ENDPOINT PROTECTOR | by CoSoSys

내부정보 유출 방지 (DLP)

매체 제어, 개인정보 검색, SW 보안USB, eDiscovery, MDM/MAM

Windows PC / Server / VDI, macOS, Linux 등을 위한 DLP 장비

모든 운영체제를 지원하는 매체제어, DLP, 개인정보 검색 기능

Srv iOS

즉시 사용 가능한 DLP 장비로 제공

ENDPOINT PROTECTOR

by CoSoSys

USB 외부 저장장치, 스마트 폰, 클라우드 서비스, 다양한 모바일 기기, 이메일, 네트워크 등으로 유출되는 정보를 검출하여 차단하는 내부정보 유출방지 DLP 솔루션으로서, 복잡한 설치 없이 즉시 사용이 가능한 DLP 장비입니다.

Endpoint Protector는 개인정보보호법에서 보호 대상으로 정한 중요한 개인정보의 유출을 실시간으로 차단하고, 기업의 영업비밀 보호를 위한 매체제어 및 내부정보 유출 방지(DLP), SW 보안USB, eDiscovery 및 모바일 기기 관리(MDM) 기능을 함께 제공하는 DLP 장비입니다.

Windows, macOS, Linux 환경에서 PC 및 서버의 정보 유출을 예방하고 iOS, Android, macOS 기반 모바일 기기를 관리합니다.

Endpoint Protector는 사용이 간편한 DLP 장비로 제공되어서 복잡한 설치 과정 없이 장비의 IP만 입력하면 바로 사용할 수 있습니다. 필요한 것은 오직 DLP 장비 한 개입니다.

Endpoint Protector는 국가용 정보보호제품 보안요구사항 중 매체제어 제품 및 호스트 자료유출 방지 제품으로 국내용 CC인증을 받았고 매체제어, SW 보안USB, 개인정보 검색 삭제 및 암호화 기능을 인증 범위에 포함하고 있습니다. 또한 라이선스만 구매하면 MDM/MAM 기능이 제공됩니다.

장비의 기능

콘텐츠 인식 보호
Windows, macOS, Linux

- 내부정보, 개인정보 유출을 감시. 응용프로그램의 파일 전송을 제어, OCR 스캔, 심층 패킷 검사(macOS).
- 파일 확장자, 개인정보 콘텐츠, 사용자 키워드, 소스 코드, 도메인 및 URL, 정규식 등으로 필터 설정.

매체 제어
Windows, macOS, Linux

- USB 장치 관리, 스마트폰 통제, 테더링 통제, BadUSB 차단, 다양한 포트 및 저장 매체 사용을 제어.
- 사용자, 컴퓨터, 그룹, 전체 등으로 체계적인 사용 권한 제어, 사내 및 사외 정책, 근무시간 외 정책 등 지원.

모바일 기기 관리
Android, iOS, macOS

- 스마트폰, 태블릿 등의 보안 설정 및 기기 관리, 신규 버전의 OS 지속적 지원.
- 기기 보안 설정, 네트워크 설정, 응용프로그램 등의 정책적 관리.

SW 보안USB
Windows, macOS

- 보안USB 사용 정책. USB 저장장치로 복사되는 파일을 자동 암호화.
- 크로스 플랫폼, AES256 CBC 및 ARIA 256 블록 암호화 지원.
- 1TB 이상 보안USB 저장장치 지원, 중앙집중 보안USB 관리, 암호 설정 관리 등.

eDiscovery
Windows, macOS, Linux

- 개인정보 검색, 파일 완전삭제 혹은 암호화, 중앙집중식 파일 관리, 자동 반복 실행 지원 등.
- 파일 확장자, 개인정보 콘텐츠, 사용자 키워드, 소스 코드, 검색위치, 정규식 등으로 필터 설정 등.

콘텐츠 인식 보호
Windows, macOS, Linux 용

- **이메일:** Outlook, Thunderbird, Lotus Notes, Eudora, Opera Mail, Zimbra Desktop Mail, SeaMonkey Mail 등 다수
- **웹브라우저:** IE, Chrome, FireFox, 네이버 Whale, Swing, Tor, Safari, Opera, AOL Desktop, Maxthon, SeaMonkey 등 다수
- **인스턴트 메시징:** 카카오톡, 라인, 네이트온 메신저, Skype, Lync, QQ, ICQ, AIM, Google Talk, eBuddy, FaceBook 메신저 등
- **클라우드 및 파일공유:** 네이버 N-Drive, 올레/다음 cloud, DropBox, OneDrive, iCloud, Torrent, FTP, Evernote 등 다수
- **응용 프로그램:** 알드라이브, 파일질라, iTunes, Samsung Kies, Total Commander, TeamViewer, Wormhole Switch DSS 등

개인정보 콘텐츠 필터
신용카드번호, 주민등록번호, 운전면허번호 등과 같이 국가별로 개인정보보호를 위하여 요구하는 정보들을 검출하고 유출을 차단하는 필터를 설정할 수 있습니다.

사용자 정의 콘텐츠 필터
사용자가 만들 수 있는 다양한 키워드 사전을 활용하여, 바이너리 파일을 포함한 모든 파일에 정밀한 키워드 검사를 실시합니다.

문맥 감지 콘텐츠 검사
개인정보와 같은 민감한 내용을 보다 정확하게 검사하기 위한 향상된 검사 매커니즘 제공. 콘텐츠 문맥을 사용자가 정의할 수 있습니다.

정규식 필터
데이터에서 반복되는 패턴이 있는 경우에는 표준 정규식을 사용하여 패턴을 정의하고 모든 전송되는 파일에서 정의된 패턴을 검사할 수 있습니다.

파일 종류 필터
파일 종류를 엄격하게 판별하기 위한 기술을 사용하여 변경된 파일 확장자를 식별하고, 사용자의 정책에 따라서 특정한 종류의 파일 전송을 제어합니다.

정책 대상 블랙리스트
감시하는 많은 응용프로그램들 목록에 차단 필터 적용 가능. USB 저장장치, 네트워크 공유 등 다양한 정보유출 대상에도 콘텐츠 검사 수행.

파일 화이트리스트
콘텐츠 인식 파일 전송이 차단되어도 파일 화이트리스트는 전송의 예외를 허락하고 생산성을 높이기 위해서 사용될 수 있습니다.

이메일 도메인 및 URL 화이트리스트
조직의 내부에서 내부로, 반출이 허용된 목적지로 필요한 업무를 하는데 허용된 목적지를 지정하여 반출을 허락하여 유연성을 제공합니다.

Print Screen 사용 안 함
컴퓨터의 화면인쇄 기능을 꺼서 화면에 보이는 중요한 데이터가 유출되지 않도록 지원합니다.

클립보드 모니터링
복사 & 붙여넣기 / 잘라내기 & 붙여넣기를 통한 콘텐츠의 복사를 감시하여 민감한 콘텐츠의 이동 위험을 제거하여 데이터 보안 정책을 강화합니다.

보고 및 분석
로그 및 분석은 파일 전송에 관련된 활동을 모니터 합니다. 또한 SIEM 솔루션으로 로그를 내보낼 수 있습니다. 감사 로깅 기능은 디지털 포렌직 수준의 자료를 제공합니다.

대시보드 및 그래픽 보고
중요한 이벤트들과 감사 로그의 통계들을 시각화하여 그래픽 및 차트로 제공합니다. 중요 정보 표시 기능은 정보보안 관리자에게 편리한 운영 환경을 제공합니다.

OCR 스캔
사진 및 이미지의 콘텐츠 검사. 스캔한 문서 이미지 등에서 민감한 정보를 검사합니다.

범용, 정규 필터 임계값
전송 파일에 허용되는 위반의 수를 정의하여 탐지 감도를 조정. 전체 위반의 수 혹은 각각의 경우 별 위반의 수를 선택 가능합니다.

전송 제한
파일의 수 또는 파일의 크기 등의 전송 제한 값으로 파일 전송을 제한합니다. 전송 제한에 도달하면 이메일 경고도 가능합니다.

파일 추적
외부 저장장치, 네트워크 폴더 파일 이동, 웹 전송, 이메일 첨부, 메신저, 응용프로그램과 클라우드를 통한 파일 전송을 기록합니다.

파일 보관
외부 저장장치, 네트워크 폴더 파일 이동, 웹 전송, 이메일 첨부, 메신저, 응용프로그램과 클라우드를 통한 파일 전송 때 사본을 보관합니다.

오프라인 임시 암호
네트워크 연결이 없는 클라이언트 컴퓨터에서 파일 전송을 임시로 허용하여 생산성을 높이기 위하여 사용됩니다.

이메일 경고 만들기
미리 설정된 혹은 사용자가 정의한 경고 메일을 만들어서 시스템의 중요한 이벤트나 정보의 유출 발생과 같은 상황 정보를 제공합니다.

프린터 정보유출방지
중요 정보가 인쇄되지 않게 정책에 따라서 인쇄할 내용을 필터링하고 감사 로그를 작성하는 로컬 및 네트워크 프린터 감시 기능입니다.

Active Directory
LDAP, LDAPS 등 지원. AD 싱크, AD 가져오기 기능. AD 그룹과 객체를 가져오거나 동기화 합니다. 에이전트는 AD 사용자 모드에서 동작합니다.

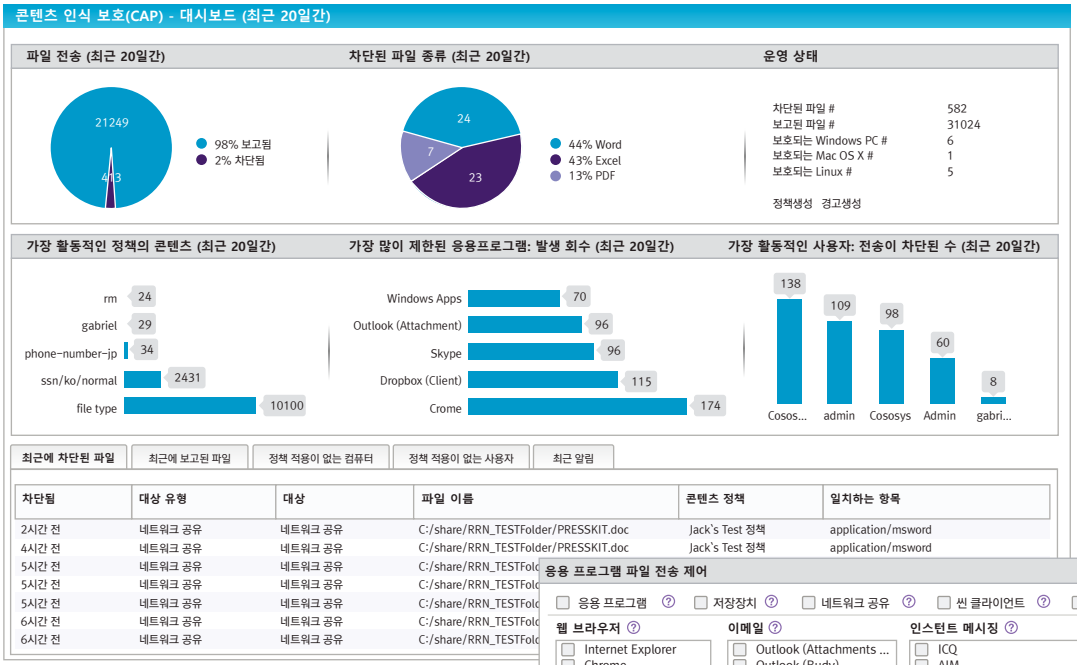
HIPAA 콘텐츠 인식 정책
문서의 전송 전에 PHI 정보, FDA가 허용한 약품, ICD-9 코드 등의 유무를 전문적인 심도로 검사합니다.

GDPR EU 일반정보보호 규정 지원
여러 유럽 국가의 언어 지원 및 개인 ID, 전화번호, 여권번호, 세금 ID, VAT ID, 건강보험 번호 등을 지원합니다.

씬 클라이언트 DLP
터미널 서버의 데이터를 보호하고, 씬 클라이언트 환경 및 RDP 환경에서 서버 자료의 전송을 관리하고 자료의 손실을 예방합니다.

ENDPOINT PROTECTOR 5

콘텐츠 인식 보호 (DLP)



DLP 파일 전송 제어

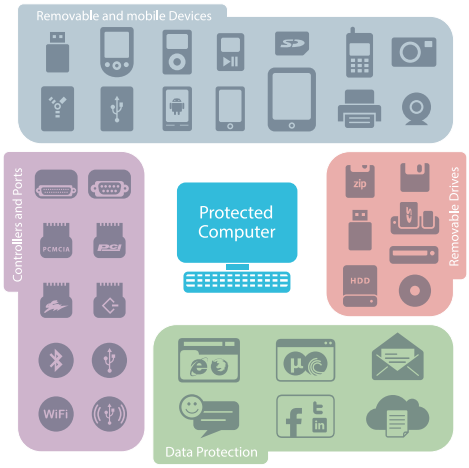
- 네트워크/저장장치 전송검사
- 보고, 차단, 보고 및 차단
- 파일의 종류에 따른 필터링
- 개인정보 여부에 따른 필터링
- 사용자 키워드로 필터링
- 정규식 필터링
- 반출 파일 크기 제한 설정
- 중요 정보의 프린팅 차단
- SIEM 로그 연동

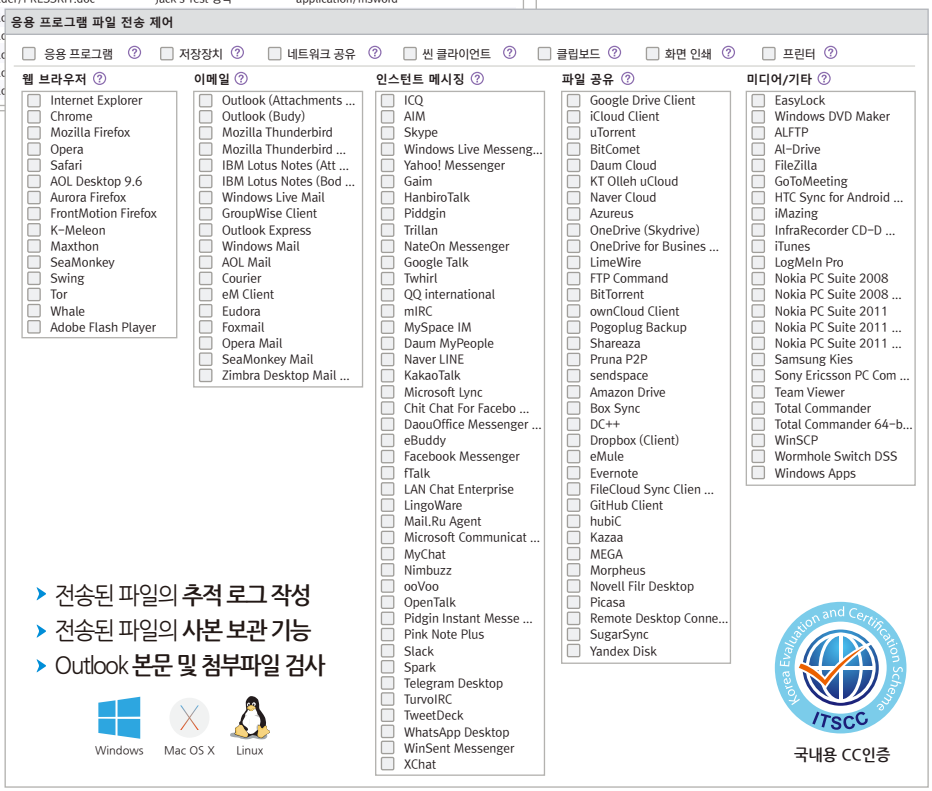
나라장터 국가종합전자조달

조달청 나라장터 등록제품

CONTENT AWARE PROTECTION

by ENDPOINT PROTECTOR



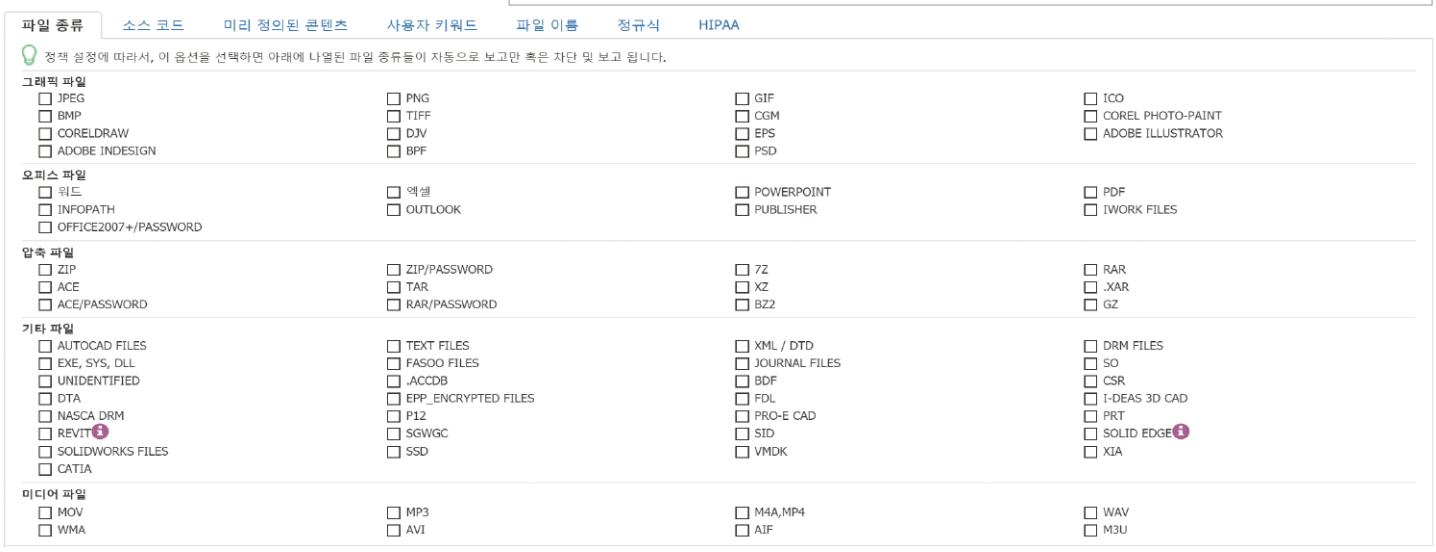


- 전송된 파일의 **추적 로그 작성**
- 전송된 파일의 **사본 보관 기능**
- Outlook **본문 및 첨부파일 검사**

Windows Mac OS X Linux

Korea Evaluation and Certification Scheme ITSCC

국내용 CC인증



eDiscovery

Windows, macOS, Linux 용

- 파일 유형: 그래픽 파일 / 오피스 파일 / 압축 파일 / 프로그래밍 파일 / 미디어 파일 등.
- 미리 정의된 콘텐츠: 신용카드번호 / 개인식별정보 / 주소 / 주민등록번호 / ID / 여권번호 / 전화번호 / 세금 ID / 건강보험번호 등,
- 사용자 키워드 / 파일 이름 / 정규식 / HIPAA / GDPR 지원

콘텐츠 및 파일 유형 검사

파일 유형, 미리 정의된 콘텐츠, 파일 이름, 정규식 또는 HIPPA 규정 콘텐츠를 기반으로 조직의 민감한 자료를 보호하기 위한 사용자 정의 eDiscovery 정책을 만듭니다. 정의된 컨텐츠에 따라 민감한 자료의 검색을 시작합니다.

저장 데이터 (Data at Rest) 암호화

기밀 자료가 발견되면 바로 허가되지 않은 직원 엑세스와 유출 가능한 데이터를 막기 위해 강력한 AES 256으로 암호화 할 수 있는 옵션이 있습니다.

저장 데이터 (Data at Rest) 삭제

회사 보안 정책에 위반되는 민감한 정보를 복구 불가능하게 완전히 삭제 함으로써 데이터를 보호하고 정보보호 규정을 준수합니다.

자동 검색

전체 검색 및 증분 검색에 추가하여 자동 검색을 만들 수 있습니다. 시간 또는 일정 주기(주 또는 월)로 수행할 수 있습니다.

검색 위치 블랙리스트

미리 정의된 디렉토리 위치 기반으로 필터를 만들 수 있습니다. 저장 데이터의 의미 없는 검사를 피하고 목표 콘텐츠 검사를 수행합니다.

검사 결과 내보내기

검사 결과를 Excel, PDF 또는 CSV 파일로 내보내고 관리 또는 감사 문서의 보고서로 사용할 수 있습니다. 검사 결과는 민감한 데이터를 저장한 컴퓨터, 민감한 데이터, 경로, 발견 시간, 암호화/삭제 또는 보고 여부 및 기타 중요한 정보를 제공합니다.

파일 유형 블랙리스트

파일 유형 블랙리스트는 네트워크의 엔드포인트에 저장된 특정 문서를 탐지할 수 있습니다. 그래픽 파일, 오피스 파일, 압축 파일, 프로그래밍 파일 등의 파일을 탐지합니다.

미리 정의된 콘텐츠 블랙리스트

이 블랙리스트는 신용카드번호, 주민등록번호, 여권권호, 전화번호, 개인식별정보 및 기타 개인정보 보호에 필요한 데이터를 추가해서 정책 위반 여부 및 파일 저장 위치를 검색합니다. PCI DSS, HIPAA, GDPR 등의 규정 준수를 돕습니다.

SIEM 통합

SIEM 솔루션을 연동해서 로그를 외부로 전송합니다. 원활한 사용자 경험을 제공합니다.

사용자 키워드 블랙리스트

키워드 및 표현 같은 사용자 정의 콘텐츠 기반으로 블랙리스트를 만듭니다. 다양한 블랙리스트 사전 내용은 복사/붙여넣기, 입력 또는 가져오기로 만들 수 있습니다.

CC인증을 받은 개인정보 삭제 및 암호화

주민등록번호, 운전면허번호, 여권번호, 건강보험번호, 신용카드번호, 전화번호 등 개인정보 처리

GDPR EU 일반정보보호 규정 지원

여러 유럽 국가의 언어 지원 및 개인 ID, 전화번호, 여권번호, 세금 ID, VAT ID, 건강보험 번호 등을 지원합니다.

HIPAA 규정 데이터

PHI 정보, FDA 승인 약품, ICD-10/ICD-9 코드 등을 기반으로 엔드포인트를 상세하게 검사합니다.
엔드포인트에 존재하는 기밀 의료 정보 탐지와 필요한 경우 삭제/암호화 같은 보호 조치로 HIPAA 규정을 준수합니다.

파일 이름 블랙리스트

파일 이름과 위치 기반으로 특정 파일을 검색합니다. 이 결과는 eDiscovery 검사 결과에서 파일 목록과 삭제/암호화/복호화 액션 여부와 함께 표시됩니다.

정규식 블랙리스트

향상된 사용자 정의 블랙리스트는 정규식을 사용하여 특정한 반복적인 패턴이 포함된 자료의 검색이 가능합니다.

파일 위치 블랙리스트 및 화이트리스트

내장 HDD 속의 위치에 따라서 필터링. 위치에는 하부 폴더들을 포함 미포함으로 설정 가능함.

MIME 유형 화이트리스트

생산성을 증가시키고 불필요한 검사를 피하기 위해 화이트리스트에 추가해서 검사에서 MIME 유형을 배제합니다. eDiscovery 정책을 효율적으로 관리합니다.

임계값

임계값 옵션을 사용해서 불필요한 검사를 회피합니다. 특정 위반으로 검사를 중지해야 할 때 또는 최소 파일 크기로 검사해야 하는 파일들을 지정할 수 있습니다.

분석 및 보고

eDiscovery 검색과 관련된 로그를 모니터링하고 필요하면 소명합니다. 로그 및 보고서는 SIEM 솔루션으로 내보낼 수도 있습니다.

다른 추가 기능 정보

당사의 웹사이트 www.cososys.kr을 방문
혹은 support@cososys.kr로 메일 주세요.

매체 제어
Windows, macOS, Linux 용

- USB 저장 장치
- CD, DVD, BR 드라이브
- 메모리 카드 리더
- 로컬 프린터
- Bluetooth 장치
- MP3 플레이어
- 외장 HDD
- Android MTP
- Android ADB, Teensy Board
- 디지털 카메라
- 웹캠
- Thunderbolt
- PDA
- 네트워크 공유 폴더
- FireWire
- iPhone
- iPad
- iPod
- ZIP 드라이브
- 시리얼 포트
- LPT 포트
- PCMCIA 저장 장치
- 생체인식 장치
- IrDA 동글
- 추가 키보드 및 BadUSB
- USB 테더링/모뎀
- 다른 여러가지 장치들 지원 및 신종 장치 업데이트 제공

전체 권한 설정
매체 제어를 위한 전체 기본 설정으로 네트워크를 통하여 연결된 모든 에이전트에게 전달 됩니다.
35 종 이상의 정교한 매체 제어를 제공합니다.

그룹 권한 설정
장치 권한은 그룹을 기반으로 세분화해서 구성할 수 있습니다. 여러 그룹에 다른 권한을 허용합니다.

컴퓨터 권한 설정
컴퓨터별로 장치 권한은 구성할 수 있습니다. 조직에서 컴퓨터에 예외 처리를 할 때 유용합니다.

사용자 권한 설정
역할 및 직무를 기반으로 각 사용자는 회사 정책에 따라 다른 장치 접근 권한을 부여 받을 수 있습니다.

장치 권한 설정
각각의 장치를 벤더 ID, 제품 ID, 일련 번호를 기반으로 장치별로 사용 정책을 설정 할 수 있습니다.

사용자 클래스
권한이 같은 제조업체 제품을 쉽게 관리하도록 사용자가 원하는 장치 클래스를 만들 수 있습니다.

Trusted Device
신뢰할 수 있는 암호화 저장 장치로, 사용 권한을 암호화 레벨에 따라 설정 할 수 있습니다.

오프라인 임시 암호
네트워크에 연결 안 된 컴퓨터에서 파일 전송을 임시로 허용하여 보안 및 생산성을 제공합니다.

파일 추적
USB 저장 장치 및 다양한 저장 장치에 대한 모든 파일 전송을 기록합니다. 데이터의 사용에 대한 확실한 기록을 제공합니다.

파일 보관
감사를 목적으로 제어되는 장치에 전송되는 파일의 복사본을 보관합니다.

근무시간 이후 정책
근무시간 이후에 적용되는 매체제어 정책을 설정할 수 있습니다. 근무시간은 출근 및 퇴근 시간과 근무 요일을 기반으로 설정합니다.

외부 네트워크 정책
컴퓨터가 회사 밖의 외부 네트워크에 있을 때 매체제어 정책을 설정할 수 있습니다.

사용자 및 컴퓨터 정보
매체의 사용자에 관한 가시성 확보를 위해서 사번, 팀명, 위치, 정확한 연락처 등 많은 정보를 수집 제공.

이메일 경고 만들기
미리 설정된 혹은 사용자가 정의한 경고 메일을 만들어서 시스템의 중요한 이벤트나 정보의 유출 발생과 같은 상황 정보를 제공합니다.

대시보드 및 그래픽
가장 중요한 이벤트와 통계에 대한 빠른 시각적 개요를 제공하는 그래픽 및 차트로 정보를 표시합니다.

보고 및 분석
로그 및 분석은 파일 전송에 관련된 활동을 모니터 합니다. 또한 SIEM 솔루션으로 로그를 내보낼 수 있습니다. 로깅 기능은 포렌직 수준의 자료를 제공합니다.

보안USB 암호화 기능
Windows, macOS 용

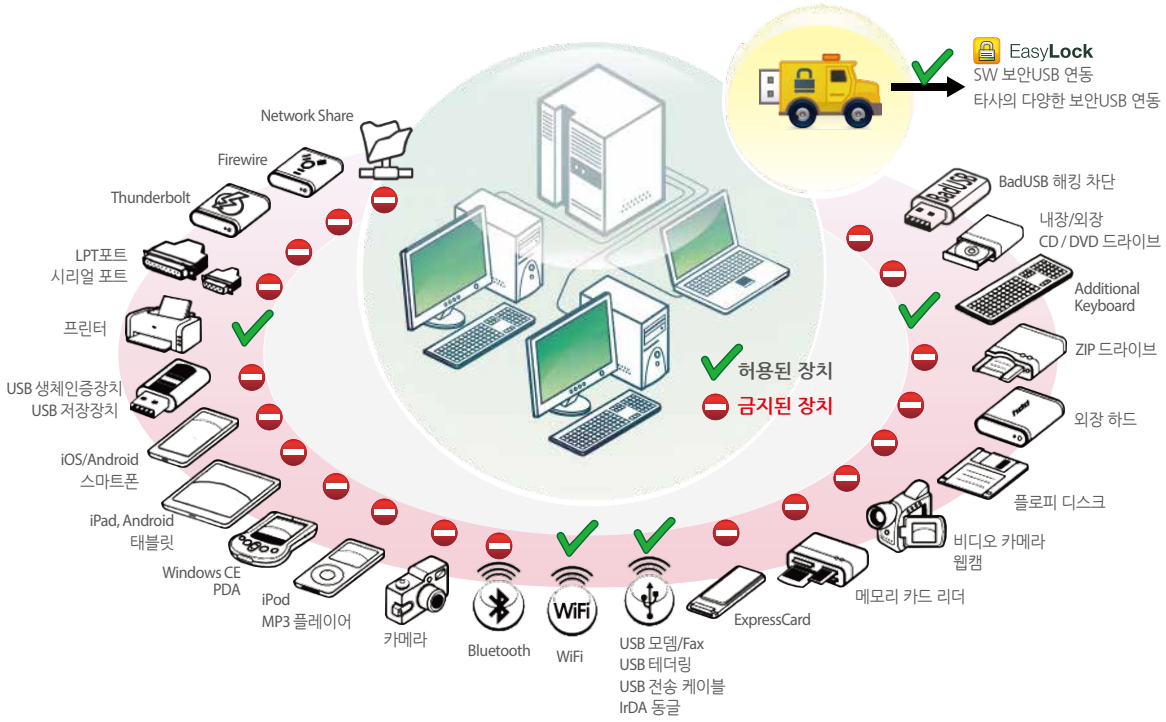
보안USB 사용 정책
보안USB 장치만 사용을 허가하고 복사된 모든 데이터는 자동 암호화로 보호됩니다.

강력한 암호화 메커니즘
군사용 수준의 AES 256bit CBC 모드 암호화를 사용하고, 국내용 CC인증 제품은 검정필 ARIA 256 블럭모드 암호화 기술를 사용합니다.

마스터 비밀번호
마스터 비밀번호 만들기는 사용자 비밀번호 재설정과 같은 다양한 환경에서 연속성을 제공합니다.

보안USB 중앙관리 기능
보안USB 사용자 관리, 원격 설치, 원격 초기화, 메시지 전송 내부 사용내용 로깅, 외부 사용내용 로깅, 사이트 라이선스

매체 제어 (Device Control)

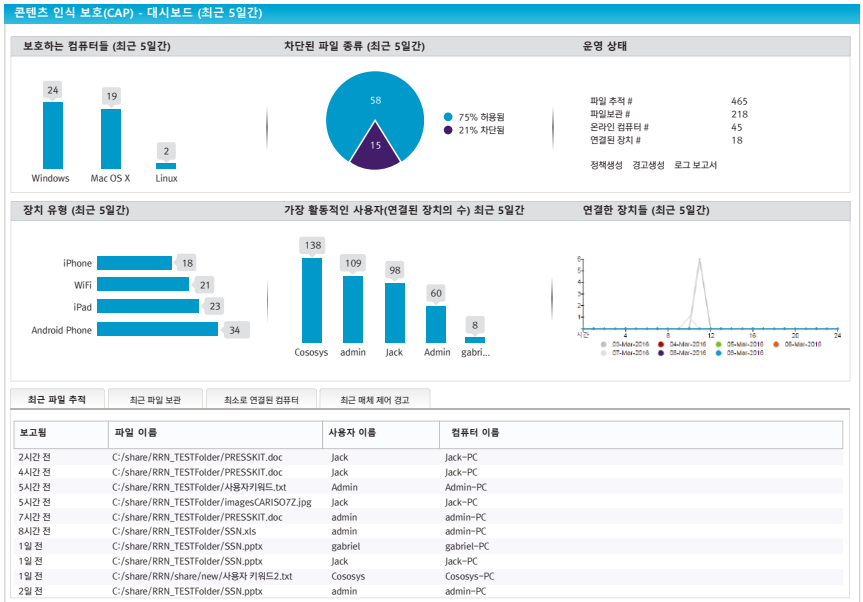


Windows 10, Windows Server, macOS, Linux
코소시스의 Endpoint Protector 5는 다양한 OS에서 정교한 매체제어를 제공합니다.

DEVICE CONTROL
by ENDPOINT PROTECTOR

정교한 매체 제어!

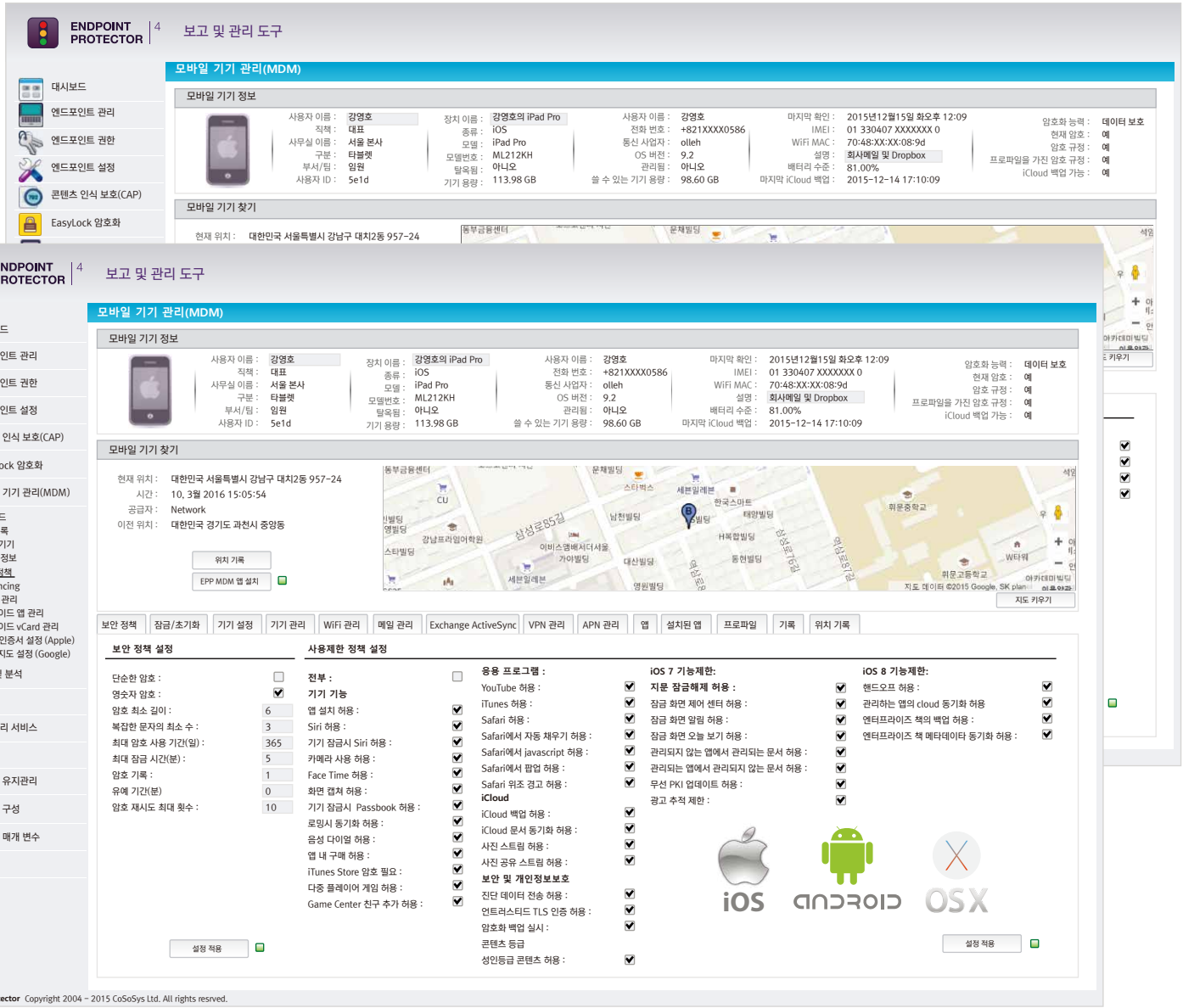
- USB로 연결되는 모든 장치를 통한 정보 유출 통제
- 스마트폰, 태블릿 등 다양한 스마트 기기를 제어
- 2G, 3G, 4G LTE 테더링 기기, USB 모뎀 등 제어
- 네트워크 공유 폴더 통제 및 파일 전송 내용 추적
- eSATA, Thunderbolt, FireWire 외장 하드 사용 추적
- 주변 장치를 통해서 반출된 파일 추적, 사본 보관
- SW 보안USB 연동 및 보안USB 사용 이력을 추적



제어되는 장치	Windows	Mac	Linux
알 수 없는 저장 장치	●	●	●
USB 저장 장치	●	●	●
CD/DVD RW 드라이브	●	●	●
내장형 카드 리더기	●	●	●
플로피 드라이브	●		●
네트워크 프린터	●	●	●
로컬 프린터	●	●	●
MTP	●	●	●
디지털 카메라 (PTP)	●	●	●
블랙베리	●		
스마트폰 (USB Sync)	●		●
스마트폰 (Windows CE)	●		
스마트폰 (Symbian)	●		●
웹캠	●	●	●
iPhone	●	●	
iPad	●	●	
iPod	●	●	
eSATA 컨트롤러	●		
WiFi	●	●	●
Bluetooth	●	●	●
FireWire 버스	●	●	
직렬 포트	●		
PCMCIA 장치	●		
MTD 방식 카드 리더	●		
SCSI 방식 카드 리더	●		
ZIP 드라이브	●		
Teensy 보드, ADB	●	●	
Thunderbolt	●	●	
네트워크 공유	●	●	
RDP 저장소	●		
IrDA 동글	●		
LPT 포트	●		
Additional Keyboard, BadUSB	●		
USB 테더링/모뎀	●	●	●
Chip Card Device (FIDO)	●	●	

ENDPOINT PROTECTOR 5

모바일 기기 관리 (MDM) 모바일 앱 관리 (MAM)



Endpoint Protector 장비의 모바일 기기 관리(MDM) 기능은 설치 과정없이 즉시 사용 가능합니다.

끊임 없이 업데이트 되는 새로운 스마트 기기 및 새로운 운영체제를 지속적으로 지원합니다.

모바일 보안 정책
기업의 중요한 정보가 담긴 모바일기기의 안전한 사용과 분실등의 위험을 관리함

MAM, 모바일 어플리케이션 관리
iOS 및 Android에서 기업에게 필요한 어플리케이션의 배포, 회수, 보안성 확보

암호관리 규정 준수
비밀번호가 취약한 기기를 정책으로 관리하여 보안 수준 규정 준수

분실된 기기의 추적 및 회수
분실 및 도난에 대비하여 기기의 위치를 추적하고, 기기에 문자를 보냄(iOS)

원격 잠금 및 초기화
분실된 모바일 기기를 원격 잠금 및 원격 초기화 하여 기업의 정보 보호

Geofencing 위치 정책
GPS 위치정보를 활용하여 미리 설정된 지역에서 지정된 기기 정책을 실행함

BYOD 환경 지원
개인 소유 기기를 활용한 모바일 오피스 구현에서 필수적인 관리 기능 제공

간편 다양한 기기등록
SMS, 이메일, QR코드 등 개별 기기등록 혹은 다수 기기 대량등록 가능함

Windows, Linux 서버용 정보 유출방지 (DLP)

대한민국에서 **5천개 이상의 서버를 보호**하고 있습니다!

Windows, Linux Server DLP 및 매체 제어
Endpoint Protector V5.0

나라장터 국가종합전자조달
조달청 나라장터 등록제품

중앙 집중식 매체 제어
- 자료유출 가능한 모든 주변장치 통제
- USB 포트, 메모리 카드리더 봉쇄
- 주변장치 접속/사용/차단 기록 로깅
- 정책에 따른 매체/장치의 사용 통제
- 네트워크 공유폴더 사용 추적/통제

네트워크 정보유출 감지
- 다양한 웹브라우저, 이메일 클라이언트, 각종 메신저, P2P, FTP 프로그램, 클라우드 서비스 등을 통한 자료 유출 차단
- 파일형식, 개인정보, 소스 코드, 키워드, 도메인 및 URL, 정규식을 통한 반출자료 감시 및 자료유출 차단

파일 추적 및 반출 파일 사본 보관
- 저장매체로 이동된 모든 파일 추적
- 네트워크 공유로 이동된 파일 추적
- 쓰기/읽기/복사/삭제/이름변경 등 파일 이벤트 기록
- 반출파일 사본 보관으로 감사 지원

개인정보, 키워드 등 내용인식 유출 차단
- 저장장치에 기록되는 파일들의 내용을 식별하여 중요 정보 검출 시에는 유출차단
- 자료 반출이 가능한 프로그램을 사용한 전송의 경우에도 규정위반을 검출하여 차단
- 한국, 미국, 중국 등 18 개국 개인정보 지원

미인가 장치 차단 및 조기 경보
- 정책적으로 허용되지 않는 장치 차단
- 외부 미등록 장치의 네트워크 침입탐지
- 자동경보 기능으로 즉각적인 보안대응
- SIEM 연동

응용 프로그램을 통한 파일 반출 차단
- 네트워크에서 사용이 허용되지 않은 프로그램을 통한 자료유출 검출 및 차단
- 반출 시도 확인 및 관심 파일들 로그 작성

모바일 기기 사용 통제
- 테더링을 통한 외부망 연결 차단
- MTP/PTP 연결 차단
- 외부 AP 연결 차단
- 모바일 기기 접속 감지, 사용로그 제공

클라우드 사용, RDP 및 터미널 서버 통제
- DropBox, OneDrive, Google Drive 등 클라우드 서비스 사용 통제
- 터미널 서버 및 RDP 스토리지 사용 추적 및 통제

BadUSB 해킹 공격 차단
- 정상적인 USB 장치로 위장된 해커의 키보드 매크로 공격을 차단
- 코소시스의 BadUSB 차단 기능은 IT 보안 인증사무국의 CC인증을 받았습니다.

IT보안인증사무국 CC인증
Endpoint Protector V5.0은 Windows 10을 대상으로 하여 매체 제어 제품 및 호스트 자료유출방지 제품으로 IT보안인증사무국의 국내용 CC인증을 완료했습니다.

제어되는 장치	Windows	Mac	Linux
알 수 없는 저장 장치	●	●	●
USB 저장 장치	●	●	●
CD/DVD RW 드라이브	●	●	●
내장형 카드 리더기	●	●	●
플로피 드라이브	●		●
네트워크 프린터	●	●	●
로컬 프린터	●	●	●
MTP	●	●	●
디지털 카메라 (PTP)	●	●	●
블랙베리	●		
스마트폰 (USB Sync)	●		●
스마트폰 (Windows CE)	●		
스마트폰 (Symbian)	●		●
웹캠	●	●	●
iPhone	●	●	
iPad	●	●	
iPod	●	●	
eSATA 컨트롤러	●		
WiFi	●	●	●
Bluetooth	●	●	●
FireWire 버스	●	●	
직렬 포트	●		
PCMCIA 장치	●		
MTD 방식 카드 리더	●		
SCSI 방식 카드 리더	●		
ZIP 드라이브	●		
Teensy 보드, ADB	●	●	
Thunderbolt	●	●	
네트워크 공유	●	●	
RDP 저장소	●		
IrDA 동글	●		
LPT 포트	●		
Additional Keyboard, BadUSB	●		
USB 테더링/모뎀	●	●	●
Chip Card Device (FIDO)	●	●	

지원되는 OS PC - Windows XP, Vista, 7, 8/8.1, Windows 10 Server - Windows 2003 ~ Windows 2012 R2, Windows 2016 (32/64) Mac OS X - 10.5 ~ 10.14 Linux - Red Hat, Ubuntu, CentOS, openSUSE, Oracle Linux, Fedora

macOS 정보유출방지 (DLP)

macOS 매체제어 DLP

주변 장치 / 매체 제어

- USB 저장 장치
- CD/DVD/BR 드라이브
- Thunderbolt 저장장치
- FireWire 저장장치
- Android MTP 장치
- iPhone, iPad, iPod
- 내장/와장 메모리 카드 리더
- 네트워크 프린터
- 로컬 프린터
- Bluetooth
  - 스마트폰 - 테블릿 - 라디오
  - 키보드 - 마우스
  - 기타 장치 (각 기기별 제어 가능)
- WiFi 장치
- 웹캠 (Webcam)
- Chip Card Device

내부정보유출방지 (DLP)

- 웹을 통한 자료유출 제어
- 이메일 첨부 파일 제어
- 인터넷 메신저 파일 전송 제어
- 클라우드 파일 동기화 제어
- MTP 파일 전송 제어
- AirDrop 파일 전송 제어
- 네트워크 공유 파일 전송 제어
- 파일 종류에 따른 차단 필터
- 개인정보유출 차단 필터
- 사용자 키워드 차단 필터
- 정규식을 사용한 차단 필터
- 소스 코드 인식 차단 필터
- 클립보드 내용 검사
- 외부 저장장치 파일 전송 필터
- 도메인 및 URL 블랙리스트
- 인터넷 정보 유출 감지/차단
- 반출된 파일의 추적 및 사본보관

USB 테더링, 스마트폰, 블루투스 등 무선장치 통제

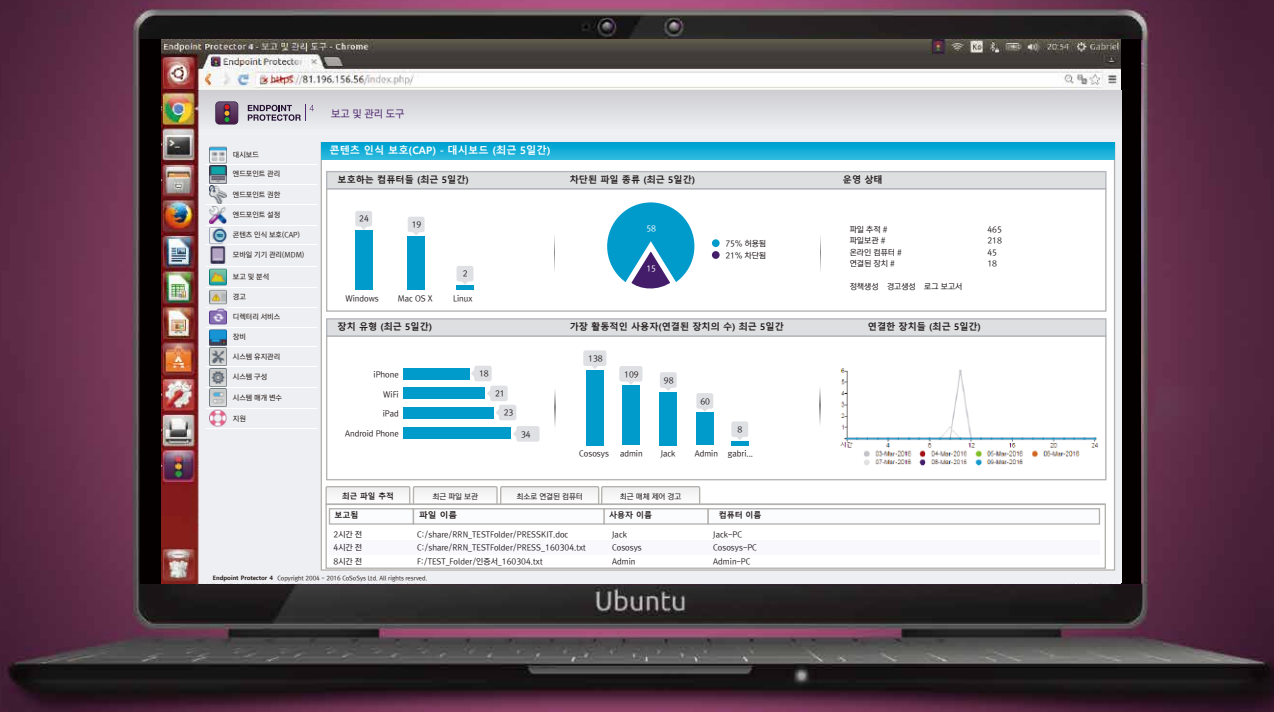
EasyLock SW 보안USB Win / Mac

- 중앙관리 콘솔 - 자동배포, 파기, 사용자관리
- 감사로그 - 사내 및 사외 사용이력 추적 로그
- 보안관리 - 분실된 보안USB 사용 시도 차단

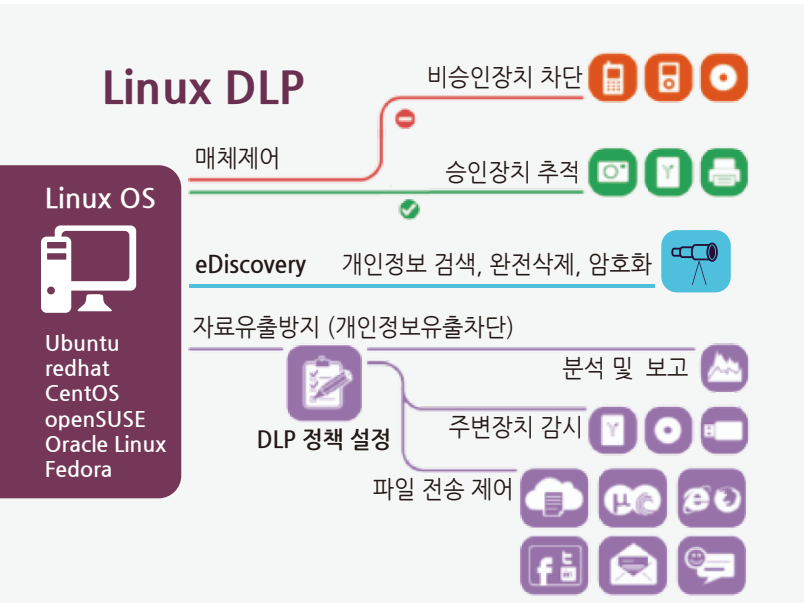
- Mac OS X 10.7 Lion
- Mac OS X 10.8 Mountin Lion
- Mac OS X 10.9 Maverick
- Mac OS X 10.10 Yosemite
- Mac OS X 10.11 El Capitan
- masOS 10.12 Sierra
- macOS 10.13 High Sierra
- macOS 10.14 Mojave

코소시스의 Mac DLP는 빠르고 지속적인 macOS의 버전 업데이트를 빠짐없이 꾸준하게 지원하고 있습니다.

멀티 OS 용 (Windows, Mac, Linux)
개인정보 검색, 완전삭제, 암호화 제공



Linux PC 및 Server에서 USB 저장장치, CD/DVD, 메모리 카드리더, Bluetooth 등 각종 주변 장치의
안전한 사용과 네트워크를 통한 웹, 이메일, 메신저, 클라우드 등의 내부정보 유출을 차단합니다!



주변 장치 / 매체 제어	컨텐츠 인식 보호 (DLP)
USB 저장 장치	Web 파일전송 제어
내장 CD/DVD/BR 드라이브	이메일 첨부파일 제어
내장 메모리 카드 리더	메신저 파일전송 제어
내장 플로피 드라이브	클라우드 서비스 전송 제어
네트워크 프린터	소스 코드 필터
로컬 프린터	토렌트, 팀뷰어 파일전송 제어
안드로이드 MTP	ADB, SCP, FTP, MC 파일전송 제어
디지털 카메라 (PTP)	반출파일 및 전송파일 로깅
스마트폰 (USB 동기화)	파일 종류 필터, 정규식 필터
노키아폰 (Symbian)	개인정보보호 필터
웹캠(Webcam)	사용자 키워드 필터
WiFi	USB 저장 파일 내용 검사
Bluetooth	개인정보 검색, 완전삭제, 암호화
USB 모뎀	클립보드 내용 검색

ubuntu redhat CentOS openSUSE fedora ORACLE LINUX

Ubuntu 12.04/14.04/16.04/18.04 LTS, redhat 7.0+, CentOS 7.0+, openSUSE 11.4, 12.2, leap 42+, Fedora 26/27, Oracle Linux 6.5 (다른 배포판은 상담이 필요함)

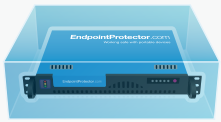
100% 모든 고객의 필요에 적합

어떤 유형의 네트워크에도 적합하기 때문에 코소시스의 제품은 대기업, 중소 비즈니스, 소규모 사업자 및 개인이 사용할 수 있습니다. 클라이언트 - 서버 구조로 장비로 제공이 되어 설치가 매우 쉽고 웹 기반 인터페이스로 중앙 관리합니다. 하드웨어 및 가상 어플라이언스, 클라우드 버전 이외에 기본 매체 제어 기능에 충실한 독립 설치형 SW버전이 있습니다.

Endpoint Protector

매체 제어, 콘텐츠 인식 보호 (DLP), 보안USB 기능을 Windows, Mac, Linux 운영체제 컴퓨터에서 사용 가능합니다.
모바일 기기 관리 및 모바일 앱 관리는 또한 iOS와 Android 모바일 기기에서 사용 할 수 있습니다.

하드웨어 어플라이언스



가상 어플라이언스

My Endpoint Protector

매체제어, 콘텐츠 인식 보호 기능을 Windows와 macOS 운영체제 컴퓨터에서 사용 가능합니다. 선택 옵션으로 SW 보안USB 연동을 추가 할 수 있습니다.

국내 여러 기업들의 선택을 통해 서비스의 보안성, 안정성, 기밀성에서 신뢰를 받고 있는 클라우드 서비스로 제공하고 있습니다.

https://my.endpointprotector.com
위 사이트에서 클라우드 DLP 및
클라우드 MDM을 확인하세요.

Cloud Solution

사용가능한 OS

보호되는 엔드포인트

			DLP	eDiscovery	매체 제어	보안USB	MDM
Windows	Windows XP / Windows Vista	(32/64 bit)	●	●	●	●	
	Windows 7 / 8 / 8.1 / 10	(32/64 bit)	●	●	●	●	
	Windows Server 2003-2016 R2	(32/64 bit)	●	●	●	●	
macOS	Mac OS X 10.7	Lion	●	●	●	●	●
	Mac OS X 10.8	Mountain Lion	●	●	●	●	●
	Mac OS X 10.9	Mavericks	●	●	●	●	●
	Mac OS X 10.10	Yosemite	●	●	●	●	●
	Mac OS X 10.11	El Capitan	●	●	●	●	●
	macOS 10.12	Sierra	●	●	●	●	●
	macOS 10.13	High Sierra	●	●	●	●	●
	macOS 10.14	Mojave	●	●	●	●	●
Linux	Ubuntu		●	●	●	n/a	
	openSUSE		●	●	●	n/a	
	CentOS / RedHat		●	●	●	n/a	
	Fedora		●	●	●	n/a	
	Oracle Linux		●	●	●	n/a	
iOS	iOS 6, iOS 7, iOS 8, iOS 9, iOS 10, iOS 11, iOS 12 및 상위 버전						●
Android	Jelly Bean (4.1+), KitKat (4.4+), Lollipop (5.0+), Marshmallow (6.0+), naougat (7.0+), Oreo (8.0+) 및 상위 버전						●

*일부 배포판에 한해 지원되지 않을 수도 있습니다. 사용하는 리눅스 버전을 확인하여 주십시오. support@cososys.kr

COSOSYS

www.cososys.kr

	한국	독일
이메일	support@cososys.kr	vertrieb@endpointprotector.de
영업팀	070 4633 3090	+49 7541 978 26730
지원팀	070 4633 0353/4	+49 7541 978 26733

	루마니아	북미
이메일	sales@cososys.com	sales.us@endpointprotector.com
영업팀	+40 264 593 110 / ext. 103	+1 888 271 9349
지원팀	+40 264 593 113 / ext. 202	+1 877 377 6475

(주)코소시스코리아에서 공급하는 DLP 제품은 국내용 CC인증을 획득한 국산 장비입니다.

코소시스 파트너