ENDPOINT PROTECTOR | 4

iOS, Android, OS X 모바일 기기 관리 (MDM) 솔루션
iOS, Android 모바일 앱 관리 (MAM) 솔루션

Endpoint Protector 장비의 모바일 기기 관리(MDM) 기능은 별도의 설치 과정이 없이 즉각 사용이 가능합니다. 모든 규모의 기업 및 다양한 조직에서 회사 소유 또는 개인소유(BYOD)의 모바일 기기 사용이 점점 증가하면서 커지고 있는 보안위협 및 모바일 기기 관리의 취약점을 즉시 보완합니다.

Endpoint Protector는 매체제어, 자료유출방지(DLP), SW 보안USB 그리고 MDM / MAM 기능을 하나의 장비로 구현한 통합 자료보안 솔루션으로 IT 관리자가 전체 네트워크의 컴퓨터(Windows, Mac OS X, Linux)는 물론 모바일 기기(iOS 및 Android)까지 자료유출의 위협에서 보호할 수 있는 매우 효율적이고 경제적인 솔루션입니다.

쏟아져 나오는 새로운 휴대용 스마트 기기들이 기업이 일하는 방식과 가정의 생활까지 변화시키는 요즘, Endpoint Protector는 신종 기기들의 홍수 속에서 기업의 생산성을 유지시키고 또한 주변기기의 악용에 의한 위협으로부터 기업의 중요한 정보 자산을 안전하게 지킬 수 있게 합니다.

Endpoint Protector는 하드웨어 장비 혹은 가상화 환경을 위한 가상 어플라이언스로 공급되어, 상자에서 꺼내면 바로 설치되고 즉시 사용이 가능해서 즉각적으로 기업의 중요한 자료의 유출 및 도난 위험을 현격하게 줄여 줍니다.

주요 장점들

- iOS, Android, OS X 모바일 기기 관리
- HW 장비 또는 가상 어플라이언스로 제공되어 십분 안에 설치 및 가동이 가능
- 웹 브라우저로 사용 가능한 관리자 환경
- 즉각적인 모바일 기기 보안 관리 강화
- 비전문가도 운영 가능한 모바일 기기 및 엔드포인트 자료유출방지 제품
- 휴대용 주변 장치의 규정 위반 오용방지를 통한 자료 유출의 사전 예방
- VMware, Hyper-V 등 가상화 지원

모바일 엔드포인트 보안

기업에서 사용하는 스마트폰과 태블릿에 강력한 보안정책을 적용함으로써 기업의 중요한 데이터를 가지고 있는 모바일 기기들에게 대한 허락되지 않은 접근에 따른 정보유출의 위험을 미리 예방합니다.

iOS, Android 기반의 모바일 기기 지원

요즘 가장 많이 사용되고 있고 가장 빠르게 성장하고 있는 두 가지 모바일 플랫폼인 iOS 및 Android 계열의 모든 모바일 기기들을 제어하고 관리해서 기업의 중요한 자료를 안전하게 보호합니다.

비밀번호 정책의 적용 강화

정기적으로 무선으로 직접 비밀번호를 변경하거나 또는 기기 사용자에게 주기적으로 비밀번호를 변경하도록 유도합니다.

분실 기기 추적 및 위치 찾기

기업에서 사용하는 등록된 모바일 기기들의 위치를 파악해서 기업의 중요한 민감한 자료가 들어있는 기기의 위치를 추적 할 수 있습니다. iOS는 MDM 앱을 통해서 위치를 파악할 수 있습니다.

원격삭제 / 원격잠금으로 도난 방지

분실 기기를 원격으로 제어해서 기밀 자료가 유출되지 않도록 봉쇄합니다. 모바일 기기를 분실하거나 도난 당했을 경우에는 원격삭제를 실행하거나, 원격잠금 기능으로 기기의 사용을 차단해서 자료유출을 막습니다.

iOS 내장 응용 프로그램 통제

회사의 정책이 허용하는 iOS 내장 기능들만 사용하게 할 수 있습니다. 다음과 같은 기능들을 정책에 따라서 끌 수 있습니다. iCloud, FaceTime, YouTube, App Store, In-App Purchases, iTunes, Siri, 내장 카메라 등.

소리내기 기능으로 분실 기기 찾기(Android)

잃어버린 스마트폰 및 태블릿을 찾는다면 원격으로 좋아하는 노래를 틀어서 잘못 놓여진 기기를 쉽게 찾을 수 있습니다.

iOS 기기의 이메일, VPN 및 WiFi 설정을 관리

원격으로 iOS를 사용하는 기기들의 이메일과 VPN 및 WiFi 설정을 관리합니다.

iOS 기기의 이메일과 WiFi 설정 정보 삭제

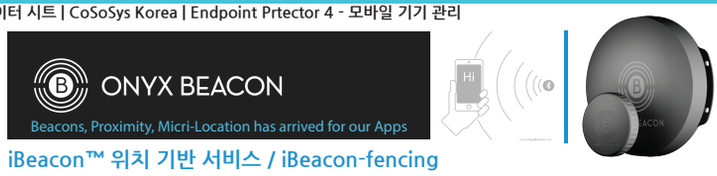
원격으로 회사 이메일 내용과 무선 설정을 제거하고, 개인 이메일을 건드리지 않고 회사 메일을 삭제 할 수 있습니다.

모바일 응용 프로그램 관리

개인 또는 회사 소유의 스마트폰이나 태블릿에 설치된 응용 프로그램들을 파악해서 악성 코드나 신뢰할 수 없는 응용 프로그램으로 인한 중요한 자료의 훼손이나 유출을 방지할 수 있습니다.

BYOD (Bring-Your-Own-Device) 업무 형태 지원

개인 또는 회사 소유의 기기에 있는 중요한 회사 자료들에 관리 권한을 가지고, 기업의 중요한 자료의 유출을 관리하면서도 개인 소유 기기의 사용을 제한하지 않아서 직원들이 효율적으로 일할 수 있도록 합니다.



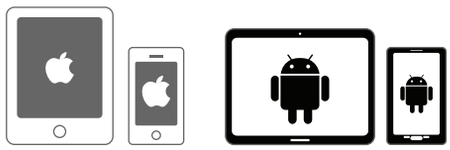
iBeacon™ 위치 기반 서비스 / iBeacon-fencing

실내에서 비컨을 기준으로 특정 위치를 지정하고 모바일 기기 정책이 작동하도록 합니다. 예 : 비컨 영역에서 스마트폰의 카메라 끄기.

GPS 영역 기반 서비스 / Geofencing

위치기반 서비스를 사용해서 지상에 가상의 영역을 정의하고 이 영역 안에서만 모바일 기기 정책이 작동 하도록 합니다.

기업 은 모바일 기기 관리 정책을 명확하게 정의하고 실행함으로써 스스로를 보호해야 합니다.



주요 장점들

- 모바일 기기 사용 정책 실행
- 모바일 기기 사용으로 인한 기업의 정보유출 방지
- 모바일 기기에 대한 즉각적인 제어
- MDM/MAM과 DLP를 한 장비로 구현
- 무선 원격 설치
- 사용자 및 관리자에게 미치는 영향과 필요한 노력을 최소화
- 규정 준수 및 생산성 유지
- BYOD 보안 및 관리 솔루션 제공

간편한 웹 기반 관리 및 보고 및 보기 쉬운 실시간 대시 보드 제공

모바일 기기들의 사용을 중앙에서 웹 기반으로 관리합니다. 이 관리 및 보고 도구를 기반으로 IT 보안 관리자의 요구 및 정책 관리자의 요구를 모두 만족 시키고, 조직 전체가 사용하는 모바일 기기 및 주변 장치 그리고 사용되는 모든 매체들의 활용에 관한 사용정보를 실시간으로 관리합니다.

모바일 기기 인벤토리 관리

기업 또는 직원들이 업무용으로 사용하는 모바일 기기들 전체를 쉽게 관리할 수 있게 돕고, 각 기기들의 활동들을 구체적으로 기록하고 로깅함으로써 추후 감사 활동을 돕습니다.

모바일 기기 암호화

iPhone 및 iPad는 256bit AES 하드웨어 암호화가 구축되어 있습니다. 이 기능은 기기 암호가 설정되면 항상 작동하게 되고, MDM 정책으로 관리됩니다.

사용자가 직접 혹은 원격 무선등록 / 모바일들 기기 설정

일회용 코드를 사용한 사용자 셀프서비스 또는 원격 무선등록 방식으로 쉽고 안전하게 기기들을 관리하는 MDM 플랫폼에 등록하고, 모바일 기기들을 설정할 수 있습니다.

모바일 기기를 위한 자산 관리

회사 및 개인소유(BYOD) 모바일 기기에 대한 전체정보를 쉽게 유지할 수 있습니다.

지원하는 모바일 기기**

- iPad, iPhone, iOS 5.0 이상 모든 iOS 기반의 기기 (지속적인 신버전 지원)
- Android 2.3 이상 모든 기기 (지속적인 신버전 지원)
- Mac OS X 버전 10.5 이상 모든 Apple Mac 컴퓨터 (El Capitan 지원)

MDM 설정을 위한 필요 사항

- iOS MDM 설정은 무료 APNS (Apple Push Notification Service) 계정이 필요하고, 무료 Apple ID로 만들 수 있습니다.
- Android MDM 설정은 Android용 무료 Google 클라우드 메시징(GCM) 계정이 필요하고, 무료 Google 계정으로 만들 수 있습니다.

당사의 MDM 기능 및 iOS/Android 기능은 계속 업데이트됩니다.

www.cososys.co.kr
support@cososys.co.kr

MDM 기능 요약 그리고 iOS 및 Android 지원 기능 비교

iOS 및 Android 기반 기기를 위한 MDM 기능들은 계속 확장되고 있으며, 모바일 기기의 보안에 대한 새로운 요구들이 생기면 그에 따라서 필요한 기능들도 지속적으로 강화될 것입니다. Live Update로 새로운 기능을 계속 제공합니다.

MDM 기능들	iOS	Android
기기 등록	✓	✓
이메일, URL, QR Code, SMS문자, CSV, 100+ 국가지원	✓	✓
강력한 보안 정책	✓	✓
비밀번호 변수(길이, 재시도, 숫자, 문자 등)	✓	✓
화면 잠금 시간	✓	✓
비밀번호 강제 적용	✓	✓
기기 암호화 적용(기기/OS 내장 암호화 기능)	✓	✓
기기 추적 및 위치 찾기(MDM 앱 필요)	✓ (필요)	✓ (아님)
분실 기기 찾기 (소리내기 기능)		✓
원격 잠금	✓	✓
원격 데이터 삭제	✓	✓
모바일 기기 삭제	✓	✓
SD 카드 삭제		✓
회사의 이메일 내용 및 이메일 설정 삭제	✓	
모바일 앱 관리 (MAM)	✓	✓
Geofencing(위치기반 정착 구현)	✓	✓
무료 SMS로 실시간 등록 한국, 미국, 영국, 독일 등 100개 이상 국가 지원	✓	✓
네트워크 설정 보내기	✓	✓
WiFi 및 Bluetooth 차단		✓
이메일 설정, WiFi 설정, VPN 설정	✓	
기기 기능 사용 제한		
iTunes, iCloud, 엡 스토어, 앱 내 구매 Siri, 카메라, FaceTime iTunes 백업 강제 암호화 Safari, YouTube 등등 MAM 기능 : 앱 강제 설치 혹은 삭제 및 관리 기능	✓	
카메라 사용제한	✓	✓
그 밖에도 많은 기능 이용 가능, 매뉴얼 참고 바람	...	...
지원되는 OS 버전	Apple iOS 5 이상	Android 2.3 이상

주의 : 기기 보안 및 관리 기능 중 일부는 오래된 OS 버전 또는 구형 장치에서는 지원되지 않을 수도 있습니다.

컴퓨터의 매체 제어 기능을 함께 제공(옵션)

Endpoint Protector는 휴대폰 자료유출방지를 위해 Windows, Mac OS X 및 Linux 기반 컴퓨터의 USB 포트 통제 기능 및 주변 장치 통제 기능들을 제공합니다.

자료유출방지(DLP) - 개인정보보호 및 유출차단 기능(옵션)

자료유출방지 기능은 기업의 네트워크에서 외부로 전송되는 민감한 자료를 콘텐츠 수준에서 제어하고 관리합니다. 효율적인 콘텐츠 검사를 실시함으로써 기업의 중요한 문서가 외부로 전송될 경우 기록을 남기고, 정책에 따라서 유출을 실시간 차단합니다. 이 기능은 USB 휴대용 저장장치부터 Outlook, Skype, NateOn/LINE/카카오톡/마이피플 등 메신저 또는 uCloud, 다음 Cloud, N-Drive, iCloud, Dropbox 등 클라우드 및 FTP, bitTorrent와 같은 P2P 응용 프로그램들을 통해서 빠져 나가는 내부자료유출 및 개인정보유출을 방지합니다.

개인정보보호법에서 규정된 개인정보의 유출방지 기능(옵션)

Endpoint Protector의 DLP 기능은 개인식별정보인 주민등록번호, 운전면허번호, 의료보험번호, 전화번호, 전자메일 주소, 신용카드번호 등등의 유출을 방지합니다.

고성능 저전력 상온 운전이 가능한 신형 장비 (1U, 1/4 길이의 소형)

- 내장 RAID1 스토리지 (1TB-6TB), 서버용 CPU 4/6/8/16 코어, 4~32GB ECC RAM
- 50, 100, 250, 500, 1000, 2000(개발중) 클라이언트 모델에 적용

Endpoint Protector 가상 어플라이언스 편의성

Endpoint Protector 가상 어플라이언스는 모든 규모의 기업에서 사용할 수 있습니다. 가상 어플라이언스는 VMX, OVF 및 VHD 등 다양한 형식을 지원하기 때문에 많이 사용되는 대부분의 가상화 플랫폼들과 호환이 가능하고 또한 하드웨어 비용이 없습니다.

가상 어플라이언스는 설치하는 즉시 허가 받지 않은 장치의 사용과 자료 유출로부터 네트워크를 보호할 수 있습니다.

VMWARE CERTIFIED VIRTUAL APPLIANCE

vmware READY

지원 가능한 가상 환경	버전	.ovf	.vmx	.VHD
VMware Workstation	7.1.4 ~ 12.0	-	*	-
VMware Player	6.0.0 ~ 12.1	-	*	-
VMware vSphere (ESXi)	5.1 ~ 6.0 U1	*	-	-
Oracle VirtualBox	4 / 5	*	-	-
Parallels Desktop for Mac	9 ~ 11	-	*	-
Microsoft Hyper-V	2008~2012 R2	-	-	*

그 밖의 다른 가상화 환경도 지원합니다.

Endpoint Protector는 다양한 주변기기 및 USB 저장장치와 각종 매체들이 사용되는 작업 환경에서 내부 자료의 유출을 방지합니다. 네트워크에서 자료유출 차단 보안 정책을 실행하면서도 허가된 장치 및 매체들을 지속적으로 사용할 수 있기 때문에 사용자의 업무 효율성에 영향을 주지 않습니다. MDM 고객은 저렴하게 추가 가능합니다.

www.cososys.co.kr 에서 데모 버전 검토 및 무료 평가판을 다운로드 할 수 있습니다.

CoSoSys 독일
이메일 : sales.de@cososys.com
전화 : +49-7541-978-2627-0
팩스 : +49-7541-978-2627-9

CoSoSys 북미
sales.us@cososys.com
+1-208-850-7563

(주)코소시스코리아
sales@cososys.co.kr
070-4633-0353
010-2025-0586

제품문의는 (주)코소시스코리아에, 구입문의는 **전문파트너**에게 하여 주세요.

(주)코소시스코리아 대표번호 : 070-4633-0353, Fax : 02-6008-5330
기술지원 요청 : support@cososys.co.kr, 영업관련 요청: sales@cososys.co.kr

www.cososys.co.kr 에서 데모 버전 검토 및 무료 평가판을 다운로드 할 수 있습니다.

Korea Evaluation and Certification Scheme ITSCC
DLP
국내용 CC인증

전문 기술 파트너 :

COSOSYS

2016년 2월 23일 수정됨.