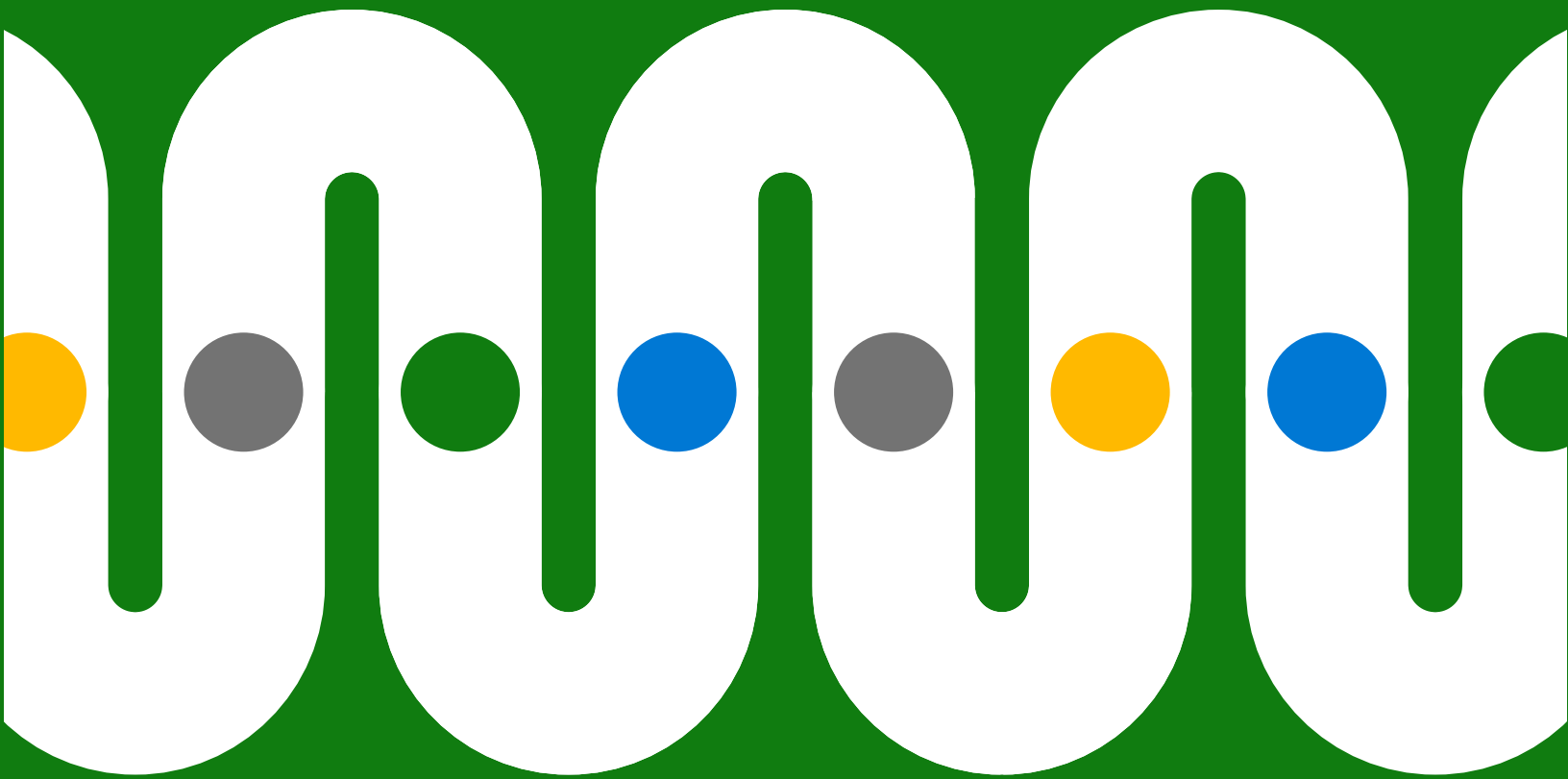
Microsoft Security

엔드 투 엔드 데이터를 보호하는 3단계



목차

규정 준수 의사 결정권자를 대상으로 진행한 한 설문조사에 따르면 95%가 데이터 보호 문제에 대해 우려하고 있는 것으로 나타났습니다.[2]

소개말

하이브리드 업무가 채택되면서 디지털 입지가 크게 증가하여 이미 기존 사무실을 훨씬 뛰어넘었습니다.

이로 인해 더 많은 데이터 조각화와 유출이 발생했으며, 이 모든 것은 다양한 애플리케이션, 디바이스, 업무 장소의 급속한 성장으로 인해 복잡해졌습니다. 또한 많은 직원들이 더 나은 업무 수행 또는 유연성을 찾아 직장 내 역할을 전환했습니다. 이러한 사실은 당면한 도전 과제에 또다른 부담을 지우고 있으며 계속 증가하는 데이터 영역에서 새로운 사각지대를 만들고 있습니다.[1]

이러한 모든 요인으로 인해 CIO와 CISO는 정보 보호에 대한 접근 방식을 재고하고 있습니다. 500명 이상의 미국 규정 준수 의사 결정권자를 대상으로 진행한 한 추적 설문조사에서 거의 모든 사람들(95%)이 데이터 보호 문제에 대해 우려하고 있었습니다.[2]

[1] "규모 개편 (Great Reshuffle)의 시기에 Microsoft가 내부자 위험을 줄이는 데 도움이 되는 방법, Alym Rayani", Microsoft 보안. 2022년 2월 28일.

[2] "512명의 미국 규정 준수 의사 결정권자를 대상으로 진행한 2021년 9월 설문조사, Microsoft의 의뢰로 Vital Findings에서 진행".

IT 및 보안 팀에서는 멀티클라우드, 하이브리드 클라우드, 온-프레미스 환경에 걸쳐 전체 데이터 수명 주기를 더 효율적으로 관리할 방법을 찾고 있습니다. 이 엔드 투 엔드 접근 방식에는 다음과 같은 주요 3단계가 포함됩니다.

1단계: 데이터 식별

데이터가 있는 위치, 데이터의 종류, 사용 또는 공유되는 방법 결정

2단계: 데이터 분류

적용할 올바른 정책과 위험 완화를 알 수 있도록 데이터 분류 및 레이블 지정

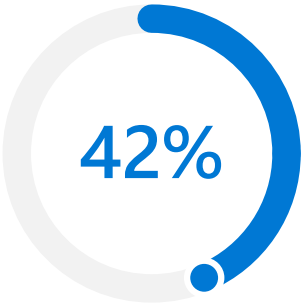
3단계: 데이터 손실 방지

인텔리전트한 감지 및 제어를 통해 직원을 위한 위험 감소와 유연성 간의 균형 유지

이 접근 방식의 목표는 무엇일까요? 바로 생산성 저하 없이 격차를 좁히고 위험을 최소화하는 것입니다.

1단계

데이터 식별



얼마나 많은 데이터가 '다크 데이터'인지 묻는 질문에 조직의 42%가 절반 이상이라고 답했습니다.[3]

이처럼 '숨겨진' 데이터는 이메일 첨부 파일에서 사용자 맞춤형 고객 통화 기록, 그리고 기계 로그 및 비디오 영상에 이르기까지 다양한 형태일 수 있습니다.

데이터가 어디에 있는지, 어떤 종류의 데이터인지, 또는 어떻게 사용 및 공유되고 있는지 식별할 수 없다면 적절한 정책 또는 보호를 적용하기란 불가능합니다.

현대 조직은 방대한 양의 데이터를 지속적으로 생성합니다. 문서, 이메일, 메시지뿐만 아니라 보안 영상에서 지리적 위치 데이터에 이르기까지 모든 데이터가 앱, 디바이스, 스토리지, 온-프레미스, 클라우드 전반에서 확산하여 더욱 복잡해집니다.

이 모든 데이터를 식별하는 것은 어려울 수 있으며 조직의 42%는 데이터의 절반 이상이 '다크 (dark) 데이터'라고 말합니다.[3] 즉, 수집되었지만 알려지지 않았거나 비즈니스 목적으로 사용되지 않은 정보입니다. 때로는 데이터를 생성한 사람이 프로젝트나 역할을 바꿀 때 데이터는 다크 데이터가 됩니다. 생성 또는 수정 시점에서 데이터를 식별할 수 있는 시스템이 없는 경우가 많습니다.

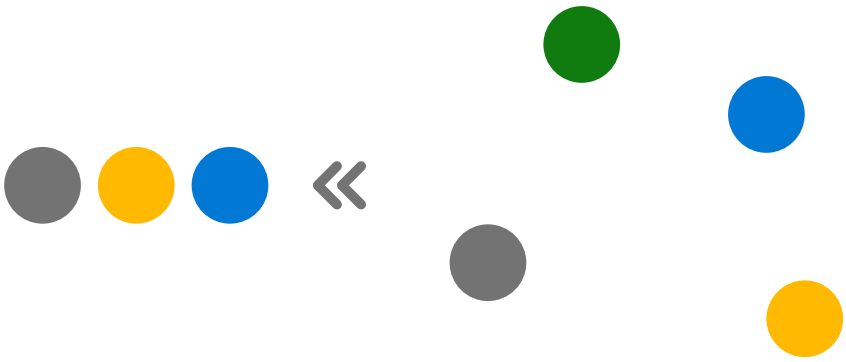
[3] "2022 State of Data Governance and Empowerment Report", Enterprise Strategy Group. 2022년 7월.

단일 플랫폼에서 엔드 투 엔드 검색 워크플로를 구축하고 싶으신가요?

Microsoft.com에서 Microsoft Purview에서의 데이터 검색에 대해 알아보세요.

이러한 어려움은 점점 더 심화될 것입니다. 생성, 캡처, 복제, 소비되는 새로운 데이터의 양은 2026년까지 두 배 이상 증가할 것으로 예상되며, 엔터프라이즈급 데이터는 소비자 데이터보다 두 배 이상 빠르게 증가할 것으로 예상됩니다.[4]

AI 및 ML(머신 러닝)은 이메일 주소, 건강 데이터, 신용 카드 번호 또는 지적 재산과 같은 민감한 데이터를 인식하고 자동으로 분류하여 도움이 될 수 있습니다. AI 및 ML은 분류 정확도를 높이고 데이터를 소급하여 검토할 수도 있습니다. 이러한 식별 프로세스는 전체 데이터 자산에서 클라우드 전반에 걸쳐 콘텐츠가 있는 곳이라면 어디서나 콘텐츠를 보존, 수집, 분석, 검토 및 내보낼 수 있습니다.



[4] "Worldwide IDC Global DataSphere Forecast, 2022–2026: Enterprise Organizations Driving Most of the Data Growth", John Rydning, IDC. 2022년 5월.

2단계

데이터 분류

분류와 정책 모두 데이터가 이동할 때 따라야 합니다.

예를 들어, 한 직원이 Microsoft Word 문서의 신용 카드 번호를 Excel로 복사하는 경우 분류 및 정책이 두 문서 모두에 자동으로 적용되어야 합니다.

적절한 데이터 분류는 다양한 유형의 데이터가 실수 또는 의도적으로 남용되거나 승인 없이 액세스되지 않도록 하는 올바른 정책 및 위험 완화를 결정하는 데 도움이 됩니다. 암호화 및 워터마킹은 미사용 데이터, 전송 중인 데이터 또는 사용 중인 데이터에 대한 보호를 강화할 수 있습니다.

그러나 분류 및 정책은 데이터가 조직 전체를 이동할 때 데이터를 따라야 합니다. 레이블 지정 및 보호 정책은 개별 문서로 국한될 수 없기 때문에 온-프레미스에서 클라우드 리포지토리로, SaaS(software-as-a-service)에서 OS 네이티브 앱으로 전체 디지털 자산에 걸쳐 있어야 합니다.

전통적인 분류에 대한 접근 방식에는 상당한 수동 작업이 포함되기 때문에 오류가 발생하거나 민감한 데이터를 실수로 간과할 위험이 있습니다. 내장형 및 학습 가능한 분류자는 이 프로세스를 자동화하는 데 도움이 될 수 있으며, 통합 솔루션을 통해 관리자는 모든 시스템의 중앙에서 정책을 관리할 수 있습니다.

귀사 환경 전반에서 중요한 데이터를 더 잘 관리하고 보호하고 싶으신가요?

Microsoft.com에서 Microsoft Purview에서의 분류 및 보호에 대해 알아보세요.

3단계

데이터 손실 방지

DLP 정책은 규정 위반 작업을 방지할 수 있습니다.

예를 들어, 한 직원이 신용 카드 번호가 있는 스프레드시트를 플래시 드라이브에 다운로드하거나 클라우드 스토리지에 업로드하려고 하면 DLP 정책에서 활동을 규정 위반으로 식별하고 방지할 수 있습니다.

데이터를 식별하고 분류한 후에는 DLP(데이터 손실 방지) 솔루션이 다크 데이터 및 데이터 유출과 같은 위협을 완화하는 엔드 투 엔드 보호 정책을 적용할 수 있으므로 현재 및 과거 직원이 의도적이거나 실수로 승인 없이 민감한 데이터를 공유, 노출 또는 전송하지 않습니다.

인텔리전트한 DLP 솔루션은 컨텍스트를 유연성 제공 및 고위험 작업의 차단 간의 균형을 찾습니다. 예를 들어, 개인은 잠재적 위험 및 적용 가능한 정책에 대해 상기된 후 작업을 계속할 수 있습니다. 이를 통해 민감한 데이터를 보호하는 동시에 사용자가 위험에 대한 이해도를 높일 수 있도록 교육할 수 있습니다.

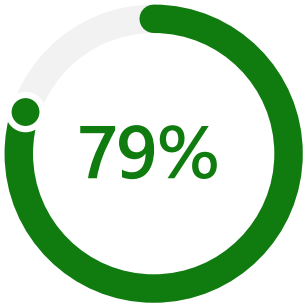
DLP 솔루션을 통해 지적 재산권 및 기타 중요한 비즈니스 데이터를 보호하는 동시에 GDPR(General Data Protection Regulation, 개인정보보호 규정), HIPAA(Health Information Portability and Accountability Act, 건강 정보 양도 및 책임에 대한 법), CCPA(California Consumer Privacy Act, 캘리포니아 소비자 개인정보 보호법)와 같은 규정 준수를 강화할 수 있습니다.

DLP에 대한 포괄적인 접근 방식은 귀사 전체에서 일관적으로 정책을 적용하여 데이터 수명 주기에서 '가장 취약한 링크'를 보호합니다.

민감한 정보를 인텔리전트한 방식으로 감지하고 제어하고 싶으신가요?

Microsoft.com에서 Microsoft Purview에서의 데이터 손실 방지에 대해 알아보세요.

볼트온 접근 방식이 아닌, 빌트인 방식으로 데이터를 보호하세요.



규정 준수 의사 결정자를 대상으로 진행한 한 설문조사에 따르면 79%가 여러 규정 준수 및 데이터 보호 제품을 구매한 것으로 나타났습니다.

대다수는 세 개 이상의 제품을 구입했습니다.[5]

많은 조직에서 정보 보호에 대한 '볼트온' 접근 방식을 시도하여 여러 솔루션을 통해 데이터 수명 주기의 개별 부분을 관리했습니다. 그러나 이로 인해 보안, 데이터 거버넌스, 규정 준수, 법률 팀은 비효율적이고 리소스에 부담을 주는 패치워크를 함께 연결해야 하는 경우가 많습니다.

'빌트인' 접근 방식은 격차를 좁혀 데이터 식별, 데이터 분류, DLP를 통합할 수 있습니다. 통합 솔루션을 사용하면 중앙에서 더 쉽게 정책을 관리하고 적용할 수 있습니다. 또한 기본적으로 애플리케이션 내에서 익숙한 방식으로 정책 알림을 받는 사용자의 교육 시간을 줄입니다.

[5] "미국 규정 준수 의사 결정권자를 대상으로 진행한 2022년 2월 설문조사(n=100 599-999명의 직원, n=100 1000명 이상의 직원), Microsoft에서 의뢰하고 MDC Research에서 진행."

빌트인 방식의 통합 솔루션: Microsoft Purview

Microsoft Purview를 사용하면 전체 데이터 자산을 관리, 보호, 관리하는 데 도움이 되는 포괄적인 솔루션 집합을 통해 오늘날 분산되고 데이터가 풍부한 업무 공간의 과제를 해결할 수 있습니다.

거버넌스를 넘어서세요.

Microsoft Purview를 통해 데이터 보호하는 방법에 대해 자세히 알아보기 >

특정 데이터 보호 영역에 관심이 있으신가요? 다음과 같이 Microsoft Purview에서 지원하는 방법에 대해 자세히 알아보세요.

데이터 검색 >

데이터 분류 및 보호 >

데이터 손실 방지 >

Microsoft Security