ENDPOINT PROTECTOR | by CoSoSys

빠른 설정 가이드

전체 네트워크 보호

빠른 설정 가이드

Endpoint Protector는 직원이 사용하는 엔트포인트 시스템을 위해 설계된 DLP (Data Loss Prevention) 솔루션 입니다. 사용자가 노트북, 데스크탑, 서버를 통해서 데이터에 접근할 때 이러한 엔드포인트 시스템의 DLP는 조직의 데이터 유출 보호에 도움을 줍니다.

우발적인 데이터 유출에서 악의적인 내부자 활동에 이르기까지 민감한 데이터를 보호하는 것은 데이터 위반의 결과인 운영 중단, 규정 이슈, 평판 훼손을 예방하는데 매우 중요합니다.

이러한 점이 엔드포인트 기반 DLP가 끊임없이 진화하는 사이버 위협에서 필수가된 이유입니다. DLP가 없으면 네트워크 관리자는 우발적인 데이터 유출을 예방하거나 관련 사용자를 식별하기 매우 어렵습니다.

PCI-DSS, HIPAA, GDPR 등과 같은 규정 준수 요구 사항을 해결하려는 경우 Endpoint Protector는 이러한 정보의 위치를 찾기 위한 검색 패턴을 가지고 있고 대응 전략을 제공합니다. 다른 대안으로 IP (Intellectual Property), 특허 정보 또는 고객 목록 보호와 검색에 집중한다면 Endpoint Protector는 또한 이러한 부분에 도움을 줄 수 있습니다.

매체 제어, 콘텐츠 인식 보호, eDiscovery, 암호화 정책 모듈을 통해서 Endpoint Protector는 인터넷 연결 및 외부 저장 장치 모두를 통한 데이터 유출을 차단하는데 도움이 됩니다. 엔드포인트의 모든 장치 활동을 제어할 뿐만 아니라 민감한 콘텐츠의 가능한 엔트포인트를 모니터링 및 검색합니다. 중요한 비즈니스 데이터가 장치에 복사되거나 허가 없이 인터넷을 통해 전송되는 모든 데이터 이슈를 보고함으로써 내부 네트워크를 벗어나지 않도록 보장합니다. 또한 로컬에 저장된 저장 데이터 (Data at rest)에 민감한 콘텐츠가 있는지 검사하고 교정 초치를 취할 수 있으며 외부 USB 장치로 전송되는 모든 콘텐츠에 암호화를 강제 적용할 수 있습니다. 이 모든 기능은 Endpoint Protector 단일 웹 기반 인터페이스를 통해 수행됩니다.

다음 섹션에서 Endpoint Protector를 사용하여 엔드포인트 보호를 시작하는데 필요한 기본 배포, 설정, 구성 작업에 대해서 알아보겠습니다.

1. Endpoint Protector 서버 환경

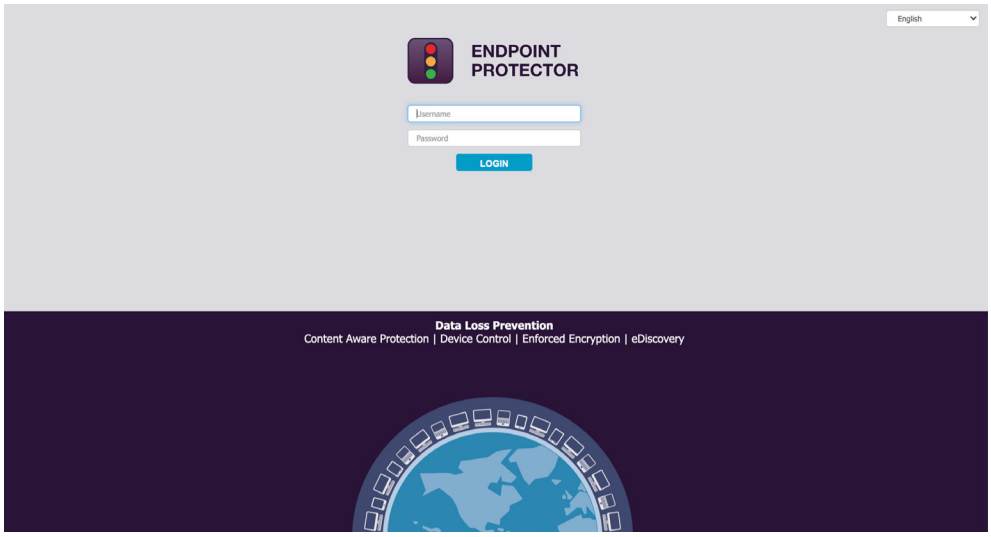
Endpoint Protector 사용을 시작하려면 서버 인스턴스를 사용할 수 있어야 합니다. 서버는 모든 엔트포인트 제어와 동작을 구성할 수 있는 위치이고 엔드포인트 시스템에 Endpoint Protector 에이전트를 전달하는 수단입니다.

서버는 On-Premise 또는 Hosted-Cloud 환경에 설치 될 수 있습니다.

On-Premise 옵션은 고객의 LAN 설정에서 가상화 이미지 설정을 허용합니다. 가상화 옵션은 Vmware와 Hyper-V로 제한되지 않습니다. Hosted-Cloud 배포는 AWS (Amazon Web Services), Azure, GCP (Google Cloud Platform) 인스턴스 사용을 허용합니다.

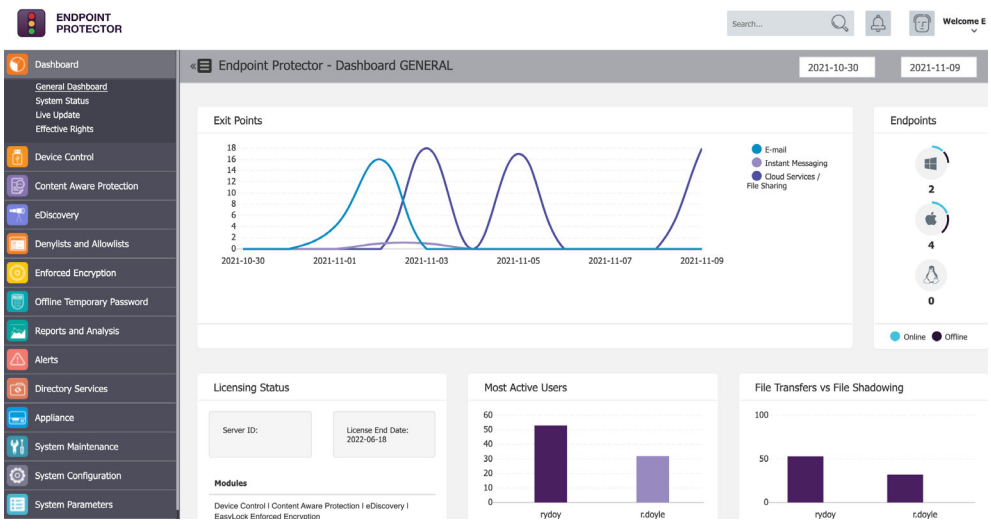
2. Endpoint Protector 서버 로그인

Endpoint Protector 서버가 프로비저닝되면 기능 모듈의 구성을 수행할 수 있습니다. 에이전트 배포 준비 정책 관리를 위해 서버 설정으로 구성된 웹 사용자 인터페이스에 로그인이 필요합니다. 일반적으로 고정 IP 또는 도메인 구성이 될 것입니다. 주소 창에 Endpoint Protector 서버 주소를 입력하면 사용자 로그인이 준비됩니다. 처음 로그인 시 기본 계정 (root, epp2011)을 사용합니다. 이미 따로 설정 했다면 할당된 사용자 이름과 비밀 번호를 입력합니다.



로그인에 성공하면 **대시보드 > 통합 대시보드** 창이 나타납니다 (아래 이미지 참조). 이 화면은 활동, 라이선스 상태, 모듈 라이선스 뿐만 아니라 관리를 위한 엔드포인트의 전체 상황을 높은 수준으로 제공합니다.

왼쪽 하단에 사용 가능한 모듈이 표시됩니다. 이러한 모듈은 모듈 특정 정책을 관리하기 위해 선택 될 수 있습니다. 궁극적으로 정책은 엔드포인트에서 허용 / 허용하지 않음 액션을 정의합니다.



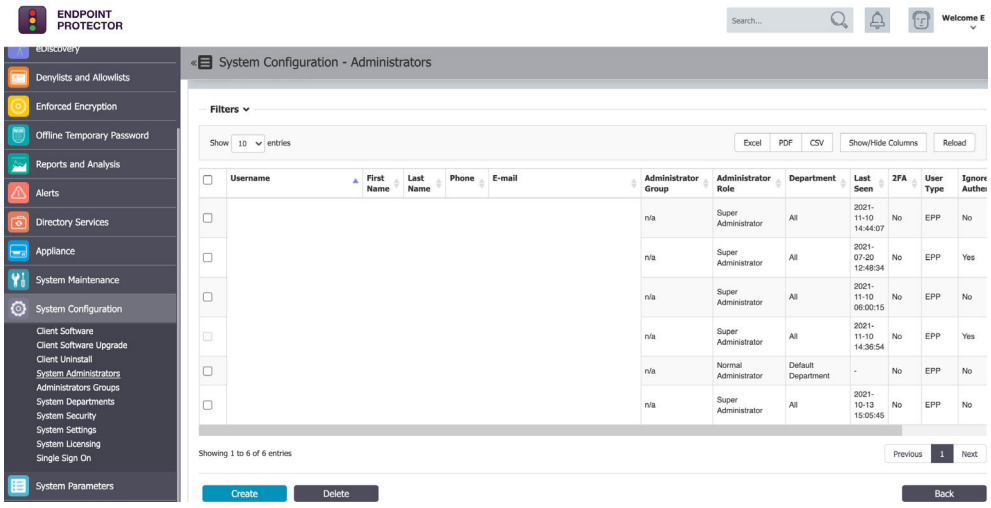
에이전트 배포 전에 각 모듈 정책을 검토해야 합니다. 만약 에이전트가 이미 시스템에 배포되었다면 활성화된 정책 매핑을 검증하여 정책 구성을 검토할 수 있습니다. 정책이 만들어지거나 편집되면 정의된 대상 또는 대상 그룹에 매핑됩니다. 이 내용은 각 모듈에 대한 섹션 뒷분에서 설명하겠습니다.

3. 관리자 관리하기

관리자는 중요한 역할을 수행합니다. Endpoint Protector를 최신 버전 업데이트를 유지할 뿐만 아니라 조직의 보안을 위해 DLP 정책을 배포하고 유지보수하는 매우 중요한 역할을 수행합니다. 이러한 이유로 관리자를 선택할 때 조직에 필요한 기능을 기반으로 장치와 콘텐츠 제어를 완전히 이해를 가지고 있는가 여부가 중요합니다. 이 섹션은 Endpoint Protector에서 관리자 추가와 관리자 권한 관리 방법에 대해서 알아보겠습니다.

참고 - 기본 관리자 정보를 아직 변경하지 않았다면 관리자 추가 전에 수정할 것을 권장합니다.

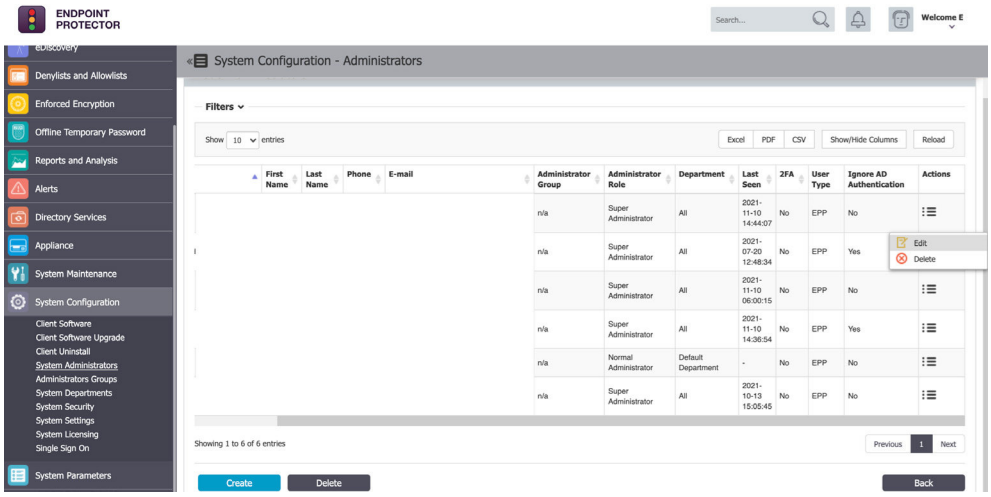
Endpoint Protector 관리자 콘솔에 로그인 후 시스템 구성 섹션을 검색합니다. '시스템 관리자'를 선택합니다.



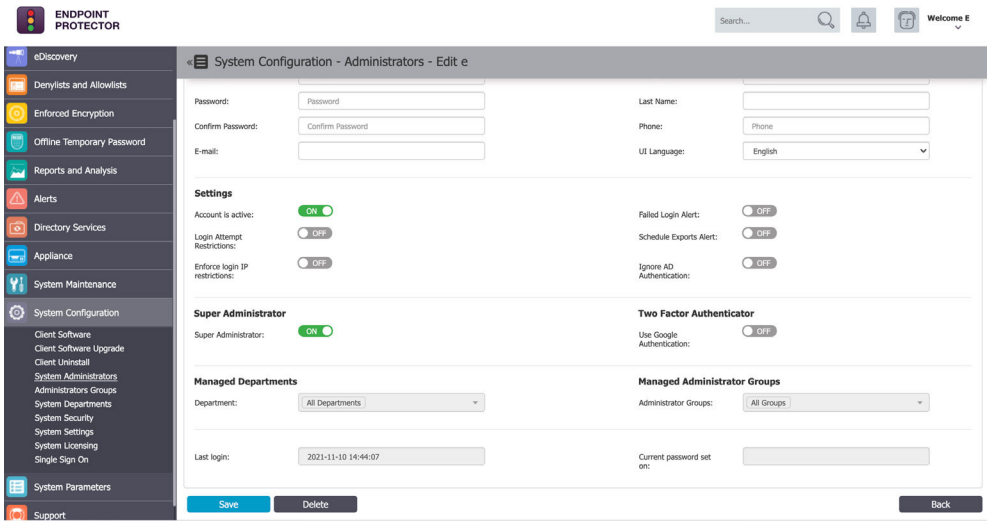
'만들기' 버튼을 사용해서 관리자 추가를 시작할 수 있습니다. 만약 관리적인 제한이 필요함다면 관리자를 만들 때 적절한 '관리자 그룹' 을 정의할 수 있습니다. 일반적으로 ReadOnly 그룹 옵션을 사용하지 않으면 여러 관리자 그룹을 하나의 계정에 할당할 수 있습니다. 이러한 그룹 목록은 '시스템 구성 > 관리자 그룹' 섹션에서 찾을 수 있습니다.

3.1. 시스템 관리자 편집

관리자 편집은 관리 콘솔의 '시트템 관리자'에서 할 수 있습니다. 편집하려는 관리자 계정의 '액션' 컬럼을 클릭하고 '편집'을 선택합니다.



A 필요한 편집을 할 수 있는 새로운 페이지를 볼 수 있습니다. 아래 이미지를 참조하시기 바랍니다. 관리자 콘솔에서 가장 높은 권한을 가진 계정이 필요하다면 '최고 관리자' 슬라이드를 토글해서 ON 으로 설정합니다. 모든 편집이 완료되면 가장 아래에 있는 '저장' 버튼을 선택합니다. 만약 변경하지 않으려면 '뒤로' 버튼을 선택하거나 관리 콘솔의 또 다른 섹션을 선택하면 취소되고 해당 계정에 변경 내용이 적용되지 않습니다.



4. 매체 제어 구성

Endpoint Protector 기능을 사용하면 반드시 엔드포인트에 에이전트가 배포되어야 합니다. 주어진 환경에서 에이전트가 동작하는 방법을 아는 것도 마찬가지로 중요합니다. 매체 제어는 Endpoint Protector와 에이전트 동작의 핵심이므로 일반적으로 매체 제어 정책을 검토하는 것으로 시작합니다.

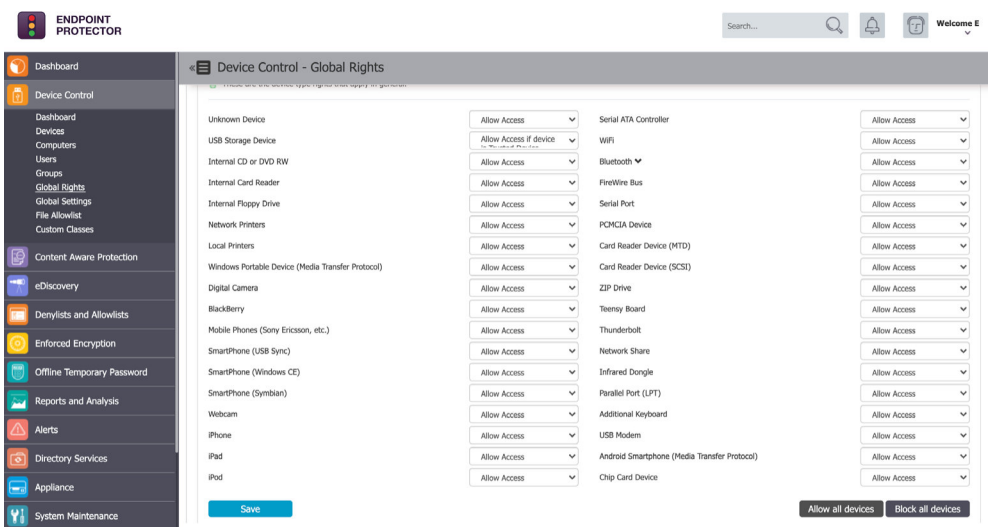
매체 제어는 관리자에게 특정 주변 장치에 대한 엑세스를 허용하거나 거부할 수 있는 기능을 제공합니다. 또한 이 기능은 해당 장치 중 특정 장치만 제어할 수 있는 기능을 제공합니다. 이는 관리자가 특정 USB 저장 장치 브랜드만 엑세스할 수 있도록 설정할 수 있는 것을 의미합니다. 이러한 기능은 '커스텀 클래스' 하위 섹션인 '장치 마법사' 에서 제공합니다. 이 세션은 뒷부분에서 다루겠습니다.

최상위 설정인 '전체 권한' 을 고려해봐야 합니다. 그 아래에 '그룹' 그리고 그 아래에 '컴퓨터' 및 '사용자' 순서로 되어 있습니다. '시스템 구성 > 시스템 설정' 섹션에서 관리자는 컴퓨터 권한, 사용자 권한, 모두 사용할 수 있도록 정의할 수 있습니다.

일반적으로 전체적인 우선순위를 이해하는 방법은 최하위 구성이 우선한다는 것을 고려하는 것입니다. 예를 들어 시스템 A에 대한 컴퓨터 권한이 '사용 거부' 제한이 되어 있다고 가정합니다. 글로벌 권한 (정책)을 모두 '사용 허용' 으로 변경하면 시스템 A를 제외한 모든 시스템은 사용이 거부되지 않을 것입니다 (다른 시스템이 따로 제한이 걸려 있지 않다고 가정한 경우).

4.1 '모든 장치 허용' 매체 제어 정책 설정하기

In a Endpoint Protector 초기 배포에서 사용자 중단을 최소화하기 위한 전략의 첫 번째 모범 사례는 '전체 권한'을 모두 '사용 허용'으로 설정하는 것입니다. 나중에 매체 제어에 ' 사용 거부' 정책이 필요하다면 '전체 권한' 또는 '그룹' 섹션이 관리적인 효용성을 유지하는 최적의 위치입니다.



5. 콘텐츠 인식 보호 (CAP)구성

콘텐츠 인식 보호 (CAP, Content Aware Protection)를 가장 잘 이해하려면 이 모듈이 안티바이러스의 활성화된 검색 기능과 유사한 동작을 한다고 생각하시면 됩니다. CAP는 활성 파일을 보고 이러한 파일의 속성을 확인합니다. 파일은 사용 중일 때 특히 사용자의 엔드포인트로 전송하려고 할 때 시스템에서 활성 상태가 됩니다.

데이터 유출 방지는 모든 DLP 솔루션의 핵심 구성 요소이며 따라서 데이터 속성 결정을 통해서 일어나는 탐지 또는 분류는 이 모듈의 필수적인 부분입니다. '미리 정의된 정책' 옵션을 사용하면 특정 파일 유형 또는 특정 규정 항목 (HIPAA, PII, PCI-DSS 등)에 집중할 수 있습니다. 사용하고 있는 운영 체제에 따라서 정책을 Windows, macOS, Linux 시스템에 각 정책을 만들 수 있습니다. 사용자 키워드에 따른 정책이 필요하면 '거부목록 및 허용목록' 세션에서 '사용자 키워드'를 입력하거나 가져올 수 있습니다. '사용자 키워드'가 추가되면 관련 항목인 '사용자 키워드' 탭에 있는 정책에 연결할 수 있습니다.

정책이 만들어진 후에 대상을 할당해야 합니다. 대상은 구분, 그룹, 컴퓨터 및/또는 사용자가 될 수 있습니다. 콘텐츠 인식 정책에 할당된 대상을 보려면 관리 콘솔에서 콘텐츠 인식 정책 섹션의 정책을 선택하고 페이지 아래로 스크롤합니다. 할당되 대상의 편집이 필요하면 수정 후 정책 대상을 정의하는 바로 아래에 있는 '저장' 버튼을 클릭하시기 바랍니다.

5.1. 콘텐츠 인식 보호 정책의 '보고만' 설정

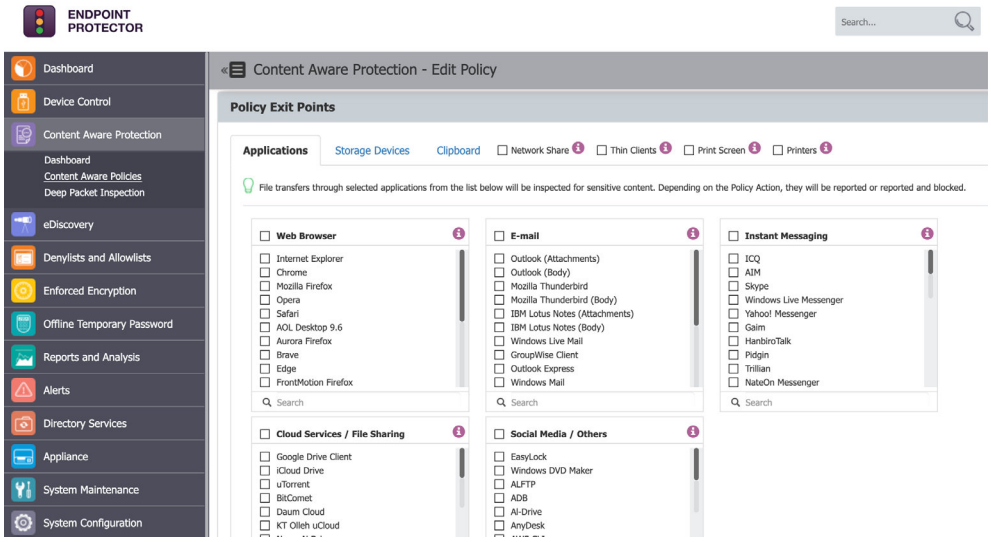
매체 제어 정책의 '모두 허용'을 보완하려면 콘텐츠 인식 보호의 '보고만' 정책을 다음으로 만드는 것을 권장합니다. 이는 엔드포인트에서 파일 이동을 이해하기 위한 첫 번째 단계입니다.

Endpoint Protector 관리 콘솔 내에서 '콘텐츠 인식 보호 > 콘텐츠 인식 정책'의 CAP 정책에서 "보고만"을 설정하여 정책을 만드시기 바랍니다. '사용자 정책 만들기' 버튼을 클릭하고 OS 종류, 정책 이름 (정책 이름 또는 설명에 "보고" 또는 "보고만"을 포함할 것을 권장함)을 입력하고 정책 작업에서 '보고만'을 선택합니다. 페이지 하단에 저장 버튼을 클릭하면 정책 창으로 변경되고 설정한 정책을 볼 수 있습니다. 만약 여러 운영 체제의 환경을 가지고 있다면 해당 운영 체제에 대해서 위의 과정을 다시 따르시기 바랍니다.

보고만 정책 프레임워크가 만들어지면 첫 번째 정책을 선택하고 편집 아이콘을 선택합니다. 편집 아이콘은 정책의 우측에서 찾을 수 있습니다. 정책 편집 페이지에서 필요한 엔드포인트를 선택합니다. 이 엔드포인트는 차후에 여러분의 차단 정책으로 사용될 수도 있습니다.

비록 이 정책에서 사용되는 용어는 '거부목록' 이지만 제한 없이 이 정책은 보고만 합니다. 뒤에서 자동으로 조치되도록 이 정책에 대한 자금 작업을 생성하는 것을 안내하겠습니다. 또한 CAP 모듈은 동작 객체만 집중하므로 최소 엔드포인트 리소스를 사용합니다. 이는 에이전트가 설치된 환경에서 발견되는 변수만 정책 내에서 설정하는 것이 가장 좋습니다. 탐지 지점에서 불필요한 처리가 발생하지 않도록 합니다.

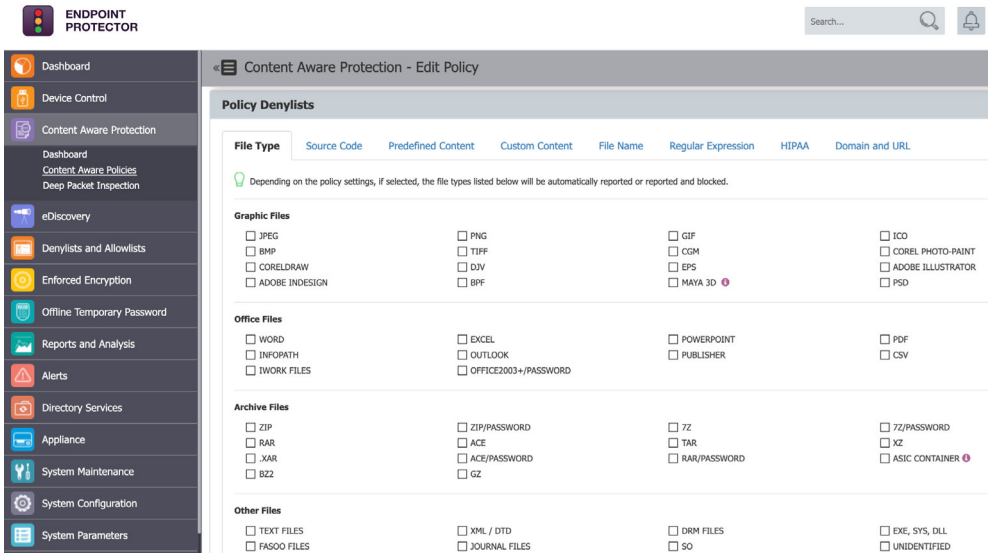
일반적으로 정책 대상의 응용프로그램 탭은 클라이언트 환경에서 범용적인 이메일 클라이언트 또는 웹 브라우저 등이 해당됩니다. 저장 장치 탭은 저장 장치에 민감한 파일의 전송을 제한 하려는 의도로 나중에 사용될 수 있습니다.



정책 거부목록 섹션은 분류 및 정책 결정에 중점을 둔 객체를 선택하는 방법을 제공합니다. 주어진 파일의 감사를 진행하려면 '파일 종류' 탭은 시스템의 일반적인 파일 종류에 대한 여러가지 옵션을 제공합니다. 규제에 더 집중하려면 '미리 정의된 콘텐츠' 탭을 이용하는 것이 더 적절합니다.

실제로 사용자 정의 정책이 필요한 경우 '사용자 정의 콘텐츠'에 관련된 탭에서 관리자가 만든 항목과 매핑되는 정책을 사용할 수 있습니다. 정규식 탭의 경우 관리자가 직접 논리 연산자를 만들어 사용할 수 있습니다.

거부목록 섹션과 관련된 모범 사례는 신용카드번호, 주민등록번호, PII (Personal Indentifiable Information)을 포함하는 것일 수 있습니다.



정책 편집 페이지 하단에 저장을 선택합니다. 각각의 만들어진 '보고만' 정책에도 저장을 선택합니다. 에이전트 배포를 진행하면 이 정책으로 돌아와서 대상 클라이언트 시스템을 선택하고 이 정책을 사용합니다.

16. eDiscovery 검색 구성

CAP 모듈을 지원하는 eDiscovery는 주어진 환경에서 발견되는 정보에 더 큰 인사이트를 제공합니다. 위에서 언급한 내용을 다시 사용해서 eDiscovery는 훨씬 더 안티바이러스 검색과 같다고 생각하시면 됩니다. 차이점은 eDiscovery는 활성화된 검색보다 수동 검색을 제공하는 것입니다. 안티바이러스의 '전체 검색'과 같이 수동 스캔은 저장 데이터 (Data at Rest)를 찾고 콘텐츠에 따라서 이러한 객체를 분류합니다. 그러므로 eDiscovery는 조직이 대응하고 규정 요구 사항을 위반할 수 있는 사용자 엔드포인트에 저장된 데이터의 더 많은 것을 볼 수 있도록 제공합니다.

조직은 가장 중요한 데이터가 어디에 보관되어 있는지 알고 있어야 잘 관리하고 보호할 수 있습니다. 이것은 매우 중요합니다. 민감한 데이터 위치를 이해함으로써 더 올바르게 권한을 사용할 수 있고 더 엄격한 보안을 구축할 수 있습니다. 궁극적으로 사이버 보안 관점에서 보다 책임감 있는 관리를 할 수 있습니다.

eDiscovery 검색을 구성하는 것은 새로운 콘텐츠 인식 보호 정책을 만드는 것과 유사하지만 몇 가지 차이점을 고려해야 합니다. 첫 째, eDiscovery는 검색 방식에서 더 광범위해서 자연스럽게 엔드포인트 처리 리소스를 더 많이 소비합니다. 따라서 Endpoint Protector는 업계에서 가장 가볍고 효율적인 에이전트를 제공하지만 집중 근무시간 외에 검색을 실행하는 것이 바람직합니다.

둘 째, 검색 변수가 더 많이 구성된 정책은 검색이 실행될 때 더 강도가 높습니다. 검색을 제한된 데이터 유형으로 제한하는 것이 가장 좋습니다. 여러가지 데이터 유형으로 검색을 원한다면 별도의 정책을 만들고 차이를 두고 검사를 실행합니다.

마지막으로, 콘텐츠 인식 보호 정책과 일관성을 보이기 위해 eDiscovery에서 사용되는 용어와 변수는 매우 유사합니다. 거부목록과 허용목록이 사용되지만 거부목록 섹션은 허용목록 섹션이 고려하지 않는 항목을 의도적으로 해결하려는 항목의 영역입니다. 이 부분은 eDiscovery 검색 결과에 대한 교정 옵션을 논의할 때 연관이 되어 있습니다.

6.1. eDiscovery 검색을 만들고 시작하기

'eDiscovery > 정책 및 검색'으로 이동합니다. 사용자 정책 만들기를 클릭하고 OS 종류, 정책 이름, 항목을 선택 후 페이지 하단의 저장 버튼을 클릭합니다. Endpoint Protector 에이전트 배포 후 이 정책 섹션으로 돌아가서 정책 검색 대상을 선택합니다.

추가로 에이전트가 배포되면 '정책 및 검색' 섹션에 나타날 것입니다. '수동 검색' 또는 '자동 검색'은 정의된 검색을 선택하여 정의할 수 있으며 자동 검색을 선택하면 간격 세부 정보를 구성하는 창이 나타납니다. 검색은 '전체 검색' 또는 '증분 검색'으로 실행할 수 있습니다. 일반적으로 초기에 전체 검색을 실행한 후에 증분 검색을 사용합니다. 검색이 완료되면 '작업'에서 '발견된 항목 검사'를 선택하거나 관리 콘솔 왼쪽의 eDiscovery 섹션에서 '검색 결과 및 액션' 으로 이동합니다. 뒷 부분에서 검색 결과 리뷰와 교정 조치에 관련해서 알아 보겠습니다.

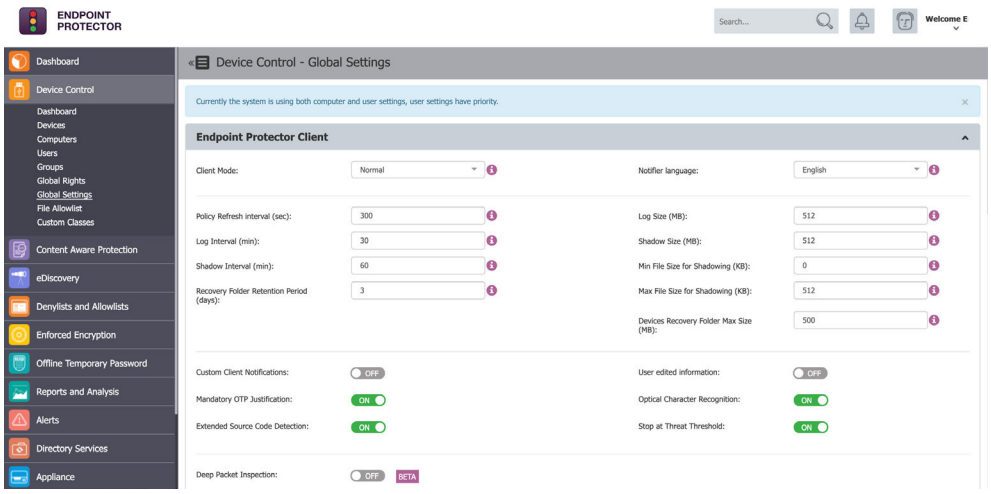
7. 사용자 경험 구성

많은 조직은 고유한 요구사항을 가지고 있으며 조직 내에서 직원의 역할 등에 따라 다양한 사용자 경험이 필요할 수도 있습니다. 이러한 점을 염두에 두고 고유한 요구를 수용할 수 있도록 Endpoint Protector 클라이언트의 사용자 맞춤 변경을 할 수 있습니다. 이 섹션에서는 사용 가능한 클라이언트 설정을 알아보고 관리 콘솔에서 이 설정을 구현하는 방법을 살펴보겠습니다.

7.1. 클라이언트 설정

Endpoint Protector 클라이언트와 직접 관련된 몇 가지 설정이 있습니다. 이러한 설정은 클라이언트의 동작을 설정하며 특정 객체 매핑을 위해 구성할 수 있습니다. 특정 객체 매핑은 전체, 그룹, 컴퓨터, 사용자가 포함됩니다.

클라이언트 설정은 관리 콘솔의 매체 제어 섹션에 위치하고 구성되어 있습니다. 매체 제어 섹션에서 전체 설정을 보시기 바랍니다. 설정을 하위 단계에서 구성하려면 각 하위 단계 (컴퓨터, 사용자 등)에서 작업에서 '설정 관리'를 보시기 바랍니다. 이러한 설정의 우선 순위는 앞에서 설명한 매체 제어의 권한과 매우 유사합니다.



7.1.1. 클라이언트 모드

Endpoint Protector 클라이언트는 최종 사용자 시스템에서 정의된 동작을 할 수 있는 여러가지 모드를 제공합니다. 6가지 모드를 선택할 수 있고 언제든지 변경이 가능합니다. 아래에서 관리자가 사용에 참고 할 수 있도록 간략하게 요약하겠습니다.

정상모드

Endpoint Protector 에이전트의 기본 배포 모드입니다. 완전한 이해 없이 정상모드에서 다른 모드로 변경하는 것을 권장하지 않습니다. 만약 정상모드가 조직의 조건과 맞지 않으면 아이콘 숨기 또는 무언모드가 좋은 대안이 될 수 있습니다.

패닉모드

이 모드는 사용자의 악의적인 의도가 있거나 도난 활동이 탐지되는 등 극단적인 상황에서 사용할 수 있습니다. 특수한 상황에서 관리자는 모든 장치를 차단하기 위해 이 구성으로 전환할 수 있지만 이 모드를 사용할 경우 극도로 주의를 기울이는 것이 좋습니다.

- 시스템 트레이에 아이콘이 표시됨
- 시스템 트레이에 알림이 나타남
- 인가 여부에 관계없이 모두 차단
- 사본 저장 및 파일 추적을 사용하여 사용자의 모든 활동을 모니터링하고 볼 수 있음
- 관리자는 패닉모드로 전환 및 해제 시 경고를 받음

투명모드

이 모드는 모든 장치 차단에 사용하지만 사용자는 모든 제한이나 Endpoint Protector 클라이언트의 존재 및 활동을 인식하지 못합니다.

- 시스템 트레이에 아이콘이 표시되지 않음
- 시스템 트레이에 알림이 나타나지 않음
- 인가 여부에 관계없이 모두 차단
- 관리자는 모든 활동의 경고를 받음

아이콘 숨김 모드

이 모드는 정상모드와 매우 유사합니다. 차이점은 Endpoint Protector 클라이언트가 사용자에게 보이지 않은 것입니다.

- 시스템 트레이에 아이콘이 표시되지 않음
- 시스템 트레이에 알림이 나타나지 않음
- 구성된 모든 권한 및 설정이 해당 구성에 따라 적용됨

은폐모드

이 모드는 모든 사용자와 컴퓨터를 모니터링 하지만 사용자는 모든 제한이나 Endpoint Protector 클라이언트의 존재 및 활동을 인식하지 못합니다. 모든 것을 사용 허용으로 설정하고 사용자의 활동을 매일 중단없이 볼 수 있습니다.

- 시스템 트레이에 아이콘이 표시되지 않음
- 시스템 트레이에 알림이 나타나지 않음
- 인가 여부에 관계없이 모두 허용
- 사본 저장 및 파일 추적을 사용하여 사용자의 모든 활동을 모니터링하고 볼 수 있음
- 관리자는 모든 활동의 경고를 받음

모언 모드

이 모드는 정상모드와 매우 유사합니다. 차이점은 팝업 알림이 사용자에게 보이지 않습니다.

- 시스템 트레이에 아이콘이 표시됨
- 시스템 트레이에 알림이 표시되지 않음
- 구성된 모든 권한 및 설정이 해당 구성에 따라 적용됨

7.1.2. 클라이언트 모드

알림 언어

Endpoint Protector 클라이언트 알림 언어입니다.

정책 갱신 주기 (초)

Endpoint Protector 클라이언트가 서버와 연결되고 최신 설정, 권한, 정책을 업데이트하는 정책 갱신 주기입니다.

알림 메시지 팝업

관리자는 시스템 트레이 알림과 팝업 알림을 선택할 수 있습니다. 이 설정은 직접적으로 사용자 경험과 관련이 있습니다. 차단은 정책 설정대로 동작합니다.

7.2. 사용자 수정 설정 구성

참고 - 사용자 수정은 프림미엄 기능입니다. 그러므로 이 섹션은 프림미엄 라이선스가 있어야만 사용할 수 있습니다.

사용자 교정 기능은 직원이 민감한 정보를 전송하려고 할 때 우회할 수 있도록 설계된 선택적 기능입니다. 해당 직원에게 차단 메시지를 표시하는 대신 (추가적인 관리자 개입이 필요함) '사용자 수정'은 특정 직원에게 역할, 기능, 의무에 따라서 정보를 전송할 수 있도록 합니다. '허용 요청 (ask for permission)' 모델이라기 보다는 '관면 요청 (ask for forgiveness)' 접근의 기능입니다. 이러한 우회는 적시에 콘텐츠를 전달하면서 정당한 근거의 상세 내용이 요구됩니다. 이 내용은 관리자에게 전송되어 추가 정밀 조사 및 실사를 진행할 수도 있습니다.

사용자 수정 팝업

이 설정은 사용자 수정 기능이 활성화 될 때 사용 가능합니다. 관리자는 최종 사용자의 사용자 수정 팝업을 사용할 수 있는 옵션을 가지고 있습니다.

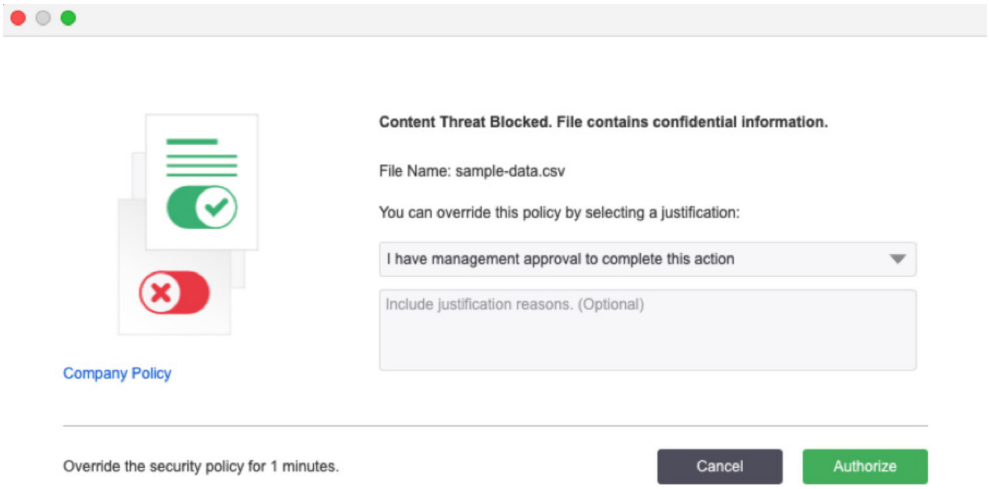
강제 사용자 수정 팝업

이 설정은 사용자 수정 팝업을 사용 할 때만 사용 가능합니다. 이 설정이 사용되면 최종 사용자는 사용자 수정 팝업 알림을 비활성화 할 수 없습니다.

7.2.1. 사용자 수정 설정 구성

Endpoint Protector 관리 콘솔의 '시스템 매개 변수 > 사용자 수정' 으로 이동하면 이 기능의 변수를 볼 수 있습니다. 여기에 있는 변수는 사용자 지정 로고, 사용자 지정 URL, 시간 간격이 포함될 수 있지만 이에 국한되지는 않습니다. 한 가지 고려해야 할 사항은 개별 객체 (개별 전송 채널과 관련된) 전송에 대해서 창을 얼마나 오랫동안 열어 있는 상태가 되어야 할 지 결정하는 것입니다. 구체적으로 사용자가 PII 정보가 포함된 문서를 전자 메일 첨부로 보내려고 할 경우 인증 작업은 작업이 선택된 후 전자 메일로 보내는 해당 항목에 몇 분의 정의된 시간을 줄 수 있습니다.

.다음 이미지는 '사용자 수정' 팝업 메시지 예입니다.

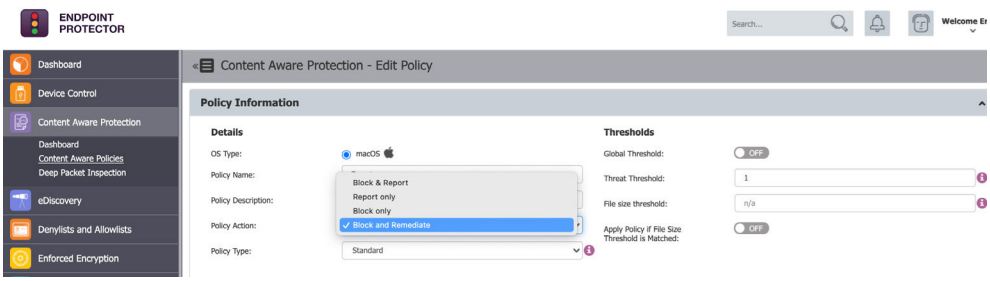


7.2.3. 사용자 수정 보고

사용자 수정 개입의 최종 사용자 로그 및 상세 내용은 Endpoint Protector 관리 콘솔의 '보고 및 분석 > 콘텐츠 인식 보고' 에서 확인 할 수 있습니다. 사용자 수정이 민감한 콘텐츠의 우회 및 전송을 인가에 사용되면 정당한 사유 영역은 사용자가 제출한 메시지를 제공합니다.

7.2.4. 사용자 수정 구현

콘텐츠 인식 보호의 차단 정책을 구성한 후에 사용자 수정으로 변경하는 것을 권장하지만 이 부분을 다루겠습니다. 사용자 수정으로 변경하기 위해서는 콘텐츠 인식 보호 정책의 '정책 작업' 영역을 수정해야 합니다. '차단 및 수정'을 선택함으로써 사용자 교정 기능은 Endpoint Protector 서버에 엔드포인트가 연결 될 때 사용할 수 있습니다.



7.3. “오프라인 임시 암호” 설정

‘사용자 수정’ 기능을 사용하지 않는 환경에서 ‘오프라인 임시 암호’는 또 다른 정책 우회를 제공합니다.

Endpoint Protector의 관리자 콘솔에서 이 섹션은 관리자는 오프라인 임시 암호 (OTP, Offline Temporary Password)를 생성하고 임시적으로 사용자 접근 권한을 허용할 수 있습니다. 임시적으로만 접근이 필요한 경우에 클라이언트 컴퓨터가 오프라인 상태로 Endpoint Protector 서버와 연결이 안되는 경우에 사용할 수 있습니다 (사용자 수정의 경우는 사용이 어렵습니다.).

오프라인 임시 암호는 아래 객체에 대해 생성할 수 있습니다:

- 장치 (특정 장치)
- 컴퓨터와 사용자 (모든 장치)
- 컴퓨터와 사용자 (모든 파일 전송)

사용자 매뉴얼에서 여러 시간대에 관련된 설정 등을 참조 하시기 바랍니다.

암호는 특정 기간과 연결되고 특정 장치 및 컴퓨터에 대해서 고유합니다. 이는 다른 장치 또는 컴퓨터 사용에 같은 암호가 사용되지 않는 것을 의미합니다. 또한 두 번 사용할 수 없습니다 (범용 오프라인 임시 암호의 경우는 예외). 사용 가능한 시간 간격은 15분, 30분, 1시간, 2시간, 4시간, 8시간, 1일, 2일, 5일, 14일 및 30일입니다.

8. Endpoint Protector 에이전트 배포

이제 Endpoint Protector 에이전트를 배포할 준비가 되었습니다. 차단 정책을 수정하기 전에 엔드포인트 시스템에 에이전트를 배포하는 것을 권장합니다. 이를 통해 허용이 필요할 수 있는 시스템 변수를 추가로 발견할 수 있을 뿐만 아니라 최종 사용자 피드백에 대한 창을 제공할 수 있습니다.

Endpoint Protector 클라이언트 패키지는 ‘시스템 구성 > 클라이언트 소프트웨어’ 섹션에서 검색할 수 있습니다. Windows, Mac, Linux 섹션을 찾아 지침에 따라 패키지를 다운로드 합니다. Windows 패키지는 추가 기능을 제공하므로 원하는 차단 전략에 따라 패키지를 다운로드 한 후 선택한 배포 도구를 통해 배포를 시작할 수 있습니다.

일반적으로 에이전트 배포에 Active Directory와 JAMF를 사용합니다. 다른 유틸리티로 배포하려는 경우 패키지용 설치 스위치가 지원되는 한 문제는 없습니다.

소규모 배포는 관리 콘솔에서 다운로드한 에이전트 패키지를 사용하여 실행하는 것으로 충분합니다. Mac 환경에 설치할 경우 로컬 디스크 엑세스를 제공해야 합니다. '시스템 환경 설정 > 보안 및 개인 정보 보호 > 개인 정보 > 전체 디스크 접근 권한' 에서 Endpoint Protector 클라이언트 응용프로그램을 찾아서 체크 후 저장합니다.

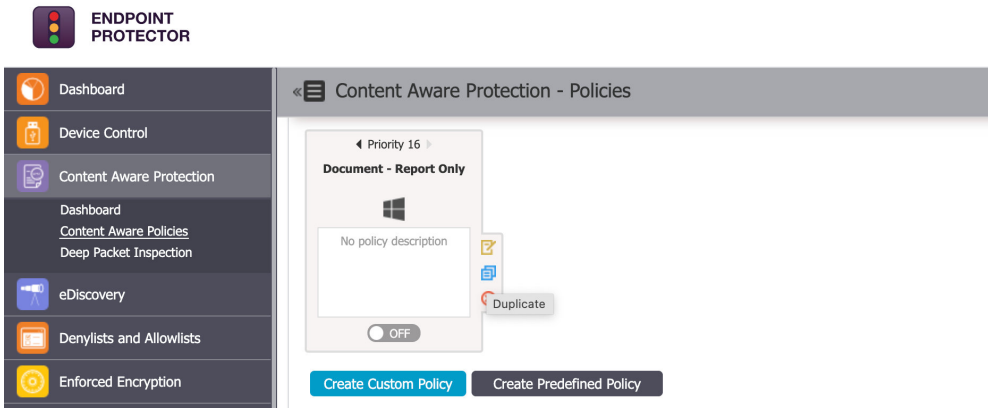
8.1. 대상 시스템에 정책 할당

처음 Endpoint Protector 에이전트가 시스템에서 실행 된 후에는 앞에서 설명한 정책을 검토하고 매팽해야 합니다. 이렇게 하면 Endpoint Protector 관리 콘솔의 보고를 통해서 적절한 분석을 수행하고 환경 내의 변수를 파악할 수 있습니다.

9. 콘텐츠 인식 보호 차단 정책 설정

이전에 만들어진 "보고만" 콘텐츠 인식 정책에서 전환된 "차단" 정책을 사용할 것입니다. 콘텐츠 인식 보고서 검토가 이루어지면 네트워크 환경의 여러 클라이언트 시스템 테스트를 수행 후 정책을 만는 것이 가장 좋습니다. 우선 "보고만" 정책을 이용하는 것이 좋습니다.

"차단" 정책을 만들기 위해서 정책 관리 페이지에서 복제 기능을 사용합니다. '콘텐츠 인식 보호 > 콘텐츠 인식 정책' 섹션에서 사용할 수 있습니다. 각 "보고만" 정책에서 오른쪽에 '복제' 아이콘을 선택합니다. 이 아이콘은 오른쪽 세 가지 아이콘 중 두 번째에 위치해 있습니다.



각 "차단" 정책의 복제 아이콘 바로 위에 위치한 편집 아이콘을 클릭해서 '정책 작업'을 차단으로 수정합니다. "차단 및 수정" 옵션은 프리미엄 라이선스 패키지라는 것을 기억해 주시기 바랍니다. 차단 정책을 수정 후 저장을 하고 기존의 "보고만" 정책을 토글을 이용하여 OFF 합니다.

10. eDiscovery 수정 조치 수행

eDiscovery 검색이 완료되면 수정 작업을 수행할 수 있습니다. '대상 암호화', 대상 복호화', '대상 삭제'의 옵션이 있고 'eDicovery > 검색 결과 및 액션' 섹션의 작업 컬럼에서 찾을 수 있습니다.

이 작업은 엔드포인트에 저장된 민감한 데이터를 찾아서 잠재적 위험을 완화하는데 도움을 줍니다. 예를 들어 사용자 엔드포인트에 고객 PII 데이터를 가지고 있으면 GDPR과 같은 개인정보보호 법률 등을 위반 할 수도 있습니다.

11. 암호화 정책 구성

이동 데이터 보호는 제 3업체가 기밀 정보에 접근하지 못하도록 보장하기 위해서 필수적입니다. USB 저장 장치에 데이터 저장이 필요할 때 이러한 장치의 분실 또는 도난에 대비하기 위해 암호화는 최고의 솔루션이 될 수 있습니다. EasyLock은 기밀 데이터 보호를 위한 크로스 플랫폼, 엔터프라이즈용, 데이터 암호화 솔루션으로 설계 되었습니다.

EasyLock 암호화 정책 - USB 저장 장치에 강력한 암호화 기능을 제공합니다. 컴퓨터 자체에서 설치가 요구되고 매체 제어와 연동합니다. 매체 제어의 'TD 1+ 장치 사용 허용'을 사용하면 Endpoint Protector 로 보호되는 컴퓨터에 연결된 USB 저장 장치에 EasyLock을 자동으로 설치하고 암호 재설정, 메시지 전송, 장치 초기화 등의 원격 관리 기능을 제공합니다.

직관적인 드래그 앤 드롭 인터페이스로 파일은 빠르게 암호화되어 복사되고 작업 흐름의 중단없이 안전하고 효율적으로 사용할 수 있습니다.