IBM Security
리더십 사고의 백서

기업 컨텐츠와 앱 동원

비즈니스를 위한 간편하고 보호되는 모바일 협력 지원

IBM

새로운 시대를 위한 모바일 전략

문: 견고한 모바일 전략이 있습니까?

답: 모바일 전략이요? 저희 직원이 모바일 장치 상에 있는 이메일에 액세스할 수 있냐는 말씀이십니까? 그렇습니다. 가능해요.

그 대답이라면 여러분은 혼자가 아닙니다. 수많은 회사에서는 여전히 직원이 사무실 외부에서 의사소통할 수 있는 방편으로 "선택할 수 있는 앱"으로 이메일에 의존합니다. 몇 년 전쯤에는 큰 성과였죠. 하지만 인정합시다. 사무실 외부에서 이메일을 확인하고 답장하는 일은 장애물을 약간 제거하고, 이동시키고, 겉치레하는 등까지도 정확히 "일하는" 것이 아닙니다. 오늘날 세계에서, 모바일 협력은 진정한 생산성을 활용하고 거의 실시간으로 실제 작업을 용이하게 하는 엄청난 잠재력이 있지만 여러 기업은 이제 막 초기 단계에 접어들었으며 비즈니스 자원에 대한 간편하고 보호된 액세스가 가능한 이동성 기능을 활용하는 견고한 모바일 전략을 아직 수용, 계획, 배치하지 않았습니다.

본 문서에서는 지속적인 모니터링이 노트북, 데스크탑 컴퓨터 및 기타 엔드포인트 장치에 어떻게 적용되는지 논의할 것입니다.

이 백서에서는 다음 사항에 대해 배우게 됩니다.

- 장치 상의 VPN 없이 데이터를 기업 데이터에 대한 모바일 액세스 보호 지원
- SharePoint, Windows File Share, 귀사의 모든 인트라넷 사이트 동원
- 민감한 기업 데이터를 강력한 보안 방침 및 DLP 통제로 보호
- 네트워크 또는 방화벽 보안 구성을 변경할 필요 없이 모바일 액세스 가능
- 사용자의 개인 장치에서 어디서나 협업 지원

읽고 어떻게 직원이 방화벽을 넘어 액세스하고 인증, 암호화 및 컨테이너화 정책으로 데이터를 보호할 수 있는지 알아보십시오.

보안을 활용한 간편한 액세스

여기 간단한 문제가 있습니다. 모든 귀중품을 보호할 수 있도록 완벽하게 안전한 집을 만듭니다. 어떻게 접근해야 합니까? 창이나 문 없이, 입구나 출구 없이 집을 지었을지도 모릅니다. 완벽하게 안전할 순 있겠지만 실제 생활에는 전혀 유용하지 않습니다. 아니면 최고의 잠금 장치와 보안 시스템을 갖춘 창과 문으로 집을 지어 동일한 수준으로 보안을 효과적으로 유지할 수도 있습니다. 출입이 가능하고 손님도 맞이할 수 있으며 귀중품을 분실할 위험 없이 신선한 공기도 마실 수 있습니다.

여러분의 모바일 전략은 창이나 문이 없는 집과 같을 수도 있습니다. 또는, 창과 문을 전혀 잠그지 않는 집일 수도 있습니다. 기업 컨텐츠 보호를 책임지고 있지만, 사용자가 생산성을 유지하도록 만들어야 합니다. 고객 연락처 목록부터 환자 데이터, 재무 정보부터 인사부 파일, 기업 앱부터 이사회 회의록까지, 액세스하고자 하는 구성 정보는 매일 커지며 액세스 차단은 더 이상 실행 가능 조치가 아닙니다. 일부 창과 문이 필요합니다. 그리고 통과할 수 있게 도와주는 보안 시스템이 있어야 합니다.

사용자가 개인 스마트폰이나 태블릿을 가져와 영업 관련 연락처로 작업하고 장치로 다운로드하면 어떨까요? 독점 재무 보고서를 가정용 이메일 주소로 전송하고 자녀가 잠든 후 저녁에 작업할 수 있다면 어떨까요? 공급업체는요? 여러분은 컨텐츠와 앱을 공유해 더욱 효율적으로 협력하고 싶으실 겁니다. 하지만 프로젝트가 끝나면 어떻게 됩니까?

이런 일은 매일 발생합니다. 필요한 것을 얻기 위해 보다 안전하고 안정적이며 간단한 방법을 가능하게 하지 않는 한, 사람들은 필요한 정보를 찾기 위한 방법을 모색하며 기업 정보를 위험에 빠뜨립니다.

컨텐츠 고려사항

기업 컨텐츠는 Windows 파일 공유, SharePoint, 인트라넷 사이트 및 웹 앱 등의 공간에 기업 네트워크를 보관합니다. 사람들이 동료, 파트너, 고객과 함께 작업을 하도록 협력해야 하는 정보는 내부 드라이브 및 데이터 보관, 지식 기반, 내부 wikis, ERP, SCM, HRM, CRM 및 기타 관리 시스템 또는 프로세스에 트랩됩니다.

여기서 의문이 듭니다. 이동 중에 액세스가 필요한 현재의 모바일 작업자를 위해 어떤 방식으로 구축하고 계십니까? 소유하지 않은 장치에 대해서도 여러 번 구축합니까?

내부 네트워크, 파일 공유, 이를 저장하는 기타 시스템을 보호하면서, 모바일 전략의 일환으로 다음 고려사항에 대해 생각하고 싶으실 수 있습니다. 일부 사항은 명백해 보이지만 사실 주목할만한 가치는 없습니다.

1. 컨텐츠는 밀기 또는 당기기 접근법을 통해 요구 시 사용자가 액세스할 수 있어야 합니다
2. 각 사용자는 컨텍스트와 신원을 바탕으로 필요한 컨텐츠에 액세스해야 합니다
3. 데이터는 시간이 지나면 장치 전반에 걸쳐 업데이트 및 동기화되어야 합니다
4. 데이터 액세스 프로세스는 사용자에게 짐이 되어서는 안 됩니다
5. 투자를 많이 해도 보안 유지에 비용이 많이 들어서는 안 됩니다
6. 보안 유지는 IT를 위해 시간을 소비해서는 안 됩니다
7. 동적 데이터는 암호화 및 보호해야 합니다
8. 데이터는 인증 없이 조직을 나가도록 승인해서는 안 됩니다
9. 앱에서 생성 및 저장된 데이터를 보호해야 합니다
10. 개인 장치는 조직이 소유해서는 안 되기 때문에, 제어하는 데 한계가 있을 수 있습니다.

연방 사이버 보안 법안의 가장 중요한 목표 중 하나는 방어자가 공격자의 행동만큼 빠르게 시스템을 보호할 수 있게 하는 것입니다.

현재 기술

오늘날 사용하는 기술, 그리고 보안 및 생산성 지원이 내재된 일부 문제에 대해 알아보겠습니다.

이메일

이메일은 협력을 위해 선택할 수 있는 앱으로, 수많은 도구 중 하나일 뿐입니다.

협력용으로 설계되지 않았습니다. 이메일은 사용자가 진정으로 생산적이야 하는 다대다 상호작용 대신 1대1 또는 1대다 의사소통을 지원합니다. 이는 협력해야 하는 그룹 간의 사일로 개발을 장려합니다.

이메일로 전송한 정보는 곧 신선도가 떨어지기 마련입니다. 사람들은 최신 사항으로 대체되었다는 점을 깨닫지 못한 채 스프레드시트를 열고 계속 작업을 합니다.

가장 큰 문제는 데이터가 원하지 않는 곳으로 자르기, 붙여넣기 및 전달이 될 수 있다는 것입니다.

VPN

VPN 로그온은 방화벽을 넘어 액세스를 제공하는 일반적인 방법입니다.

안타깝게도, 사용자가 액세스하도록 강요하면 사용자 경험을 저하시킵니다. 액세스하기 어렵고 도달하기 쉬운 신규 컨텐츠와 기존 이메일 첨부 파일들과 함께 공급되는 생산성이 떨어지는 컨텐츠 중 선택한다면, 보통 쉬운 경로를 선택할 수 있습니다.

VPN은 장치별 라이센스가 필요하며 시간이 지나면서 비용은 증가할 수 있습니다. 또한, 장치 VPN 사용으로 장치 배터리가 보다 빠르게 소모된다는 증거가 있습니다.

무선 기술을 사용해 모바일 장치를 연결하기 때문에 암호화가 필요하지 않습니다. 그러나, 액세스와 동시에 로밍 관련 문제가 있습니다. 일반적으로, 높은 수준의 암호화에 의존하는 솔루션은 사용자가 액세스 지점 간에 로밍할 때 깨질 가능성이 있습니다. 다행히도 이를 해결할 방법이 있습니다.

데스크탑 가상화

일부 애플리케이션은 모바일 장치에서 데스크탑을 표시하도록 허용합니다. 데스크탑에서 액세스 가능한 모든 항목은 스마트폰이나 태블릿에서도 이용 가능합니다. 그러나 일반적으로 비싸며 사용자 경험이 열악합니다. 이러한 접근법으로 가용성과 성능은 네트워크 연결에 따라 크게 달라집니다. 또한 화면 크기와 해상도 문제 역시 도전 과제로 남아 있으며 특히 스마트폰은 화면이 작고 작업 공간이 협소하다는 문제점이 있습니다. 데스크탑 환경에 최적화된 애플리케이션은 데스크탑 가상화를 통해 모바일 장치에 액세스할 수 있지만 그렇다고해서 유용하다는 의미는 아닙니다.

IT가 고려해야 할 또 다른 사항은 서버와 네트워크 자원이 동시에 네트워크에 연결하는 수많은 장치를 지원해야 한다는 점입니다.

제3자 파일 공유

제3자 파일 공유로 클라우드에서 참고 자료를 보관합니다. 여기서 발생하는 큰 문제는 제어할 수 없다는 점입니다. 누구나 컨텐츠를 볼 수 있고 누구나 액세스할 수 있으며 버전 제어 문제가 있을 수 있습니다.

여기에도 사용자 경험 문제가 발생합니다. 사용자는 필요한 컨텐츠에 바로 액세스하는 새로운 소프트웨어를 억지로 학습하려 들지 않으며, 또한 학습하는 데 소요되는 사용자의 시간에 대해서도 고려해야 합니다.

제3자 파일 공유에도 비용이 많이 들 수 있습니다. 사용자가 추가되면서 라이센스 추가도 필요하고 그와 더불어 앱과 컨텐츠 스토어 같은 기존 투자를 사용할 수 없을지도 모릅니다.

제3자 및 사용자 지정 앱

귀하의 앱에 대해 제3자 개발자에게로 이동할 경우, 공급업체에 따라 달라집니다. 데이터 누출 방지 (DLP)가 앱에 내장되어 있지 않을 수도 있습니다.

자체 앱을 개발하려 할 수도 있지만, 이를 지원할 직원과 새로운 장치 유형, 운영 체제 업데이트 등에 필요한 변경 사항이 있어야 할 것입니다.

수많은 보안 전문가, 최고의 연방 정부 사이버 보안 담당자, 의회 지도자는 지속적인 모니터링, 자동 모니터링 도구, 정부 정보 기술 시스템 공격에 대한 빠른 대응을 점차 강조하고 있습니다.

정책의 중요성

사용자가 개인 장치에 있는 기업 자원에 액세스할 수 있게 허용하려고 한다면 데이터 액세스 및 사용 방법 관련 규제 정책을 세워야 합니다.

중요 데이터에 액세스하기 전 사용자가 암호를 입력하게 할 수 있습니다.

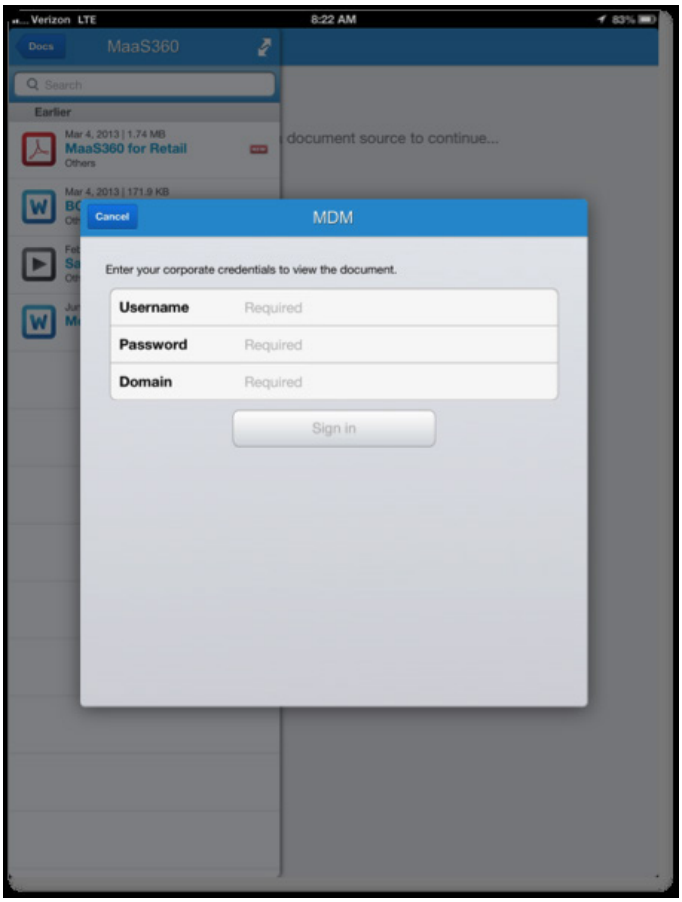

그림 1: 인증 요청

또한 문서에서 텍스트 자르기 및 붙여넣기를 제한할 수도 있습니다.

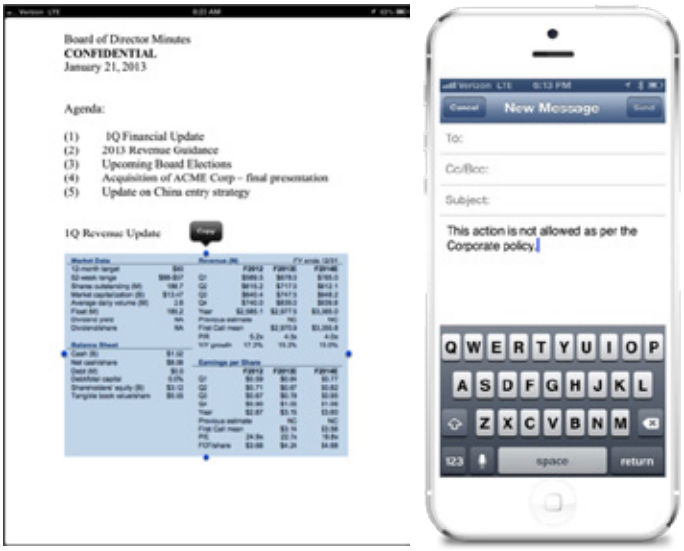

그림 2: 복사 및 붙여넣기 제한 등 데이터 유출 방지 제어

IBM® MaaS360® Productivity Suite

MaaS360 Productivity Suite은 현재 기술로 발생하는 문제를 극복하도록 도움을 주며 안전한 액세스를 지원하고 정적 데이터를 보호하는 여러 방법으로 설계되었습니다.

1. IBM® MaaS360® Secure Mobile Mail
2. IBM® MaaS360® Mobile Application Security
3. IBM® MaaS360® Secure Mobile Browser

MaaS360은 장치에서 보호되는 영역에서 회사별로 유지하는 데이터, 앱, 컨텐츠에 대한 이중 개인 접근법을 위한 컨테이너를 사용합니다. 보호 영역에 제어장치를 배치하도록 결정해 메일, 연락처, 캘린더, 앱 (및 앱 데이터) , 문서 및 웹 페이지 액세스를 보호할 수 있습니다.

그림 3: MaaS360 Productivity Suite 및 MaaS360 Content Suite

MaaS360 Productivity Suite는 개인 정책을 사용해 모든 사용자의 장치에 보안을 지정합니다. 이러한 정책은 MaaS360 포털에 생성되며 무선으로 등록 장치에 배치되므로 IT는 물리적으로 장치에 접촉할 필요가 없습니다.

장치가 규정을 준수하지 못할 경우나 프로젝트가 끝나고 공급업체가 떠날 경우, 컨테이너가 원격으로 제거되고 데이터와 앱이 사라집니다.

컨테이너에는 보안이 내장되어 있으며, FIPS 140-2 준수, AES-256 암호화를 포함합니다. 액세스할 때 사용자가 암호를 입력해야 할 수도 있습니다. 또한 장치가 탈옥 또는 루팅된 경우 또는 장치가 특정 기간 안에 확인되지 않았을 경우 이러한 정책 설정을 사용해 컨테이너를 완전히 제거할 수도 있습니다.

또한 파일을 컨테이너에서 이동, 복사 또는 인쇄하는 것을 방지하며, 파일 가져오기가 실행되지 않도록 방지할 수 있습니다.

IBM® MaaS360® Content Suite

MaaS360 Content Suite는 암호화 컨테이너 및 생산성 도구를 제공해 모바일 장치에서 문서를 배포, 보기, 생성, 편집 및 공유하며, 조직에 필요한 제어를 제공하고 직원에게 필요한 액세스를 제공합니다.

1. IBM® MaaS360® Mobile Content Management
2. IBM® MaaS360® Mobile Document Editor
3. IBM® MaaS360® Mobile Document Sync

MaaS360 Mobile Content Management는 문서를 배포, 업데이트, 관리 및 보호하는 견고한 수명 주기 관리 기능과 컨텐츠 협력을 위한 모바일 문서 컨테이너를 제공합니다. IT 관리자는 인증, 복제/붙여넣기 및 보기 전용 제한 사항을 실행할 수 있습니다. 사용자는 SharePoint, Box 및 Google Drive 등 기업 배포 컨텐츠 및 파일 저장소에 액세스할 수 있습니다.

MaaS360 Mobile Document Editor는 기업 데이터 유출을 방지하는 동시에 사용자가 생성, 편집 및 저장하도록 설계되었습니다. 사용자는 어디서나 모바일 장치 상에서 Word, Excel, PowerPoint 및 텍스트 파일로 협업할 수 있습니다.

MaaS360 Mobile Document Sync는 쉽게 관리된 모바일 장치 상에서 사용자가 쉽게 컨텐츠를 동기화하도록 지원해 중단 없이 파일을 계속 생성하거나 편집할 수 있습니다. IT는 비관리 앱에서 복사/붙여넣기 및 열기나 공유 차단 제한 등 컨텐츠에 정책을 적용합니다. 이러한 제어 장치는 모든 문서, 문서 조합 또는 개별 문서에 적용할 수 있으며, 귀중한 기업 데이터를 보호해야 하는 유연성을 제공합니다.

보호 컨텐츠 공유 사용 사례는 판매, 마케팅, 운영 또는 재무에 관계없이 거의 모든 조직에서 무수히 발견됩니다.

- 언제 어디서나 고객 미팅 바로 전에 영업 프레젠테이션에 대한 최종 변경사항을 열람하고 공유
- 비행기에 탑승하기 전에 스프레드시트로 된 최신 재무 자료를 가지고 협동작업 수행

- 카페에서 마케팅 메시지를 브레인스토밍 하고 동료와 공유
- 이사회에 분기별 재무 문서를 배부하고 회의 후 문서가 만료되도록 설정
- 거의 실시간으로 제품 자료를 영업팀과 공유함으로써 최신 데이터시트 또는 경쟁력 있는 정보를 힘들게 찾는 노력 절감
- 매장의 태블릿이 최신 제품 및 재고 정보를 보유하도록 지원

IBM® MaaS360® Gateway Suite

MaaS360 Gateway Suite는 이러한 가능성을 지원하는 핵심 구성요소입니다. 이는 모바일 장치에서 기업 컨텐츠 및 인트라넷에 대한 원활하고 보호되는 액세스를 제공함으로써 동적 데이터를 보호합니다.

- 장치 상의 VPN 없이 데이터에 대한 간편하고, 보호되는 모바일 액세스 제공, 정보를 원할 때마다 VPN에 로그인해야 할 필요 없음
- SharePoint, Windows File Shares, 인트라넷 사이트 및 웹 앱 동원
- 데이터를 강력한 보안 방침 및 DLP 통제로 보호
- 네트워크 또는 방화벽 보안 설정에 대한 변화 불필요

그림 4: MaaS360 Gateway를 활용한 데이터 흐름

MaaS360 Productivity Suite가 사용자 장치와 상호작용하는 방법을 관리하는 정책 옵션을 구성할 수 있습니다. 예를 들어, 여러분은 URL을 기업 wikis, 버그 추적 시스템 등 그리고 MaaS360 Gateway를 통해 액세스 가능한 기업 폴더로 지정할 수 있으며 이는 MaaS360 Secure Mobile Browser의 북마크로 나타나게 됩니다. 이러한 위치에 액세스하는 데 인증이 필요할 경우 지정할 수도 있습니다.

MaaS360 Gateway는 장치 상의 데이터 컨테이너에 액세스할 때 기업 자원 사용자가 무엇을 보게 되는지를 결정합니다.

구매하기 전 시도해보세요

MaaS360은 빠르고 쉽게 시도해 볼 수 있습니다. 또한, 여러분의 요구사항에 맞게 MaaS360를 구성하는 데 필요한 시간도 적절합니다. MaaS360가 조직에게 맞는 솔루션이라고 결정하고 나면 시험 환경은 실제 환경이 됩니다!

MaaS360 무료 시험판은 여기를 클릭하십시오. 바로 시작할 수 있습니다. 복잡한 설정 프로세스나 변경해야 할 인프라가 없습니다. 지금 MaaS360을 시도해보세요!

그림 5: MaaS360 제품

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

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America 2016년 3월

WGW03111-KRKO-01