ENDPOINT PROTECTOR | 4

코소시스의 Mac OS X DLP 장비는 매체 제어, 호스트 자료유출방지, SW 보안USB 및 개인정보 유출 차단 기능을 제공하여 Mac OS X를 이용하는 기업의 중요한 내부정보를 분실, 유출 및 도난의 위험에서 보호합니다.

많은 기업에서 Mac 시스템의 도입이 점차 늘고 있지만, 중요한 자료의 유출을 방지하는 보안 조치는 Windows 시스템 컴퓨터의 높은 보안성과 비교하면 매우 낮은 위험한 상황입니다.

Mac 시스템이 다루는 자료의 안정성을 확보하고 자료 유출 위험에서 보호하는 것이 정보보안을 담당하는 IT 부서의 최우선 순위 과제 중 하나가 되었습니다.

Endpoint Protector의 Mac 자료유출방지(DLP) 솔루션은 세계적으로도 유일한 Mac OS X용 DLP 제품으로 매체 제어는 Mac 시스템의 USB부터 다른 모든 주변 장치 및 CD/DVD 등의 매체 사용까지, 콘텐츠 인식 보호 기능은 웹브라우저 및 이메일 클라이언트, 인터넷 메신저, iCloud, Dropbox 등의 클라우드 서비스, iTunes 및 AirDrop 차단 등 자료 유출이 가능한 여러 경로를 차단하고 중요한 자료를 보호합니다.

Endpoint Protector는 전원을 켜는 즉시 사용이 가능한 DLP 보안 장비(Appliance)입니다. 복잡한 설치 과정 없이 정보보안 관리자는 이 장비를 사용하여 Mac 정보보안 정책을 실행하기 위한 주변 장치 및 매체 사용 그리고 각종 응용 프로그램의 파일 전송 제어를 위한 강력한 권한을 가지게 됩니다. 전사, 그룹, 특정한 Mac 컴퓨터 혹은 사용자를 위한 보안 정책 설정 및 다양한 예외 처리가 가능하고, 파일의 종류, 개인정보보호법에서 규정한 보호대상인 개인정보, 사용자 정의 키워드 사전 및 정규식 등을 사용하여 중요한 자료를 정의하고 이동 경로를 감시하거나 차단 할 수 있습니다.

다양한 파일 종류에 관한 DB 구축으로 정확하게 자료 파일을 구별 해서 특정 종류의 파일을 보호할 수 있고, 키워드 사전에 정의된 단어들, 신용카드 번호나 주민등록번호와 같은 민감한 개인정보 등을 DLP 정책에 적용하여 중요한 자료를 식별하고 실시간으로 유출을 차단합니다.

"Endpoint Protector DLP 솔루션을 도입한 이후 저는 한결 더 편해졌습니다. 우리 스튜디오에서 원본이나 편집된 동영상을 USB 저장장치나 DVD를 이용해서 훔친다는 것이 이론적으로도 불가능하다는 것을 알고 있는 것은 좋은 일이죠."

Mafilm Audio사 전무이사

주요 장점들

- Mac OS X, Windows PC, Windows Server, Linux* 환경 모두 지원
- 중요 파일의 유출 보고 및 차단, 반출 파일 보관 및 감사 로깅
- 매체 사용 및 인터넷 파일 전송 정책 설정 및 실행
- 오프라인 중 보호 및 오프라인 운영을 위한 임시 암호 기능
- 웹 기반의 직관적인 관리 및 보고 인터페이스
- Mac OS X 엔드포인트 유출사고에 선제적인 대응
- 주변기기 오남용 및 중요 자료의 도난을 예방
- 하드웨어 장비 또는 가상 어플라이언스로 즉시 설치
- AWS 제공으로 아마존 EC2 서비스로도 즉각적인 설치 가능
- VMware, Hyper-V Ready

Mac 에서 제어 가능한 응용 프로그램 및 주변 장치

- 이메일 클라이언트
  - Mail, Outlook, Opera Mail
  - Thunderbird, Postbox 등
- 웹 브라우저들
  - Safari, Chrome, Firefox
  - Opera, Camino, SeaMonkey
  - Maxthon, OmniWeb 등등
- 클라우드 서비스 / 파일 공유
  - Dropbox, iCloud, OneDrive
  - Google Drive, Evernote, 등
- 인터넷 메신저
  - iMessage, Skype, AIM
  - Daum MyPeople, Kakao Talk
  - LINE, NateOn Messenger
  - Telegram Desktop, Adium
  - QQ메신저, Yahoo 메신저 등
- 기타 응용 프로그램들
  - AirDrop, iTunes
  - Android File Transfer
  - GitHub, Team Viewer 등 다수
- 매체 제어 및 주변 장치 제어
  - USB 저장 장치
  - Android 기기 (MTP 포함)
  - USB 플래시 드라이브
  - Thunderbolt 저장 장치
  - FireWire 장치
  - iPhones / iPads / iPods
  - 메모리 카드 (SD, CF 등등)
  - 메모리 카드 리더 (내장, 외장)
  - CD/DVD 버너 (내장, 외장)
  - 외장 HDD
  - 로컬 프린터
  - 웹캠
  - WiFi 네트워크 카드
  - 디지털 카메라
  - 스마트폰
  - MP3 플레이어 / 미디어 플레이어
  - Bluetooth 장치들
  - 네트워크 공유 필터링

2015 Computing Security Awards
WINNER
DLP Solution of the Year
Endpoint Protector 4
Computing Security Awards
2015 올해의 DLP 솔루션상
2년 연속 수상

Info Security Products Guide 2015
GLOBAL EXCELLENCE
GOLD
2015 Global Excellence Awards
자료 유출 보호/유출 예방 부문
금상 수상

Mac

개인정보보호법 규정 개인정보 및 카드 정보 등 중요 민감 정보 필터링

주민등록번호, 건강보험번호, 운전면허번호, 여권번호, 전화번호 등 개인정보 혹은 사용자 키워드 사전 및 정규식 등을 필터로 사용하여 보호된 엔드포인트에서 자료 파일이 전송될 때에 파일을 필터링합니다. 미리 정의된 콘텐츠 형식은 다음과 같습니다 :

- 신용카드 세부사항(CCN) 주요 카드사들 번호, 국제계좌 번호 형식 탐지
- 주민등록번호 및 12개 국가의 사회보장번호(SSN) 및 ID 등을 탐지
- 대한민국 및 여러 나라의 전화 번호, E-mail 주소 및 기타 개인민감 정보 등등

파일의 종류를 분석하여 확장자를 기준으로 필터링

Endpoint Protector는 실제로 분석하여 얻은 파일 종류를 기준으로 하여 파일 전송을 통제합니다. 대표적으로 Office 파일(한컴오피스 포함), 그래픽 파일, 압축 파일, 실행 파일, 미디어 파일. DRM 파일, 각종 캐드 파일 등을 지원합니다.

사용자 키워드 사전을 기준으로 필터링

콘텐츠 인식 보호 기능은 주어진 키워드를 비교 검사해서 키워드가 포함된 자료의 유출이나 도난을 방지합니다. 여러 개의 사용자 지정 키워드 사전을 전송 차단 정책 설정을 위해서 만들어 사용 할 수 있습니다.

클립보드를 사용한 복사 및 붙여넣기 기능 통제

클립보드 기능의 검사를 통해 중요한 회사의 정보들이 복사 및 붙여넣기 행위로 유출 되는 것을 감시합니다. 클립보드의 사용을 통제하면 중요한 자료들을 웹메일이나 온라인 게시판 등에 붙여넣기 하는 사용자들의 위험한 행동을 중단시킬 수 있습니다.

웹 브라우저를 통한 자료 유출 필터링

인터넷을 통하여 다양한 웹 서비스가 제공 되고, Safari, Firefox, Chrome, Opera 등의 여러가지 웹 브라우저가 활용 되면, Mac 사용자들은 접근 권한이 있는 어떠한 파일도 자유롭게 업로드 할 수 있습니다. 파일을 업로드 할 수 있는 많은 웹 사이트들 예를 들면 sendspace.com 혹은 Dropbox의 웹 인터페이스 등을 통한 자료 파일 절취도 많이 발생합니다. 따라서 중요한 파일이 웹 브라우저를 통해서 인터넷으로 나가기 이전에 웹 브라우저 쪽에서 모든 중요한 파일의 접근을 통제하는 것이 매우 중요합니다. 이것은 오직 Endpoint Protector의 Mac DLP 기능으로만 통제 가능하고, 게이트웨이에서 자료 유출을 방지하는 방법으로는 해결하기가 매우 어려운 문제입니다.

여러 응용 프로그램을 통한 자료 유출 필터링

Endpoint Protector는 Skype, Yahoo 메신저, 카카오톡, 다음 마이피플, 네이버 라인, 네이트온 메신저 등과 같은 여러 메신저, Android File Transfer, AirDrop, bitTorrent, GitHub 클라이언트 등의 응용 프로그램을 통한 자료 유출을 실시간 감지하여 중요한 파일의 전송을 필터링하여 안전하게 보호합니다.

이메일 첨부를 통한 중요 자료의 유출 방지

Mac 시스템에서 이메일의 첨부 파일로 중요한 자료들이 전송되는 것을 차단하거나 감시합니다. 콘텐츠 인식 보호 기능은 가장 많이 쓰이는 이메일 클라이언트인 Mail, Outlook, Thunderbird, Opera Mail, Postbox 외 다수의 메일 앱을 지원합니다.

매우 유연한 정보보안 정책 운용

콘텐츠 인식 보호 정책은 사용자, 컴퓨터, 그룹 또는 독립부서에 선택적으로 적용 할 수 있어서 반출 문서 검열 정책에 유연한 통제력을 제공합니다.

정책 작성 | 민감한 자료를 정의 | 자료 이동 실시간 검사 | 자료 유출 차단

Mac OS X 및 Windows Bootcamp 사용자 관리

가장 중요한 이 두 플랫폼들은 흔하게 동시에 사용이 됩니다. 중요한 내부 자료의 흐름을 파악하고 유출을 차단하기 위해서 두 플랫폼 모두를 동시에 보호합니다.

보호되는 엔드포인트 클라이언트

- Mac OS X 10.5+ (Mountain Lion 및 상위 버전)
- Windows 10 (32/64bit)
- Windows 8 / 8.1 (32/64bit)
- Windows 7 (32/64bit)
- Windows Vista (32/64bit)
- Windows XP SP3 (32/64bit)
- Windows 2003 / 2008 R2 / 2012 R2 (32/64bit)
- openSUSE 12.1, Ubuntu 14.04 LTS, CentOS 7

모바일 기기 관리 기능(MDM) 옵션 제공

- iPad, iPhone, iOS 5 이상
- Mac OS X 10.5 이상
- Android 2.3 이상 버전. 기기 암호화는 Android 4 이상 버전만 가능함.

디렉터리 서비스 (필수 아님)

Active Directory 가져오기, 동기화 하기

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

모바일 기기 관리 (MDM) 기능으로 Mac OS X 관리

모바일 기기 관리 기능은 Mac OS X 시스템을 관리 할 수 있습니다. 이렇게 하면 강화된 보안정책을 적용할 수 있습니다. FileVault2를 사용한 디스크 암호화, 분실 Mac 초기화, 원격잠금 및 원격삭제 기능은 분실 혹은 도난된 Mac 시스템에 중요한 정보가 있는 경우 매우 유용합니다.
또한 WiFi, VPN, 메일 설정 관리 등이 가능하고 설치된 앱을 확인 할 수 있습니다.

가상 어플라이언스 선택 가능

Endpoint Protector 가상 어플라이언스는 VMX, OVF, VHD 등의 포맷을 지원해서 대부분의 기업용 가상화 플랫폼에서 사용할 수 있습니다.

vmware READY

amazon web services™

Amazon 웹 서비스 EC2 가상 DLP 어플라이언스

Amazon 웹 서비스 위에서 Endpoint Protector는 EC2 인스턴스를 사용하여 가상 DLP 장비로 제공 될 수 있습니다.

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.

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

Endpoint Protector는 다른 어떤 제품도 추가로 구매할 필요가 없습니다.
Windows Server, SQL, CAL, HW, HDDs 등의 구매가 필요 없습니다.

Korea Evaluation and Certification Scheme ITSCC

국내용 CC인증, DLP 전문 기술 파트너 :

COSOSYS

2016년 2월 23일 수정됨.