엔터프라이즈 프로그램 관련 제품과 서비스에 대한 자세한 정보는 IBM 담당자에게 문의하십시오.

추가적으로, IBM Global Financing은 가장 비용 효율적 방법과 전략적 방법으로 비즈니스에서 필요로 하는 IT 솔루션을 취득할 수 있도록 도와줍니다. IBM은 신용 있는 고객과 협력하여 귀사의 비즈니스 목표에 적합하고 효과적인 현금 관리를 가능하게 하며 귀사의 총소유 비용을 개선하는 맞춤형 IT 재무 솔루션을 제공합니다. IBM Global Financing은 중대한 IT 투자에 자본을 투입하고 귀사의 비즈니스를 발전시키는 가장 현명한 선택입니다. 자세한 정보는 다음 웹사이트를 참조하십시오.
ibm.com/kr/financing

IBM Corporation
서울특별시 강남구 도곡동 467-12 군인공제회관빌딩
한국 아이.비.엠 주식회사 고객만족센터

[1] IBM: "유연한 워크플레이스로 성공 실현", 2012년 5월

[2] 동일 자료

[3] Gartner, "Seven Steps to Planning and Developing a Superior Mobile Device Policy", 2011년 10월 5일

[4] 개인용 컴퓨터

[5] Gartner, "Gartner Says Bring Your Own Device Programs Herald the Most Radical Shift in Enterprise Client Computing Since the Introduction of the PC", 2012년 8월 29일

[6] IBM, "유연한 워크플레이스로 성공 실현", 2012년 5월

[7] Ponemon Institute,"2011 Cost of Data Breach Study: United States", 2011년 3월

[8] 동일 자료

[9] IBM, "유연한 워크플레이스로 성공 실현", 2012년 5월

[10] Aberdeen Group, "Hidden Costs, Unseen Value", 2012년 8월 17일

[11] Gartner, "Seven Steps to Planning and Developing a Superior Mobile Device Policy", 2011년 10월 5일

[12] 통계는 2012년 11월 기준입니다.

[13] 통계는 2012년 기준입니다.

재활용하십시오

ENW03011-KRKO-00