ENDPOINT PROTECTOR | by CoSoSys

30일 안에 DLP 솔루션을 설정하는 방법

DLP | Device Control | Content Aware Protection | Encryption | **MDM**

COSOSYS

서론

DLP (Data Loss Prevention) 솔루션은 실행이 복잡하고 어렵다는 오해가 있습니다. DLP 솔루션은 IT 보안 전략에 있지 않거나 우선순위가 떨어진다고 말하기도 합니다.

Endpoint Protector DLP 는 이와는 반대로 혁신적인 크로스 프랫폼 솔루션입니다. 또한 30일 안에 모든 설정을 마무리할 수 있습니다.

1. 제품 유형 선택

하드웨어 또는 가상 어플라이언스를 선택할 수 있습니다.

하드웨어 어플라이선스는 플로그 앤 플에이 DLP 솔루션을 찾고 있다면 명확하게 그대로 보여줍니다. 적절한 스토리지 용량과 네트워크 규모에 대응하는 처리 성능을 가진 여러 종류의 하드웨어 어플라이언스 사용이 가능합니다. 모든 모듈이 미리 설치되어 제공되기 때문에 IT 관리자는 어플라이언스르를 네트워크에 연결하고 IP 를 할당하기만 하면 됩니다.

가상화에 친숙하다면 가장 어플라이언스는 더 높은 유연성과 더 낮은 비용을 제공합니다. 보유하고 있는 가상 소프트웨어에 따라서 코소시스는 여러 종류의 가상 어플라이언스 포맷을 제공합니다. 단수하게 제공되는 링크에서 적합한 가상 이미지를 다운로드 받고 가상 이미지 임포트와 IP 를 할당하기만 하면 됩니다.

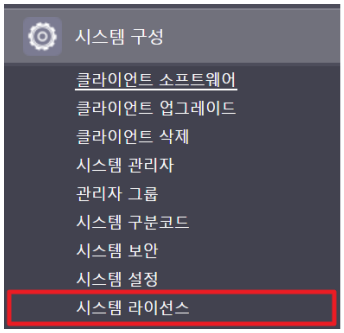
관리 콘솔은 **https://IP** 를 통해서 브라우저로 접근할 수 있습니다. 미리 정의된 로그인 계정은 Endpoint Protector 사용자 매뉴얼을 참조하시기 바랍니다.

예상 소요시간 - 30 분

2. 라이선스 가져오기

라이선스 파일을 가져오거나 라이선스를 복사 / 붙여넣기로 활성화 합니다. 그 후에 CAP, eDiscovery, MDM 등의 모듈을 활성화 할 수 있습니다.

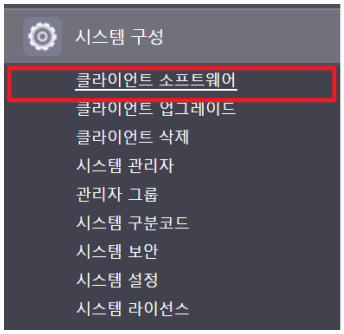
예상 소요시간 - 15 분



3. 클라이언트 소프트웨어 배포

데이터 유출 및 도난으로 부터 보호하기 원하는 컴퓨터에 클라이언트 소프트웨어를 설치합니다. 시간 절약을 위해서 Active Directory 를 통한 배포를 추천합니다.

예상 소요시간 - 5 시간 (500 사용자 컴퓨터 규모 기준)



4. 매체 제어 정책 설정

매체 제어 정책을 설정해서 어떤 휴대용 장치에 누가 접근하는 결정할 수 있습니다. 모든 컴퓨터에 대해서 글로벌 레벨로 정책을 설정할 수 있고 그룹, 컴퓨터, 사용자, 장치, 사용자 정의 클래스로 정책을 시작할 수도 있습니다.

다음을 권장합니다! 모든 컴퓨터에 대해서 사용 허용 정책으로 느슨하게 시작해서 회사 구조에 따라서 장치 사용을 제한할 수 있습니다. 예를 들어 모든 컴퓨터에 USB 장치 사용 허용을 설정하고 회계 그룹에는 읽기만 정책을 설정합니다.

예상 소요시간 - 3 시간 : 평균 500 사용자 규모 기준

5. 파일 추적 및 사본 보관 활성화

휴대용 저장 장치에 사용 허용 정책을 사용하고 파일 추적 및 사본 보관을 활성화 했다면 USB 장치에 어떤 파일이 전송되는지 추적할 수 있습니다. 보안 정책을 구축할 때 이러한 충분한 정보를 가지고 있다면 조직에 맞는 정책을 최적화하는데 도움이 될 것입니다.

다음을 권장합니다! 네트워크 오버로딩과 대역 및 디스크 공간 사용량이 넘는 것을 피하기 위해서 파일 사본 보관의 최대 파일 크기를 설정하시기 바랍니다.

예상 소요시간 - 15 분

6. 민감한 데이터 정의

회사에 중요한 정보의 세부사항을 관리하고 민감한 데이터의 유출 및 도난을 보호 해야 합니다. 고객 데이터베이스, 개인식별정보, 신용카드번호, 주민등록번호, 파일 유형 그리고 기밀 정보로 분류 될 수 있는 키워드 (월급, 고객 데이터, 마케팅 플랜, 재무, 비밀, 기밀 등)과 같은 보호하려고 하는 데이터 목록을 가지고 있어야 합니다. 이러한 목록은 계속해서 업데이트가 되어야 합니다.

예상 소요시간 - 3 시간

7. 콘텐츠 인식 보호 (CAP) 설정

CAP 정책을 보고만 액션으로 만들어서 시작합니다. 이 정책은 네트워크 외부로 어떤 파일이 전송되는지 알 수 있고 이 정보를 바탕으로 특정 사용자, 컴퓨터, 그룹을 제한하는데 사용할 수 있습니다. 파일 전송에 관련된 응용프로그램을 선택하고 6번에서 정의된 데이터 목록을 필터로 사용합니다.

파일 유형 필터, 미리 정의된 콘텐츠 필터, 사용자 정의 필터 및 정규식 필터 조합을 사용할 수 있습니다.

정책을 저장하고 이 정책에 적용되는 객체를 선택합니다. 다른 객체에 대해서 정책을 복사하거나 사용자 정의할 수 있습니다. 또는 새로운 정책를 다시 시작 할 수 있습니다.

예상 소요시간 - 24 시간

8. 콘텐츠 인식 파일 사본 보관 활성화

선택한 응용프로그램을 통해서 전송된 파일 사본을 보고 싶다면 콘텐츠 인식 파일 사본 보관을 활성화 합니다. 파일의 콘텐츠를 볼 수 있고 파일 이름이 일치하는지 아니면 몇 번 전송을 시도했는지 확인할 수 있습니다.

다음을 권장합니다! 네트워크 오버로딩 및 대역 및 디스크 공간의 사용량 초과를 피하기 위해서 파일의 최대 크기를 설정합니다.

예상 소요시간 - 20 분

9. 분석 기간

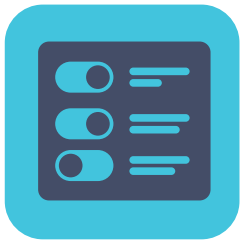
보고만 모드로 정책을 15 ~ 20일 가량 두고 리포트를 확인하는 마지막 기간에 데이터를 분석하고 어떤 것을 차단할지 어떤 사용자를 제한 할지 어떤 그룹이 위협이 되는지 특정 전송만 차단해야 하는지 등을 결정합니다.

복잡한 보고서를 사용할 수 있고 관리를 위해서 내보내기 할 수 있습니다. 어떤 응용프로그램 또는 장치를 통해서 누가 어떤 파일을 전송하는지 정확하게 볼 수 있습니다.

예상 소요시간 - 15 ~ 20 일

10. 적절한 콘텐츠 인식 보호 정책 설정

기본적인 설정이 완료되었으면 클립보드 모니터링, 기밀 데이터 복사 / 붙여넣기 방지, 프린트 스크린 사용 차단, 네트워크 공유 스캔, 기밀 로컬 및 네트워크 프린터에 대한 데이터 프린팅 차단, URL 화이트리스트, SIEM 서버 연동 등과 같은 적절한 옵션 설정을 시작할 수 있습니다.



모든 설정 매개변수와 함께 Endpoint Protector DLP는 백그랑운드에서 구동할 수 있어서 지속적인 모니터링을 필요로 하지 않습니다. 이것은 데이터 보안 또는 네트워크 통합의 다른 측면에 집중하기 위해서 시간과 다른 리소스를 절약하기 때문입니다.

30일 안에 DLP 솔루션을 설정하는 방법!