ENDPOINT PROTECTOR | by CoSoSys

DATASHEET 5.9.0.0

내부정보 유출 방지 (DLP)

모든 조직을 위한 엔터프라이즈 보안 솔루션

Windows, macOS, Linux 용 DLP

전체 네트워크 보호

ENDPOINT PROTECTOR | by CoSoSys

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

업무의 생산성과 편의성을 유지하면서 내부자 위협에서 기밀 데이터를 보호하도록 디자인되었습니다.

Endpoint Protector는 Windows, macOS, Linux 용 컴퓨터, 씬 클라이언트, DaaS (Desktop-as-a-Service) 솔루션을 위한 엔터프라이즈 등급 DLP 장비입니다. 회사의 멀티 OS 네트워크를 위한 이상적인 솔루션으로 특정 니즈를 위한 모듈 형식으로 다양한 기능을 제공합니다.

코소시스 솔루션을 사용하는 조직은 개인 정보를 보호하고 GDPR, HIPAA, LGPD, CCPA, PCI DSS 등의 규정을 준수할 수 있습니다. 또한 Endpoint Protector는 회사의 영업 비밀 및 지적 재산을 보호하는 기능을 제공합니다.

매제 제어

데이터 도난 및 자료 유출 보호 를 위해서 USB 및 주변 장치를 차단, 제어, 모니터링 합니다. 장치, 사용자, 컴퓨터, 그룹, 구분으로 권한을 설정할 수 있습니다.

Windows / macOS / Linux

콘텐츠 인식 보호 (CAP)

이동 데이터 (Data in motion)를 모니터링 또는 제어해서 기밀 파일의 전송을 결정할 수 있습니다. 필터는 파일 유형, 응용프로그램, 사용자 정의 콘텐츠, 정규식 등으로 설정 가능합니다.

Windows / macOS / Linux

암호화 정책 보안USB

AES 256bit로 USB 저장 장치에 복사되는 보안 데일터를 자동으로 암호화 합니다. 크로스 플랫폼의 패스워드 기반으로 쉽고 효율적으로 사용할 수 있습니다.

Windows / macOS

eDiscovery

네트워크 엔드포인트의 저장 데이터 (Data at Rest) 검색해서 인가되지 않은 컴퓨터에 기밀 데이터가 발견되면 암호화 또는 삭제 조치를 할 수 있습니다.

Windows / macOS / Linux

주요 장점

쉬운 설치 및 관리

Endpoint Protector는 30분만에 바로 운영할 수 있고 전문가 및 비전문가 모두 쉽게 관리할 수 있습니다.

미리 정의된 규정 준수 프로파일

미리 정의된 보호 정책을 사용해서 GDPR, CCPA, HIPAA, PCI DSS 등 규정 준수 요구 사항 보장 및 데이터를 쉽게 찾을 수 있습니다.

크로스 플랫폼 보호

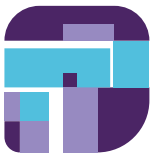
솔루션은 Windows, macOS, Linux 컴퓨터에 같은 수준의 기능과 보호를 제공합니다. 또한 ARM 기반의 M1 프로세서 Apple 기기를 지원합니다.

사용자 활동 상세 보고

Endpoint Protector로 누가 어디로 민감한 데이터를 전송하는지 추적 및 보고가 가능합니다. 이에 관련된 인사이트를 얻을 수 있습니다.

배포 옵션의 유연성

Endpoint Protector는 회사의 기존 인프라 또는 필요에 따라 다양한 방법으로 배포 할 수 있습니다.



세부적인 정책

이동식 저장 장치 및 주변 장치에 대한 세부적인 접근 권한 뿐만 아니라 사용자, 컴퓨터, 그룹에 대한 보안 정책을 쉽게 정의 할 수 있습니다.

엔터프라이즈 DLP

디지털 전환 및 WSC (Workstream Collaboration Platforms) 시대에서 데이터 손실과 규정 미준수 위험을 해결하는 것은 기업에 있어서 필수입니다. 데이터 위반의 결과는 막대한 벌금 뿐만 아니라 법률적 문제와 평판 훼손도 포함되기 때문입니다.

Endpoint Protector 엔터프라이즈는 마켓에서 더 효과적인 데이터 보안 솔루션으로 기업은 어디에서나 보호가 필요한 데이터를 지속적으로 식별, 모니터링, 제어 할 수 있습니다.

사용자 교정

Endpoint Protector 엔터프라이즈는 보안 정책을 더 유연하게 운영합니다. 사용자 교정 기능을 통해서 최종 사용자는 자체적인 수정이 가능합니다. 이는 자신의 활동에 정당성을 확인한 후에 정의된 시간 동안 특정한 민감한 정보의 전송을 허용합니다.

관리 콘솔

DLP 정책은 강력한 사용자 경험을 제공하는 Endpoint Protector 중앙 대시보드에서 전체 네트워크에 쉽게 설정 할 수 있습니다.

원활한 통합

당사의 솔루션은 AD (Active Directory) 및 SIEM (Security Information & Event Management) 기술 연결을 제공합니다.

SIEM 연결은 활동 이벤트를 보고 및 분석을 위한 SIEM 서버에 전송을 허용합니다. AD 를 이용하여 대규모 배포를 더 간단하게 할 수 있습니다.

매체 제어

Windows, macOS , Linux 용

USB 저장장치 / 프린터 / Bluetooth 장치 / CD 및 DVD / 외장 HDD / Teensy 보드 / 디지털 카메라 / 웹캠 / Thunderbolt / WiFi / 네트워크 공유 / FireWire / iPhone / iPad / iPod / ZIP 드라이브 / 카드 리더 / Android 스마트폰 / USB 모뎀 / 기타 - 지원 및 신종 장치, 업데이트 제공

세부적인 권한 설정
장치 권한은 그룹, 컴퓨터, 사용자, 장치 별로 전체 설정이 가능합니다. 기본 설정을 사용하거나 필요에 따라 조정해서 사용하시기 바랍니다.

장치 유형 및 특정 장치
권한 설정 - 사용 거부, 사용 허용, 읽기 전용 등. 권한은 장치 유형 또는 VID, PID, 시리얼 번호 기반으로 특정 장치에 적용할 수 있습니다.

사용자 클래스
같은 제조업체 장치를 더 쉽게 관리하기 위해서 VID, PID, 시리얼 번호 기반으로 장치 권한을 적용합니다. 사용자가 원하는 클래스를 만듭니다.

근무외 시간 정책
근무외 시간에 적용되는 매체제어 정책을 설정할 수 있습니다. 근무시간은 출근 및 퇴근 시간과 근무 요일을 기반으로 설정합니다.

외부 네트워크 정책
회사 네트워크 외부에있을 때 외부 네트워크 정책을 적용할 수 있습니다. FQDN 및 DNS IP 주소를 기반으로 적용합니다.

Active Directory 동기화
대규모 배포를 더 간편하게 할 수 있는 AD 장점을 이용합니다. 네트워크 그룹, 컴퓨터, 사용자를 반영해서 최신 객체를 유지하시기 바랍니다.

사용자 및 컴퓨터 정보
사번, 팀, 위치, 정확한 연락처 및 기타 (IP, MAC 주소 등) 정보로 사용자 가시성을 확보합니다.

파일 추적
다양한 장치에 대한 모든 파일 전송 또는 시도를 기록합니다.사용자 행동을 명확하게 파악할 수 있습니다.

파일 보관
감사 목적으로 제어되는 장치에 전송되는 파일의 복사본을 보관합니다.

오프라인 임시 암호
네트워크가 연결되지 않은 컴퓨터에 파일 전송을 임시로 허용합니다. 보안과 생산성을 보장합니다.

이메일 경고 만들기
회사 컴퓨터에서 사용되는 이동식 매체에 관련된 다양한 이벤트를 위한 실시간 이메일 경고를 만들 수 있습니다.

대시보드 및 그래픽
가장 중요한 이벤트 및 통계를 빠르게 시작적으로 보여주는 그래픽과 차트를 사용할 수 있습니다.

보고 및 분석
강력한 보고 및 분석 도구로 장치 사용에 관련된 모든 행동을 모니터링 합니다. 로그 및 보고서를 내보내기 할 수 있습니다.

전송 제한
특정 시간 간격 내에서 전송 제한을 설정합니다. 파일 수 또는 파일 크기 기반으로 설정이 가능합니다. 제한에 도달하면 이메일을 통해서 경고를 받을 수 있습니다.

SW 보안USB 암호화 정책

Windows, macOS 용

256bit AES 암호화 / Anti-tampering 기술 / 중앙 비밀번호 관리 / 사용자에게 메시지 보내기 / 원격 초기화 / 비밀번호 정책 설정 / 기타

SW 보안 USB 암호화 정책
암호화된 USB 장치만 인가하고 이러한 이동식 저장 장치에 복사되는 모든 데이터는 자동으로 보호가 됩니다.

자동 배포 및 읽기 전용
자동 및 수동 배포 모두 사용이 가능합니다. 암호화가 필요할 때까지 읽기 전용만 허용하는 옵션을 사용할 수 있습니다.

복잡한 마스터 및 사용자 비밀번호
비밀번호 복잡성을 필요할 때 설정할 수 있습니다. 마스터 비밀번호는 사용자 비밀번호 초기화와 같은 상황에 사용 연속성을 제공합니다.

비밀번호 관리 및 원격 초기화
사용자 비밀번호를 원격으로 변경하고 장치가 보안 위험에 있는 경우에 원격으로 초기화합니다.

콘텐츠 인식 보호 (CAP)

Windows, macOS, Linux 용

이메일 클라이언트: Outlook / Thunderbird / Apple Mail • 웹브라우저: Internet Explorer / Firefox / Chrome / Safari • Instant Messaging: Skype / Slack / WhatsApp • 클라우드 서비스 및 파일 공유: Dropbox / iCloud / OneDrive / BitTorrent / AirDrop • 기타 응용프로그램: iTunes / FileZilla / SFTP / Total Commander / TeamViewer / 기타

엔드포인트 거부목록

모니터링되는 다양한 응요프로그램 목록 기반으로 필터 설정이 가능합니다. USB 저장장치, 네트워크 공유, 다른 기타 엔드포이트를 모니터링합니다.

파일 종류 거부목록

파일 종류 필터는 실제 파일 유형 기반으로 문서를 차단하는데 사용할 수 있습니다. 심지어 사용자가 확장자를 변경해도 차단이 됩니다.

광학 문자 인식 (OCR)

사진 및 이미지 콘텐츠를 검사하고 스캔된 문서나 다른 비슷한 파일의 기밀 정보를 탐지합니다.

미리 정의된 콘텐츠 / 사용자 키워드 거부목록

사용자 정의 키워드 및 표현, 신용카드번호 또는 주민등록번호와 같은 미리 정의된 콘텐츠 기반으로 필터를 만들 수 있습니다.

파일 이름 거부목록

파일 이름 기반으로 필터를 만들 수 있습니다. 이름 또는 확장자 기반으로만 설정이 가능합니다.

파일 위치 거부목록 및 허용목록

로컬 HDD의 파일 위치 기반으로 필터를 설정합니다. 하위 폴더 포함 또는 제외 여부를 선택할 수 있습니다.

정규식 거부목록

표준 정규식을 사용해서 패턴을 정의하고 전송된 파일을 검사하는 강력한 도구입니다.

근무외 시간 및 외부 네트워크

근무외 시간 또는 외부 네트워크에서 적용되는 정책 정의 및 대비책입니다.

도메인 및 URL 허용목록

사내 보안 정책을 강화하는 동시에 직원에게 업무 유연성을 부여합니다. DPI 기능을 사용해서 회사 포탈 또는 이메일 주소 허용목록을 만듭니다.

프린트 스크린 및 클립보드 모니터링

스크린 캡쳐를 못하게 합니다. 데이터 보안 정책을 강화하는 복사 / 붙여넣기를 통한 민감한 콘텐츠의 데이터 유출을 보호합니다.

사용자 교정

사용자가 DLP 정책을 안전하게 재정의 할 수 있는 권한을 부여하고 데이터 전송의 정당화하는 옵션을 제공합니다. 조직 내에서 민감한 데이터 전송에 대한 최종 사용자의 책임감과 인식을 지원합니다.

SIEM 서버

로그를 외부로 보내는 SIEM (Security Information and Event Management) 서버와 연동합니다. 보안 제품의 연속적인 경험을 제공합니다.

필터 임계값

고급 콘텐츠 탐지 규칙은 여러가지 기준 (PII, 키워드, 정규식 등)을 AND / OR 로직으로 사용해서 콘텐츠 검사에 대한 복잡한 조건을 정의합니다.

전송 제한

특정 시간 간격 내에서 전송 제한을 설정합니다. 파일 수 또는 파일 크기 기반으로 설정이 가능합니다. 제한에 도달하면 이메일을 통해서 경고를 받을 수 있습니다.

문맥 감지

개인 정보 같은 민감한 콘텐츠의 더 정확한 탐지를 위한 발전된 검사 메커니즘을 사용할 수 있습니다. 문맥 사용자 정의가 가능합니다.

오프라인 임시 암호

네트워크가 연결되지 않은 컴퓨터에 파일 전송을 임시로 허용합니다. 보안과 생산성을 보장합니다.

대시보드, 보고 및 분석

파일 전송에 관련된 활동을 모니터터링 합니다. 중요한 이벤트들과 로그의 통계를 시작화하여 그래픽 및 차트로 제공합니다.

규정 지원 (GDPR, HIPAA 등)

PCI DSS, GDPR, HIPAA 등과 같은 산업 규정 및 법률을 지원합니다. 벌금 및 다른 손해를 피할 수 있습니다.

프린터 정보유출방지

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

씬 클라이언트 정보유출방지

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

eDiscovery

Windows, macOS , Linux 용

파일 종류: 그래픽파일 / 오피스 파일 / 압축 파일 / 프로그래밍 파일 / 미디어 파일 / 기타
• 미리 정의된 콘텐츠: 신용카드번호 / 개인식별정보 / 주소 / 주민등록번호 / ID / 여권번호 / 전화번호 / 세금ID / 건강보험번호 / 기타 • 사용자 정의 콘텐츠 / 파일 이름 / 정규식 / HIPAA / 기타

데이터 암호화 및 복호화

기밀 정보가 포함된 저장 데이터는 인가되지 않은 직원의 접근을 막기 위해서 암호화 할 수 있습니다. 복호화 또한 가능합니다.

데이터 삭제

사내 정책의 명백한 위반이 인가되지 않은 엔드포인트에서 민감한 정보가 탐지되면 바로 데이터를 삭제하시기 바랍니다.

검색 위치 거부목록

미리 정의된 위치를 기반으로 필터를 만들 수 있습니다. 대상 콘텐츠 검사로 저장 데이터의 불필요한 검색을 피할 수 있습니다.

자동 검색

전체 검색 및 증분 검색 뿐만 아니라 자동 검색 예약을 만들 수 있습니다 - 한 번 또는 주기적 (주 또는 월 단위)으로 가능합니다.

검색 결과

저장 데이터 검색 로그를 모니터링하고 필요한 완화 조치를 취하시기 바랍니다. 로그 및 보고서는 SIEM 솔루션으로 내보내기 할 수 있습니다.

검색 상태

현재 검색 상태를 간단하게 확인하시기 바랍니다. 검색 상태는 0 - 100% 로 표시됩니다.

필터 임계값

적용되는 보안 정책과 서버에 보고되는 파일에 정책 위반 수를 정의 합니다.

규정 지원 (GDPR,HIPAA 등)

PCI DSS, GDPR, HIPAA 등과 같은 산업 규정 및 법률을 지원합니다. 벌금 및 다른 손해를 피할 수 있습니다.

파일 종류 거부목록

파일 종류 필터는 실제 파일 유형 기반으로 문서를 차단하는데 사용할 수 있습니다. 심지어 사용자가 확장자를 변경해도 차단이 됩니다.

미리 정의된 콘텐츠 거부목록

신용카드번호, 주민등록번호, 운전면허번호 등 미리 정의된 콘텐츠 기반으로 필터를 만들 수 있습니다.

사용자 키워드 거부목록

특정 표현, 키워드와 같은 사용자 정의 콘텐츠를 기반으로 필터를 만들 수 있습니다. 다양한 거부목록 사전을 만들 수 있습니다.

파일 이름 거부목록

파일 이름 기반으로 필터를 만들 수 있습니다. 이름 또는 확장자 기반으로만 설정이 가능합니다.

정규식 거부목록

표준 정규식을 사용해서 패턴을 정의하고 전송된 파일을 검사하는 강력한 도구입니다.

파일 허용목록

모든 파일 전송 시도를 차단하고 따로 허용목록을 만들어서 생산성을 높이고 불필요한 검색을 피할 수 있습니다.

MIME 유형 허용목록

특정 MIME 유형에 대한 콘텐츠 검사를 제외하고 전체 레벨에서 불필요한 검색을 피할 수 있습니다.

SIEM 서버

로그를 외부로 보내는 SIEM (Security Information and Event Management) 서버와 연동합니다. 보안 제품의 연속적인 경험을 제공합니다.

100% 모든 고객의 필요에 적합

모든 유형의 네트워크에 적합한 코소시스 Endpoint Protector는 대기업, 중소 비즈니스, 소규모 사업자 및 개인도 사용할 수 있습니다. 서버-클라이언트 구조로 제공되어서 설치가 매우 쉽고 웹 기반 인터페이스로 중앙 관리를 지원합니다. 하드웨어 및 가상 어플라이언스 뿐만 아니라 Amazon Web Services, Microsoft Azure, Google Cloud 에서 사용할 수 있습니다.

로컬 계정, 온-프레미스 AD (Active Directory) 인증, Azure AD SSO (Single Sign-On), OKTA SSO (Single Sign-On) 포함한 다중 로그인 옵션이 가능합니다. 관리자를 위한 더 간단하고 쉬운 제어를 지원합니다. MFA (Multi-factor Authentication) 또한 사용 가능합니다.

콘텐츠 인식 보호, 매체 제어, SW 보안USB, eDiscovery 기능을 Windows, macOS, Linux 배포판으로 운영되는 컴퓨터에서 사용할 수 있습니다.

가상 어플라이언스

하드웨어 어플라이언스

클라우스 서비스

Amazon Web Services
Microsoft Azure
Google Cloud

Gartner peerinsights™

엔터프라이즈 DLP 부문 **Gartner Peer Insights** 의 높은 평가!

사용 가능한 OS

Windows	Windows 7 / 8 / 10 / 11	(32/64 bit)	●	●	●	●
	Windows Server 2003 - 2019	(32/64 bit)	●	●	●	●
	Windows XP / Windows Vista	(32/64 bit)	●	●	●	●
macOS (kext / kextless 에이전트)	Apple Silicon M1 / M1 Max / M2		●	●	●	●
	macOS 14.00	Sonoma	●	●	●	●
	macOS 13.00	Ventura	●	●	●	●
	macOS 12.00	Monterey	●	●	●	●
	macOS 11.00	Big Sur	●	●	●	●
	macOS 10.15	Catalina	●	●	●	●
	macOS 10.14	Mojave	●	●	●	●
	macOS 10.13	High Sierra	●	●	●	●
	macOS 10.12	Sierra	●	●	●	●
	macOS 10.11	El Capitan	●	●	●	●
	macOS 10.10	Yosemite	●	●	●	●
	macOS 10.9	Mavericks	●	●	●	●
	macOS 10.8	Mountain Lion	●	●	●	●
Linux	Debian		●	●	●	n/a
	Ubuntu		●	●	●	n/a
	OpenSUSE / SUSE		●	●	●	n/a
	CentOS / RedHat		●	●	●	n/a
	Fedora		●	●	●	n/a

COSOSYS

Official Partner

Germany

vertrieb@endpointprotector.de
+49 7541 97826730
+49 7541 97826734 / ext. 202

Romania

sales@cososys.com
+40 264 593 110 / ext. 103
+40 264 593 113 / ext. 202

North America

sales.us@endpointprotector.com
+1 888 271 9349
+1 877 377 6475

South Korea

contact@cososys.co.kr
+82 1644 7718