Advanced Data Loss Prevention (DLP)

Acronis Cyber Protect Cloud용

2022년 3월 출시 예정

고객별 자동 정책 생성 기능으로 MSP(매니지드 서비스 제공업체)를 위해 설계된 DLP(데이터 손실 방지) 솔루션 활용하기

72%의 직원이 민감한 회사 정보를 공유하는 것으로 알려진 지금, Ponemon Institute가 조사한 결과에 의하면 내부자 관련 사고가 전체 위반 행위의 45%를 차지합니다. 그러나 기존의 DLP 솔루션을 통해 그러한 위험을 해소하려면 막대한 비용을 들여 광범위하게 보안 전문 기술을 동원하고 가동해야 합니다. DLP 정책은 포괄적이지 않고 비즈니스 중심적이므로, 고객의 고유한 비즈니스 요구를 파악하고 이를 DLP 정책에 수동으로 매핑하는 길고 소모적이며 수동적인 구성 프로세스로 전락합니다.

Acronis Advanced DLP를 이용하면 프로비저닝 및 관리가 놀랍도록 단순해지므로, 주변 장치 및 네트워크 커뮤니케이션을 통해 고객의 워크로드에서 데이터가 유출되는 것을 방지할 수 있습니다. 기준 DLP 정책이 자동으로 생성되므로 각 고객의 비즈니스 고유 정책을 정확하고 효율적으로 만들 수 있습니다.

간소화된 데이터 손실 방지로 서비스 스택 개선

컨텍스트 및 내용 인식 DLP 제어	고객 고유의 기준 DLP 정책 자동 생성	적응형 DLP 정책 시행
데이터 전송 내용 및 컨텍스트를 분석하고 정책 기반의 예방적 제어를 시행함으로써 주변 장치 및 네트워크 커뮤니케이션을 통해 워크로드에서 데이터 유출이 발생하지 않도록 하여 고객의 민감한 데이터를 보호하십시오.	이제는 수동으로 고객 비즈니스 세부 정보를 드릴다운하고 정책을 정의할 필요가 없습니다. 민감한 발신 데이터 흐름을 모니터링함으로써 비즈니스 고유의 기준 DLP 정책이 자동으로 생성됩니다. 시스템이 이러한 정책을 시행하기 전에 고객이 미리 유효성을 검사할 수 있습니다.	DLP 정책을 처음 시행한 후 관리 및 조정하는 데 일반적으로 필요한 수동 작업을 없앨 수 있습니다. 적응형 정책 시행 옵션은 고객의 워크로드에서 감지된 이전에 사용된 적 없던 새 데이터 흐름으로 시행 정책을 자동 확장합니다.

새로운 수익 창출 기회

- 수요가 높은 MSP 관리형 DLP 서비스로 **고객별 매출 증가**
- 고객의 DLP 인식을 개선하는 관찰 모드로 서비스 가치를 입증하여 **더 많은 고객 확보**
- 백업 및 재해 복구, 차세대 안티맬웨어, 이메일 보안, 워크로드 관리 및 DLP용 단일 통합형 플랫폼을 사용하여 한층 더 쉽게 단계적 서비스를 수행함으로써 **TCO 제어 및 수익 증대**

생산성 향상 및 급격한 비용 증가 방지

- 자동화된 고객 고유의 기준 DLP 정책 생성을 통해 **프로비저닝 및 구성에 소요되는 시간 단축**
- 기준 정책 생성 및 간단한 시행 전 고객 유효성 검사 과정에서 이루어지는 민감한 데이터 전송에 대한 선택적 최종 사용자 타당성 확인을 통해 **비즈니스 요구 사항에 맞는 DLP 정책 규정 및 오류 최소화**
- 구성 가능한 로그 수집, 경고 및 정보 제공용 위젯을 통해 **규정 준수 보고 간소화 및 DLP 성능의 가시성 향상**

고객 데이터 유출 위험 감소

- 주변 장치 및 네트워크 커뮤니케이션을 통한 민감한 정보 유출을 방지함으로써 **고객 측 내부자와 관련된 데이터 위반의 위험 최소화**
- **사람의 오류가 미치는 영향을 최소화하고 허용 가능한 데이터 사용 정책을 회사 차원에서 시행**
- 규제 대상인 데이터를 보호함으로써 **고객의 규정 준수 수준 강화**

경쟁 우위를 확보함으로써 DLP 서비스 차별화

자동화된 DLP 정책 생성	고객 고유의 DLP 정책	비교 불가능한 제어된 채널 조합	포괄적인 DLP 제어	단일 콘솔을 통한 중앙 집중식 사이버 보호
수동 작업 및 오류 위험을 최소화합니다. 각 고객의 기준 DLP 정책을 자동으로 생성하여 프로비저닝을 간소화합니다.	조직 전체에서 민감한 발신 데이터 흐름을 모니터링하여 고객의 비즈니스 프로세스를 DLP 정책에 자동으로 매핑합니다. 정확도 향상을 위해 선택적 최종 사용자 지원을 활용하고 정책을 시행하기 전에 고객 유효성 검사를 요청합니다.	이동식 스토리지, 프린터, 리디렉션된 매핑 드라이브 및 클립보드, 이메일 및 웹메일, 인스턴트 메신저, 파일 공유 서비스, 소셜 네트워크, 네트워크 프로토콜 등을 포함한 로컬 및 네트워크 채널 전체에서 데이터 흐름을 제어합니다.	어떤 웹 브라우저에서나 소셜 미디어, 웹메일 및 파일 공유 서비스로의 데이터 전송을 제어합니다. 원격 컴퓨터 및 오프라인 컴퓨터의 이미지에서 발신 인스턴트 메시지 및 민감한 데이터 감지에 대한 내용 검사를 이용합니다.	백업, 재해 복구, 차세대 안티맬웨어, 이메일 보안, 워크로드 관리 및 DLP를 통합한 단일 솔루션을 사용하여 TCO를 제어하고 관리 오버헤드를 줄이며 수익을 증대합니다.

고객 프로비저닝 및 DLP 정책 생성과 관리 간소화

MSP(매니지드 서비스 제공업체)의 프로비저닝 및 관리 작업 간소화에 도움을 주기 위해 고급 데이터 손실 방지(DLP)는 2개의 서로 다른 모드를 지원합니다.

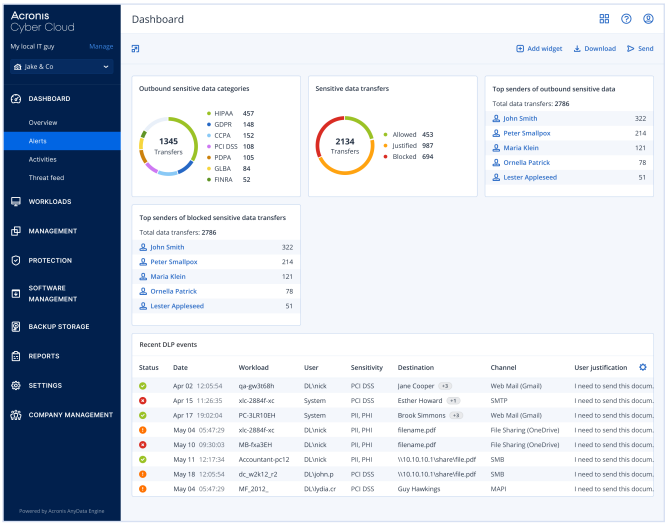
관찰 모드

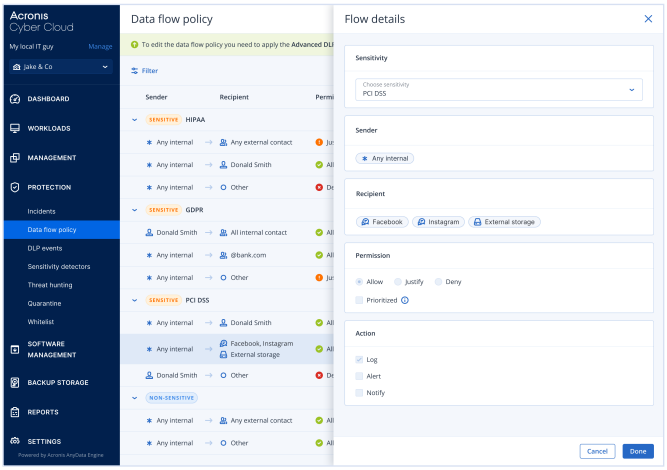
데이터 손실 방지 서비스의 가치를 입증하고 고객의 DLP 인식을 증진합니다. 관찰 모드의 에이전트는 고객의 엔드포인트 컴퓨터에서 민감한 발신 데이터 흐름을 모니터링하여 기준 DLP 정책을 자동으로 생성하며, 가장 위험한 데이터 전송에 대해서는 선택적으로 최종 사용자 검증을 실시합니다.

시행 모드

고객의 DLP 정책에 대한 검증이 완료되면 정책을 시행하여 데이터 보호를 시작할 수 있습니다. 시행 모드에서는 DLP 정책 시행 방법을 선택할 수 있습니다.

- **엄격한 시행** – 새 데이터 흐름 규칙을 적용하여 확장하지 않고 정의된 그대로 DLP 정책을 시행합니다. 정책에 정의된 데이터 흐름 규칙과 일치하지 않는 데이터 전송은, 최종 사용자가 차단 무시를 실행하는 일회성 비즈니스 관련 예외를 요청하지 않는 한 감지되는 대로 차단됩니다.
- **적응형 시행** – DLP 정책을 시행하지만, 이전에 관찰되지 않았던 비즈니스 관련 데이터 흐름을 허용하는 새 규칙에 따라 확장할 수 있는 유연성을 제공합니다.





Acronis

www.acronis.com에서 자세히 알아보세요.