Acronis

백서

DLP 서비스, 시작과 확장
MSP를 위한 가이드라인

수년간 모든 규모의 기업은 인지도 향상, 보안 프로토콜 및 규제에도 불구하고 데이터 유출 위험을 해결할 수 없었습니다. 실제로 2021년 연말 보고서: Risk Based Security의 Data Breach QuickView에 따르면 220억 개 이상의 기록이 노출되어 2005년부터 유출된 기밀 데이터의 양이 두 번째로 많은 해였습니다. 이러한 기록은 압도적으로 데이터 유출로 인해 드러났습니다. 데이터 유출은 기밀 데이터, 민감한 데이터 또는 보호 데이터가 우발적으로 또는 고의적으로 신뢰할 수 없는 환경 또는 조직 안팎의 권한 없는 사용자에게 공개되는 보안 위반 상황으로 정의됩니다.

그렇다면 무엇이 데이터 유출로 이어질까요? 두 가지의 주요 원인이 있습니다.

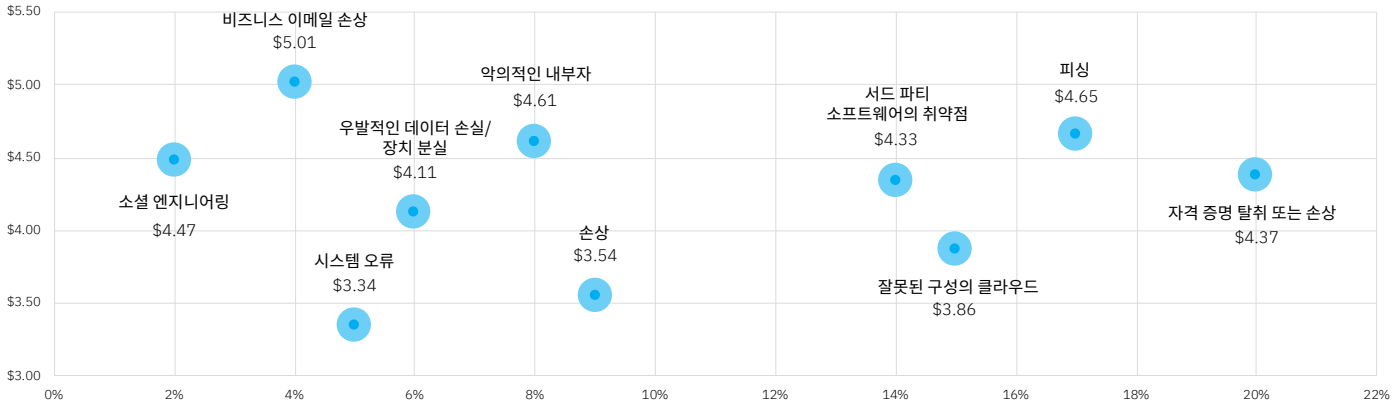
1. 외부의 사이버 위협

MITRE ATT&CK 프레임워크에 정의된 대로 데이터 유출은 악의적인 공격자가 공격 중에 수행하는 마지막 전술 중 하나입니다. Verizon의 2022년도 데이터 침해 조사 보고서(Data Breach Investigations Report)에 따르면 데이터 침해의 80% 이상에서 공격자의 동기는 재정적 이득입니다.

이것이 바로 대부분의 공격에서 민감한 데이터가 주요 대상인 이유입니다. 악의적인 공격자가 기업 환경에 대한 액세스 권한을 설정하면 여러 채널을 통해 데이터 유출을 시도할 수 있습니다. 공격이 점점 더 복잡해지고 보안 계층을 우회할 수 있게 되면서 조직 데이터에 대한 위험이 기하급수적으로 증가하고 있습니다.

2. 내부의 위험

안티맬웨어 및 기타 엔드포인트 보안 기술로 외부 공격을 감지하고 차단할 수 있긴 하지만, 내부자와 관련된 데이터와 같은 조직 데이터에 대한 다른 위험이 증가하는 추세입니다. 대표적인 예시 하나는 최종 사용자가 본인도 모르게 권한이 없는 당사자에게 데이터를 공개하는 것입니다(예: 이메일 전달). 이는 우발적인 직원 실수, 잘못된 구성의 IT 또는 악의적인 내부자를 통해 발생할 수 있습니다. 이 모두는 조직에 심각한 위협이 될 수 있으며 가장 비용이 많이 드는 데이터 침해로 이어질 수 있습니다.



일부 조직에서는 내부 위험의 영향을 과소평가하고 있지만 Ponemon Institute의 2021년 데이터 침해 비용에 관한 보고서(Cost of Data Breach Report)에 따르면 데이터 침해의 약 3분의 1이 내부자와 관련이 있다고 명시되어 있습니다.

데이터 유출이 기업에 미치는 영향

데이터 유출은 기업에 심각한 위험을 초래합니다. 권한 없는 당사자에게 민감한 데이터가 유출되면 다음과 같은 결과가 발생합니다.

- **규정 미준수** – 직원 및 고객 개인 식별 정보(PII), 건강 정보(PHI), 카드 소지자 데이터와 같은 민감한 데이터의 저장, 액세스 및 보호는 GDPR, CCPA, HIPAA, PCI-DSS, 등의 로컬 및 국제 규정에 의해 엄격하게 규제됩니다. GDPR과 같은 일부 규정에서는 엄격한 기간 내에 침해 내용을 보고해야 합니다. 규제된 데이터 침해의 보고가 지연되는 경우 조직은 큰 벌금을 물어야 하며 규정 준수 인증을 상실할 수도 있습니다.
- **재정적 피해** – 데이터가 유출되면 MSP 고객이 받을 수 있는 규제 벌금 외에도 서비스 제공업체는 소송으로 이어질 수 있는 고객 보안에 대한 책임으로 인해 재정적 피해 위협에 노출될 수 있습니다. 또한, 영업 비밀이나 지적 재산의 유출은 기업에 추가적인 재정적 손실을 초래하고 시장에서의 지위를 불안정하게 만들 수도 있습니다.
- **평판 위험** – 데이터 침해를 비판하는 보도가 이어지는 경우 기업에 악영향을 미칠 수 있습니다. 이는 고객 이탈로 이어질 뿐만 아니라 기존 파트너십과 신규 고객 확보 능력에도 지장을 줄 수 있습니다. 고객 데이터 유출은 기업의 평판과 비즈니스에도 영향을 줄 수 있습니다.

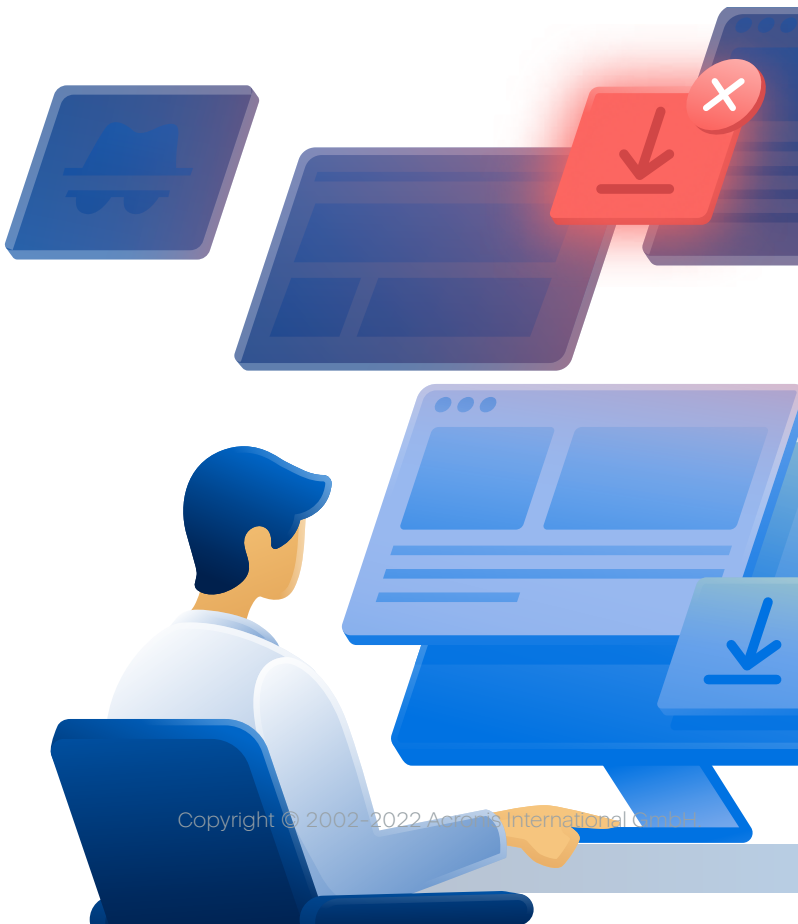
데이터 손실 방지란 무엇일까요?

데이터 손실 방지: 오랫동안 확립된 보안 솔루션의 카테고리로, 기밀 데이터 및 민감한 데이터를 무단으로 사용, 전송 및 저장하는 경우 이를 감지하고 방지하는 통합 정보 보안 기술 시스템을 의미합니다.

DLP 솔루션: 데이터 흐름 제어와 콘텐츠 분석 방법의 조합을 적용하여 수행합니다. 이러한 기술은 민감한 데이터가 내/외부 모두의 권한 없는 수신자에게 유출되는 것을 방지하는 기업 허용 데이터 사용 및 처리 정책을 조직 전체에 시행합니다.

데이터 보호는 주로 백업 및 재해 복구와 관련이 있지만 DLP, 공증 및 암호화와 같은 다른 필수 기술은 데이터 유출을 비롯한 다양한 위협으로부터 민감한 정보를 보호합니다.

유일한 기술 DLP: DLP는 조직 전체에 걸쳐 흐르고 저장되는 민감한 데이터에 대한 가시성과 제어를 제공하여 권한 없는 엔터티에 대한 유출을 방지할 수 있는 유일한 기술입니다.



데이터 상태 및 기능별 DLP의 데이터 보호 방법

조직 내에 데이터가 있을 수 있는 **세 가지 주요 상태**는 다음과 같습니다.

- **사용 중인 데이터:** 로컬 채널(예: 주변 장치, 이동식 스토리지) 또는 엔드포인트 컴퓨터의 애플리케이션에서 사용/전송되는 데이터입니다. 예를 들어 엔드포인트 컴퓨터에서 USB 드라이브로 전송되는 파일 등입니다.
- **이동 중인 데이터:** 컴퓨터 시스템 간 이동하거나 전송되는 데이터입니다. 예를 들면 로컬 파일 스토리지에서 클라우드 스토리지로 전송 중인 데이터 또는 인스턴트 메신저나 이메일을 통해 엔드포인트 컴퓨터에서 다른 엔드포인트로 전송되는 데이터입니다.
- **저장된 데이터:** 로컬 또는 네트워크에 저장 중인 데이터로 현재 액세스되거나 전송되지 않는 데이터를 의미합니다. 예를 들면 네트워크 공유 또는 온프레미스 서버에 저장된 데이터입니다.

일부 데이터는 엔드포인트의 전체 수명 주기 동안 단일 상태로 유지될 수 있지만 데이터는 자주, 그리고 지속적으로 상태를 변경한다는 사실에 유의해야 합니다. 다양한 데이터 상태와 특징 및 차이점을 이해하면 고객이 조직 데이터를 보다 안전하게 처리하고 유출로부터 보호할 수 있습니다.

각각의 데이터 상태를 보호하기 위해 사용되는 DLP는 다음과 같이 세 가지의 주요 '기능적' 유형이 존재합니다.

- **사용 중인 데이터 DLP**
- **이동 중인 데이터 DLP**
- **저장된 데이터 DLP**

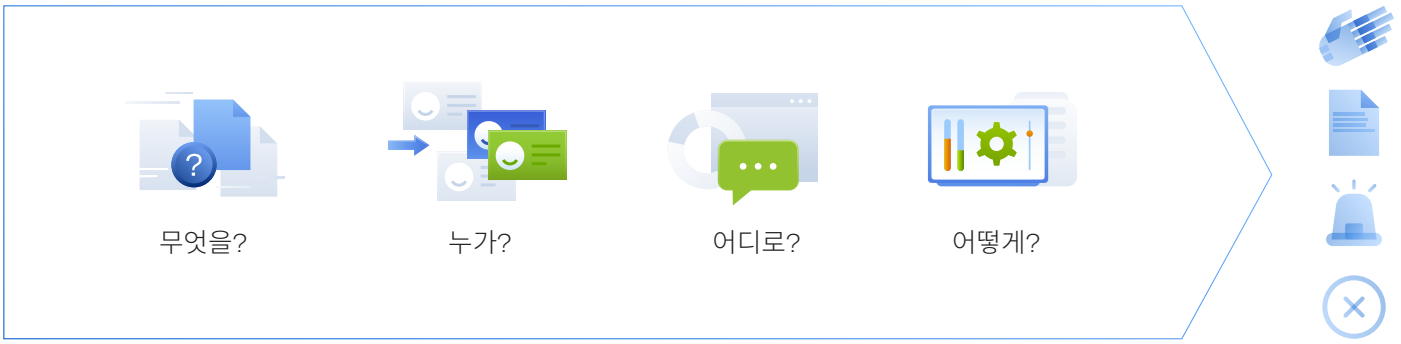
ID 관리 또는 암호화와 같은 다양한 데이터 위험(예: 접근성, 개인 정보 보호 위험)을 해결할 수 있는 다른 기술이 있다는 점에 주목할 필요가 있습니다. 그러나 DLP는 데이터 흐름에 대한 가시성을 제공하는 동시에 데이터 유출 방지라는 중대한 목적을 가지고 다양한 상태의 데이터를 보호할 수 있는 유일한 기술입니다.

DLP 제어: 콘텐츠 VS 컨텍스트

조직의 각 데이터 흐름은 각각 컨텍스트와 콘텐츠가 있습니다. 컨텍스트는 데이터 흐름과 관련 사용자, 사용된 채널, 흐름 방향 등과 같은 환경적 요인을 가리킵니다. 콘텐츠는 환자 건강 기록, 직원 개인 식별 정보(PII)와 같이 전송되는 정보의 실제 유형/카테고리를 의미합니다.

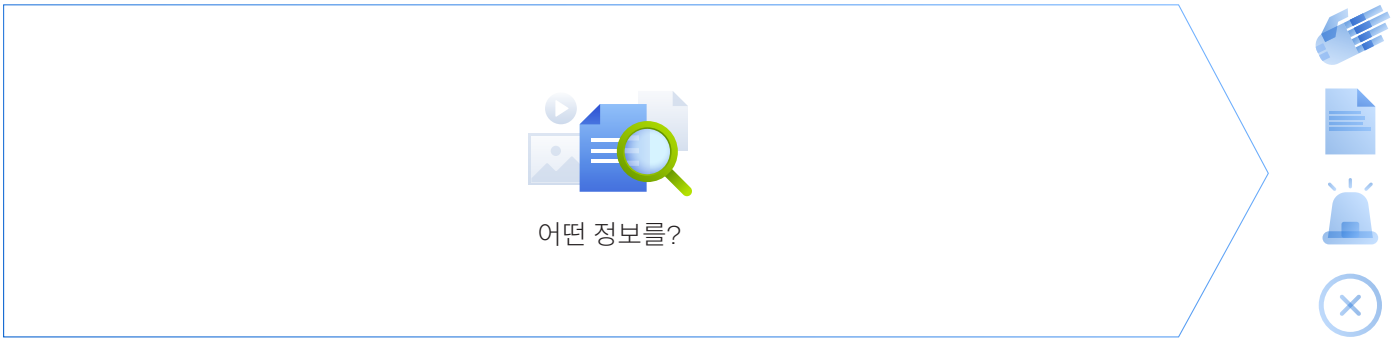
효율적인 DLP 솔루션은 컨텍스트와 콘텐츠를 기반으로 데이터 흐름에 대한 제어를 구현해야 합니다.

- **컨텍스트 인식 DLP 제어** – 관련 사용자, 사용된 채널, 전송 데이터 방향, 목적지, 시간 등과 같은 속성을 사용하여 작업 컨텍스트를 기반으로 데이터 전송 작업을 제어합니다.



예: 사용자가(누가) 데이터를(무엇을) 암호화된 USB 장치로(어디로) 복사하는 것을 허용하고, 암호화되지 않은 USB 장치로 데이터를 복사하는 것을 차단하는 정책입니다.

- **콘텐츠 인식 DLP 제어** – 실제 전송되는 정보(콘텐츠)의 유형과 민감도를 기반으로 데이터 흐름을 보다 심층적으로 제어합니다.

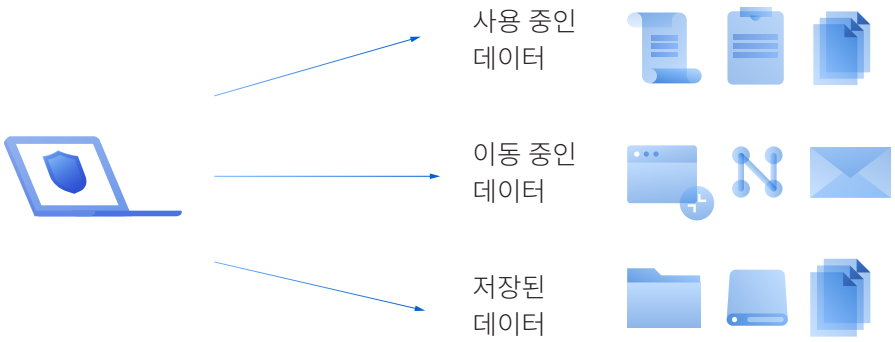


예: HIPAA 관련 정보를(어떤 정보를) 포함하는 문서는 어떤 USB 장치로도 복사할 수 없습니다.

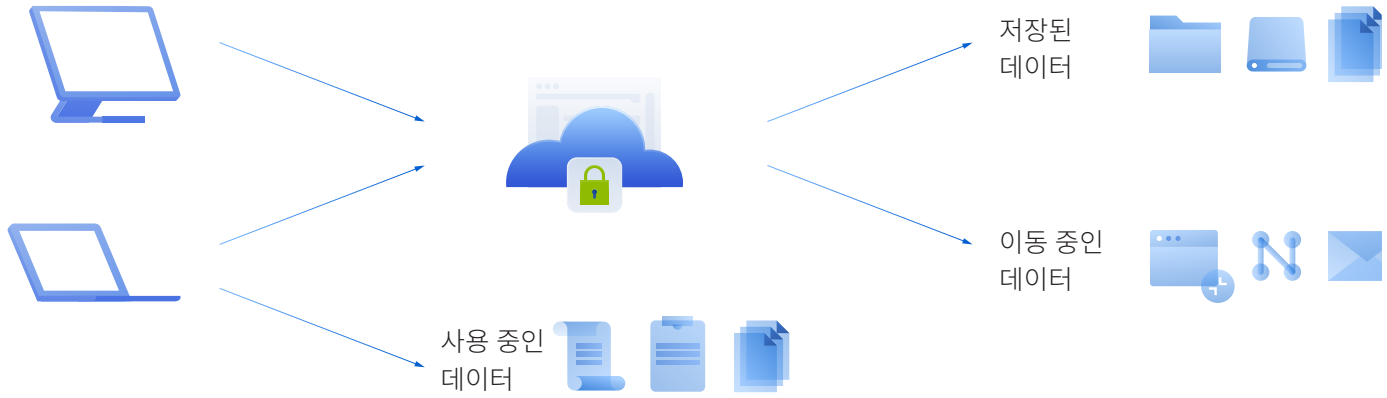
DLP 아키텍처 유형

DLP는 배포 및 운영 방식에 따라 다음과 같이 세 가지의 주요 유형이 존재합니다.

- **엔드포인트 DLP** – 엔드포인트 컴퓨터에서 DLP 에이전트를 사용하고 기업 네트워크 또는 인터넷에서 사용하는지에 관계없이 이러한 컴퓨터에서 사용 중인 데이터, 이동 중이거나 저장된 데이터가 유출되는 것을 방지하는 솔루션입니다.



- **네트워크/클라우드 DLP** – 하드웨어/가상 DLP 게이트웨이 및 서버를 포함한 네트워크 내의 컴포넌트만으로 구성된 솔루션으로, 기업 네트워크에 위치한 컴퓨터에서 이동 중이거나 저장된 데이터를 보호하여 권한 없는 수신자와 기업 네트워크 외부에 있는 목적지로 데이터가 유출되는 것을 방지합니다.



- **하이브리드 DLP** – 네트워크 및 엔드포인트 DLP 컴포넌트를 모두 활용하여 엔드포인트 및 네트워크 DLP 아키텍처의 모든 기능을 수행하는 솔루션입니다.

여기서 기억해야 할 것은 네트워크 DLP는 아키텍처로 인해 사용 중인 데이터를 보호할 수 없고 기업 네트워크 외부에 있는 권한 없는 당사자에 대해서만 데이터 유출을 제어할 수 있는 반면 엔드포인트 및 하이브리드 DLP는 모든 상태의 데이터를 보호하고, 내/외부의 권한 없는 당사자에 대해 데이터 유출을 방지할 수 있다는 사실입니다.

이 안내서는 엔드포인트 DLP 아키텍처를 기반으로 DLP 서비스를 시작하고 실행하며, 확장하는 방법에 중점을 둡니다.

고객에게 DLP가 필요한 이유

Ponemon Institute의 2021년 데이터 침해 비용에 관한 보고서에 따르면 데이터 침해로 인한 전 세계 평균 총 비용은 424만 달러로 2020년에 비해 10% 증가했습니다. 데이터 침해 비용의 증가에서 확인할 수 있듯 침해를 식별하고 방지하는 데 걸리는 실제 평균 시간은 287일입니다. 이것은 침해 방지 전 고객이 직면하게 되는 막대한 위험을 의미합니다. 이러한 위험은 재정과 평판 및 규정 준수 비용으로 이어질 수 있습니다.

DLP 서비스를 사용하여 고객의 위험을 줄일 수 있는 주요 방법은 다음과 같습니다.

- **규정 준수 달성 지원:** 규정 준수를 달성하고 PII(GDPR, CCPA), PHI(HIPAA), 결제 카드 정보(PCI DSS) 등과 같은 규제 대상 정보 보호를 지원합니다
- **고객 정보 보호:** 고객의 지적 재산 및 영업 비밀을 보호합니다
- **위험 최소화:** 소셜 엔지니어링으로 인한 맬웨어 및 공격에 의한 데이터 유출 위험을 최소화합니다
- **원격 작업 강화:** 원격 작업 및 BYOD 보안을 강화하고 민감한 데이터가 프라이빗 클라우드 기반 스토리지로의 전송을 방지합니다
- **데이터 유출 방지:** 직원의 우발적인 실수와 부주의 또는 위법 행위에 의한 데이터 유출을 방지합니다
- **신속한 대응 활성화:** DLP 이벤트에 대한 지속적인 가시성을 바탕으로 데이터 유출 사고 및 침해 후 조사에 대한 신속한 대응을 활성화합니다
- **데이터 유출 방지:** 직원의 우발적인 실수와 부주의 또는 위법 행위에 의한 데이터 유출을 방지합니다

DLP 서비스 제공 흐름

DLP 서비스 시작, 실행 및 확장 방법에 대한 자세한 내용을 살펴보기 전에 먼저 DLP 서비스의 특징으로 인해 다음의 단계를 포함한 구체적인 제공 흐름이 있다는 사실에 유의하는 것이 중요합니다.

- **DLP 에이전트 디플로이:** 회사 데이터에 대한 철저한 보호를 위해 DLP 서비스로 프로비저닝을 진행할 엔드포인트를 결정하고, 해당 엔드포인트에 DLP 에이전트를 배포하는 것이 서비스 제공 프로세스의 첫 번째 단계입니다. 민감한 데이터가 생성되거나, 저장 또는 사용되는 모든 워크로드에 DLP 에이전트를 프로비저닝하기를 권장합니다. 워크로드가 보호되지 않은 상태로 계속 유지되면 기업 IT 보안 시스템에 잠재적인 데이터 유출 격차가 발생합니다.

- **DLP 정책 생성:** 또 다른 초기 단계로는 데이터 유출을 방지하기 위해 적절한 데이터 사용 및 처리 정책을 보장하는 DLP 정책을 생성하는 것입니다. 사용된 DLP 기술에 따라 이 단계가 디플로이보다 먼저 진행될 수도 있습니다. **중요한 점**은 조직마다 내부 프로세스가 다르고 규정과 데이터 액세스 및 공유 요구 사항 또한 다르기 때문에 DLP 정책이 보편적이지 않으며 고객별로 다르다는 점입니다. DLP 정책 생성의 특징으로 인해 수동으로 정책 관리가 필요한 기존 DLP 솔루션은 서비스 제공업체가 DLP 서비스 구축을 위한 사용에 상당한 복잡성과 비용의 장벽을 제시합니다.
- **DLP 정책 유효성 검사**: 초기 DLP 정책 생성 후 중요한 단계는 각 고객의 기업 특징을 깊이 이해할 수 없기 때문에 이러한 정책이 기업 요구 사항에 맞도록 고객과 함께 유효성을 검사하는 단계입니다. 정책의 시각적 표현이 더 복잡하고 '기술적'일수록 정책 유효성 검사를 위해 고객에게 요구되는 시간 작업과 전문 지식이 증가합니다.
- **DLP 정책 시행 및 관리:** 고객이 DLP 정책 유효성을 검사하면, 민감한 기업 데이터가 유출되지 않도록 보호하기 위해 정책을 시행할 수 있습니다. DLP 기술은 조직의 민감한 데이터 흐름을 제어하여 권한 없는 데이터의 흐름을 차단합니다. 그러나 비즈니스가 끊임없이 발전하여 새로운 프로세스가 도입되고 새로운 데이터 규정이 생기면 기존의 규정이 변경될 수 있습니다. 따라서 새로운 필수 데이터 흐름은 차단되지 않고 모든 데이터 유출 시도는 방지할 수 있도록 초기 DLP 정책을 끊임없이 변화하는 기업 요구 사항에 맞게 지속적으로 조정해야 합니다. 이러한 조정은 수동 정책 미세 조정 또는 자동 적응형 정책 조정 방법으로 달성할 수 있습니다.
- **DLP 서비스 가치 보고:** DLP 서비스의 가치를 증명하기 위해 차단된 민감한 데이터 전송 및 DLP 관련 최종 사용자 작업에 대한 지속적인 보고는 고객 유지율을 높이고 데이터 유출 문제를 인식하지 못하는 고객의 위험을 줄이는 데 유용합니다.

현 DLP 솔루션의 MSP 관련 과제

DLP는 서비스 공급업체 및 중견중소기업 고객과 같은 오랫동안 확립된 참여업체를 보유한 성숙한 기업 중심의 시장으로서, DLP 제어에 대한 비즈니스 특징을 지속적으로 심층적으로 이해하고 매핑해야 하는 필요성과 규제 요구 사항에 대한 지식 및 이러한 기술의 운영을 위한 데이터 규정 준수에 대한 이해를 바탕으로 더 넓은 시장에서의 채택을 위해 노력해 왔습니다. 이로 인해 DLP 업계는 비용이 많이 드는 DLP 관리 전담 사내 전문 지식을 감당할 수 있는 대규모 조직에 주로 집중하게 되었습니다.

MSP가 DLP 서비스를 구현하고 실행할 때 직면하는 주요 과제는 다음과 같습니다.

- **많은 비용을 들여 복잡한 DLP 서비스 실행** - 기존 DLP 솔루션에는 초기 정책 생성 및 후속 조정을 위한 복잡한 수동 프로세스가 필요하므로 고객에게 효율적인 DLP를 구현하는 데 들이는 시간과 가치 창출 노력이 필요하여 서비스 비용이 너무 많이 듭니다. 또한 이러한 복잡성으로 인해 일반 IT 보안 전문가를 고용하는 것보다 훨씬 어렵고 비용이 많이 드는 DLP 전문가를 고용해야 합니다.

- **효율적인 DLP를 위한 고객별 정책 필요** – 앞서 언급한 것처럼 조직의 비즈니스 프로세스와 데이터 민감도는 각기 다르며 계속해서 변화하므로 기업별로 지속적인 DLP 정책 조정이 필요합니다. 그러나 MSP는 각 고객의 비즈니스 프로세스에 대한 깊은 이해가 부족하며 지속적으로 유지할 수도 없습니다. 이것은 기존 DLP 기술을 사용하는 MSP에 상당한 확장성 문제를 제기하는 장벽입니다.
- **잘못 구성된 DLP 정책으로 인한 비즈니스 연속성 저하** – 수동 DLP 정책 생성 및 구성은 복잡성과 세분성으로 인해 오류가 발생하기 쉽습니다. 반면 DLP 기술은 권한이 없는 데이터의 흐름을 차단합니다. 이러한 복잡성과 DLP 방지 기능이 결합되면 DLP 정책이 잘못 구성되거나 새로운 비즈니스 프로세스가 이러한 정책에 일관되게 매핑되지 않는 경우 비즈니스에 필요한 데이터 흐름을 실수로 차단하여 필수 비즈니스 프로세스를 중단시킬 수도 있습니다.
- **고객의 가장 취약한 연결고리인 직원** – MSP와 고객이 DLP 기술에 거의 액세스할 수 없는 경우에도 직원을 대상으로 하는 인적 오류와 외부 공격은 데이터 유출의 주요 원인입니다. 서비스 제공업체가 다른 엔드포인트 보호 계층으로 외부 위협의 위험을 제한할 수 있더라도 사용자가 모르는 사이에 민감한 데이터를 공개하여 데이터 침해를 일으키게 되면 서비스 제공업체가 책임을 져야 합니다.
- **데이터 유출 문제를 인지하지 못하는 고객** – DLP 액세스의 어려움으로 인해 고객이 데이터 유출 문제를 인지하지 못할 수도 있습니다. DLP 서비스를 출시한다는 것은 서비스 제공업체가 고객이 직면한 데이터 유출 위험과 조직의 규모에 관계없이 조직에 심각한 위협을 줄 수 있는 위험을 해결하는 유일한 기술인 DLP에 대해서도 교육해야 한다는 것을 의미합니다.

자동 행동 기반 정책 생성, 확장 및 모니터링과 같은 시장의 새로운 트렌드와 기술은 규제 요구 사항 외에도 끊임없이 진화하는 비즈니스 절차에 맞게 빠르게 변화하는 DLP 규칙 문제를 해결하고 있습니다. 이러한 새로운 기능은 DLP 시장을 효과적으로 민주화하고 서비스 제공업체와 고객이 DLP 시장에 액세스할 수 있도록 합니다. 지금이 바로 DLP 서비스를 통해 포트폴리오를 확장할 수 있는 절호의 기회입니다.

DLP 서비스 계획 및 시작

DLP 서비스를 계획하고 시작하는 첫 번째 단계는 고객이 실제로 DLP를 필요로 하는지 확인하는 것입니다.

고객이 다음 지표의 일부 또는 전부를 보유한 경우 데이터 유출 위험을 줄이기 위해 DLP 서비스가 필요합니다.

- 규정이 적용되는 민감한 데이터로 워크로드를 생성, 저장 또는 작업
- 유출되면 안 되는 영업 비밀 또는 지적 재산을 보유
- 규제가 엄격한 업종에 해당
- 데이터 침해를 경험했고 해당 환경을 보호하고 위험을 줄이고자 함
- 규정 준수 인증을 보유/필요
- 책임을 경감하기 위한 사이버 보험료를 지불/고려 중
- 전담 보안 직원 및 전문 지식 부족

다음은 오랫동안 DLP에 관심을 보인 업종입니다.

- 은행 및 재정 서비스
- 헬스케어
- 법무
- IT 및 통신
- 정부 및 공공 부문
- 제조
- 소매 및 물류
- 교육
- 에너지학

이러한 지표에 해당하거나 앞서 언급한 업계에 종사하는 고객이 있는 경우 데이터 유출 위험을 줄이고 규정 준수의 강화라는 급증하는 고객의 요구 사항 충족을 위해 서비스 포트폴리오에 DLP를 추가하는 것을 고려할 때입니다.

서비스 계획 및 비용 추정

서비스 가격을 결정하는 세 가지 주요 요소는 바로 인건비와 제품 비용 및 기대 마진입니다. 다음은 각 항목이 가격 견적에 영향을 미치는 방법에 대한 설명입니다.

- **인건비:** 선택한 솔루션의 복잡성에 따라 서비스 기술자가 서비스를 프로비저닝하고 관리하는데 소요되는 시간과 필요한 IT 보안 전문 지식이 결정됩니다.
- **제품 비용:** DLP는 예전부터 대기업에서 주로 사용되었으며, 높은 비용이 들기 때문에 중견중소기업에서 감당하려면 부담이 됩니다. 고객층이 대부분 중견중소기업인 경우 고객에게 비용 부담이 크지 않은 서비스를 선택해야 합니다.
- **기대 마진:** 평균 MSP는 순환 매출 모델에서 판매되는 원격 제공 서비스에 대해 최대 50%의 총 마진을 가져옵니다.

Acronis Advanced DLP 팩으로 DLP 서비스 실행하기

아크로니스에서는 몇 개월 동안 디플로이하거나 팀을 유지하고, 개인 정보 보호법에 전문 자격증이나 학위가 없더라도 고객별 정책의 일관성을 자동으로 생성하고 지속적으로 유지하는 행동 기반 DLP를 제공합니다.

Acronis Advanced DLP 팩을 사용하면 이동 중인 데이터와 사용 중인 데이터에 대해 이전에 한 번도 경험하지 못한 수준의 단순성으로 포괄적인 DLP 보호 기능을 고객에게 제공하여 다음과 같은 작업을 수행할 수 있습니다.

- **새로운 수익 창출 기회:** 포트폴리오를 확장하여 더 많은 고객을 유치하고 이전에는 기업에만 제공되던 DLP 서비스를 통해 고객당 수익을 늘려 새로운 수익 창출 기회를 획득할 수 있습니다.
- **가치 창출 노력 최소화:** 관리의 복잡성, 비용 및 인력을 늘리지 않고도 DLP를 쉽게 실무에 추가하여 가치 창출 노력을 최소화합니다.
- **고객 보안 위험 완화:** 민감한 데이터 유출을 방지하여 고객 보안 위험을 완화합니다.
- **고객 규정 준수 강화:** GDPR, HIPAA 및 PCI DSS를 포함한 일반적인 규제 프레임워크에 대한 즉각적인 데이터 분류 템플릿을 사용하여 클라이언트 규정 준수를 강화합니다.
- **서비스 프로비저닝 및 관리 간소화:** DLP 서비스 프로비저닝, 초기 정책 구성 및 후속 조정을 자동화하여 서비스 프로비저닝 및 관리를 간소화합니다.
- **모든 규모의 고객 고유의 DLP 정책 보장:** 끊임없이 변화하는 기업 특징에 맞게 동작 기반 기술을 통해 DLP 정책을 자동으로 조정해서 모든 규모의 고객 고유의 DLP 정책을 보장하여 고객별 DLP 정책을 시행하기 전에 고객과 함께 간편하게 유효성을 검사할 수 있습니다.
- **DLP 이벤트에 대한 더 빠른 대응:** 중앙 집중식 정책 기반 감사 로그 및 보안 경고를 통해 DLP 이벤트에 더 빠르게 대응하고 DLP 서비스 운영, 정책 유지 관리, IT 보안 감사, 사고 조사를 간소화합니다.

Acronis Advanced DLP 팩

Acronis Cyber Protect Cloud용 Advanced DLP 팩은 고객의 민감한 데이터가 승인되지 않은 당사자에게 유출되지 않도록 보호된다는 사실을 알려 고객이 안심할 수 있도록 돕습니다. 고유한 행동 기반 기술을 통해 각 고객의 세부 사항을 기반으로 DLP 정책을 생성하고 지속적으로 확장할 수 있으며, 이전에는 볼 수 없었던 단순성과 최소한의 가치 창출 노력으로 서비스를 쉽게 시작할 수 있습니다.

Acronis

자세히 알아보기:
www.acronis.com