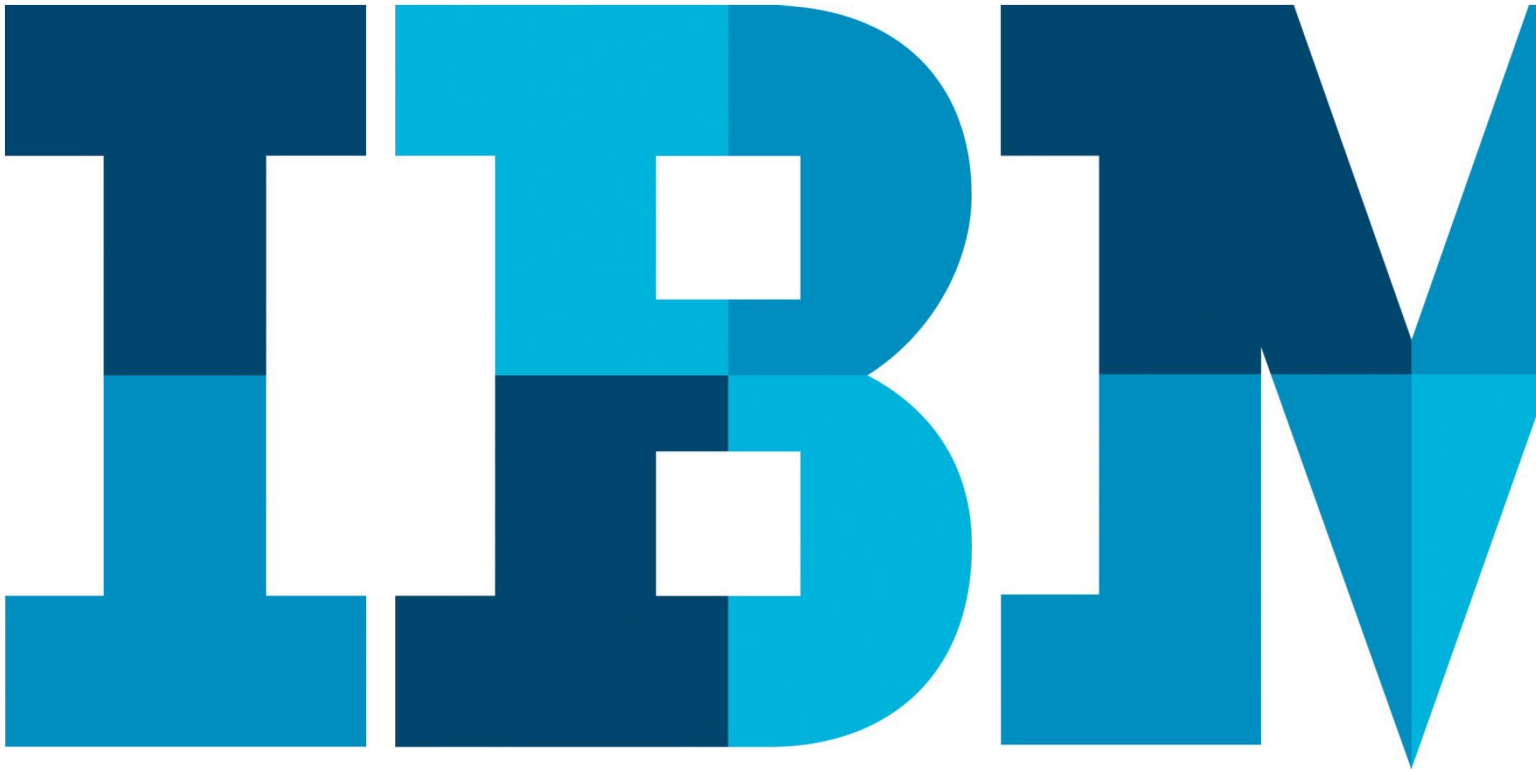
IBM Analytics

클라우드 및 사내 데이터 보안

적절한 거버넌스를 통해 하이브리드 환경의 정보 보호



IBM

들어가기 »

목차

개요: 새로운 표준에서 거버넌스의 중요성

클라우드 기반의 데이터는 업계에서 경쟁 우위를 확립하고 유지하고자 하는 기업에 풍부한 잠재적 정보를 제공합니다. 하지만 "The truth about information governance and the cloud"(정보 거버넌스 및 클라우드에 대한 진실)에서 설명한 대로, 대부분의 기업은 기존의 사내 데이터를 하둡 및 기타 오픈 소스 기술과 함께 타사의 새로운 클라우드 기반 데이터에 맞게 조정해야 하는 어려운 과제에 직면하고 있습니다. 이러한 "하이브리드" 환경에서 기업은 중요한 의사결정을 내릴 수 있는 통찰을 찾으려고 합니다.

일반적으로 하이브리드 환경이 충분한 사전 계획 없이 확장되기 때문에 계속 증가하는 데이터 저장소를 관리하는 것은 매우 어렵습니다. 하지만 해결할 수 있는 방법이 있습니다. 항상 그렇듯이 첫 번째 단계는 문제의 본질을 이해하는 것입니다. 데이터 자체에 가장 중요한 초점을 두고, 데이터의 소스나 데이터 관리에 사용되는 시스템에는 덜 집중해야 합니다. 데이터 및 데이터에서 파생된 정보의 소유권에 가장 높은 우선 순위를 두면 나머지 우선 순위는 쉽게 결정됩니다.

네 가지 핵심

기업에서 클라우드의 재무 이점을 실현하는 동시에, 클라우드 소스에서 선별한 정보가 안전하고 신뢰할 수 있는 정보인지 확인하는 방법은 무엇일까요? 그 해답은 바로 '거버넌스'입니다.

이상적인 하이브리드 정보 거버넌스는 IT 및 비즈니스의 네 가지 주요 우선순위를 기반으로 합니다.

1. **정보의 개념에 대한 광범위한 합의**
   여기에는 비즈니스에 필요한 정보와 그러한 정보의 처리 방식에 대한 일반적인 정책 및 일반 언어 규칙의 메타데이터가 포함됩니다.
2. **소유한 정보 자산을 유지관리 및 모니터링하는 방식에 대한 명확한 합의**
   예를 들면 사내 시스템의 마스터 데이터 관리에 대한 운영 데이터 품질 규칙이 있습니다.
3. **전략적 정보 자산의 보안 및 보호를 위한 전사적/부서별 표준 방침**
   예를 들면 정보에 대한 역할 기반 액세스의 명시, 정보 공유 방법을 규정하는 규칙의 작성, 중요한 정보를 제3자로부터 보호 등이 있습니다.
4. **엔터프라이즈 데이터 통합 전략**
   여기에는 데이터를 이동하고 전략적 정보로 취합하는 방법을 계획하고, 이러한 정보를 시간의 경과에 따라 유지 관리하는 방법을 파악하는 라이프사이클 관리가 포함됩니다.

이러한 요소들이 하이브리드 환경의 정보 거버넌스를 위한 기반을 형성합니다. 개별 사례에서는 프로세스와 조직적/기술적 지원 요소들이 조화를 이루어야 성공을 거둘 수 있습니다. 이러한 핵심 요소가 제 기능을 다할 때 기업은 유연하면서도 확신을 가지고 신속하게 움직일 수 있습니다.

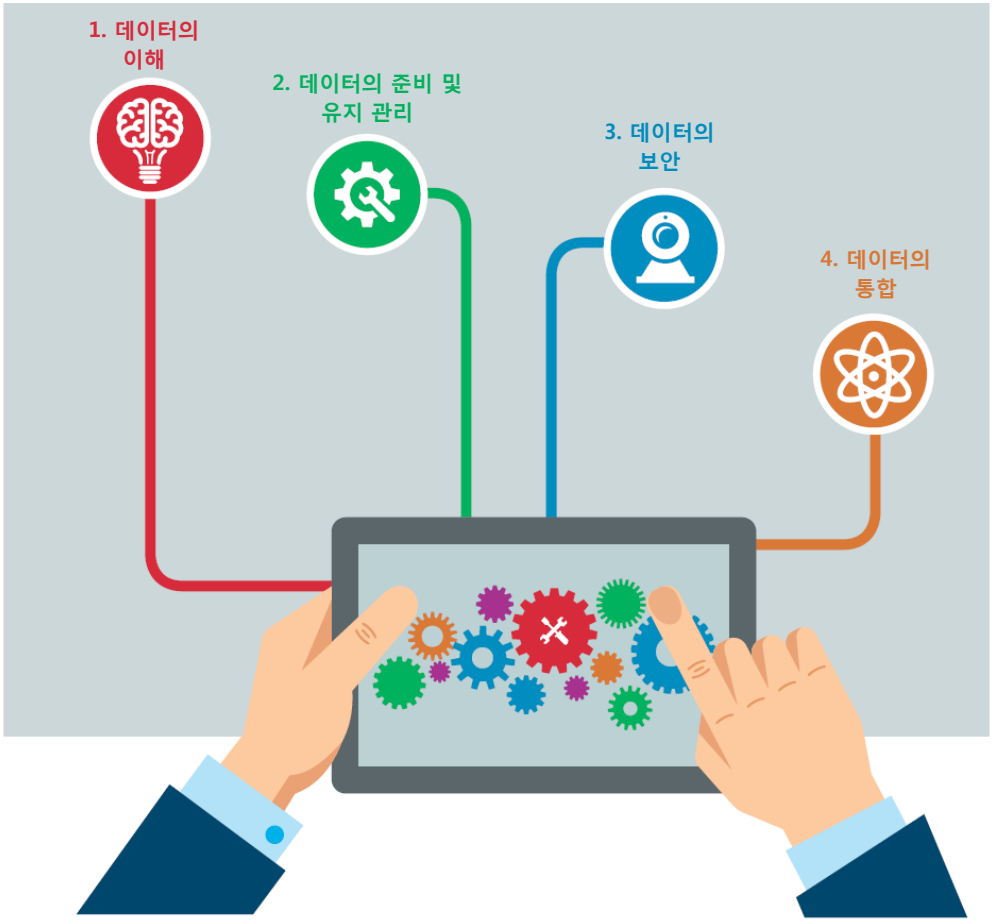
이 전자책은 세 번째 핵심: 하이브리드 환경의 데이터 보호에 중점을 둡니다.

전략적 정보의 소유권 획득

하이브리드 환경을 채택하기 위해 IT 전략을 완전히 바꿀 필요는 없습니다. 사실 환경에서 클라우드에 기반한 부분은 비즈니스 우선 순위에 대응하여 신속하게 진화합니다. 하지만 클라우드 기반 소스에서 유래하는 데이터의 비율이 아주 작더라도, IT는 데이터 통합 및 보안에 대한 계획이 필요합니다. 또한 모든 데이터 및 처리로 생성된 정보를 그 위치에 관계없이 기업이 "소유"할 수 있도록 지원해야 합니다.

하이브리드 인프라와 탈중심화된 컴퓨팅은 전략적 정보 자산 생성이라는 최종 목적을 위한 수단일 뿐입니다. 이러한 근본 개념을 인식하면 IT가 처리해야 할 문제, 더 중요하게는 IT가 비즈니스 사용자와 보다 효과적으로 협력할 수 있는 방법을 명확하게 파악할 수 있습니다.

이상적인 하이브리드 정보 거버넌스를 위한 최우선 사항의 세부 내용을 보려면 아래의 각 아이콘에 마우스를 올려 놓으십시오.



하이브리드 환경의 데이터 보호: 향후 과제

데이터 볼륨이 급증하고 기술이 급속하게 변화하는 오늘날에는 어떤 환경이든 데이터를 통제하기가 어렵습니다. 특히, 클라우드 환경의 데이터가 과거의 보안 전략에서 핵심 역할을 한 방화벽과 같은 기존 보호 방식의 범위를 벗어나 생성되거나 이동되는 경우, 이러한 문제가 더욱 가중됩니다.

IDC 조사에 따르면, 73%의 기업이 클라우드 서비스 또는 애플리케이션이 회사 IT 또는 보안 정책을 벗어나서 사용되는 경우를 한 건 이상 발견했다고 응답했습니다.[1] 대부분의 경우 이러한 새로운 클라우드 배치가 기존 IT 인프라에 도입되어 하이브리드 환경을 조성합니다(그림 1).

기업 전반의 데이터 보안 및 개인정보 보호 문제

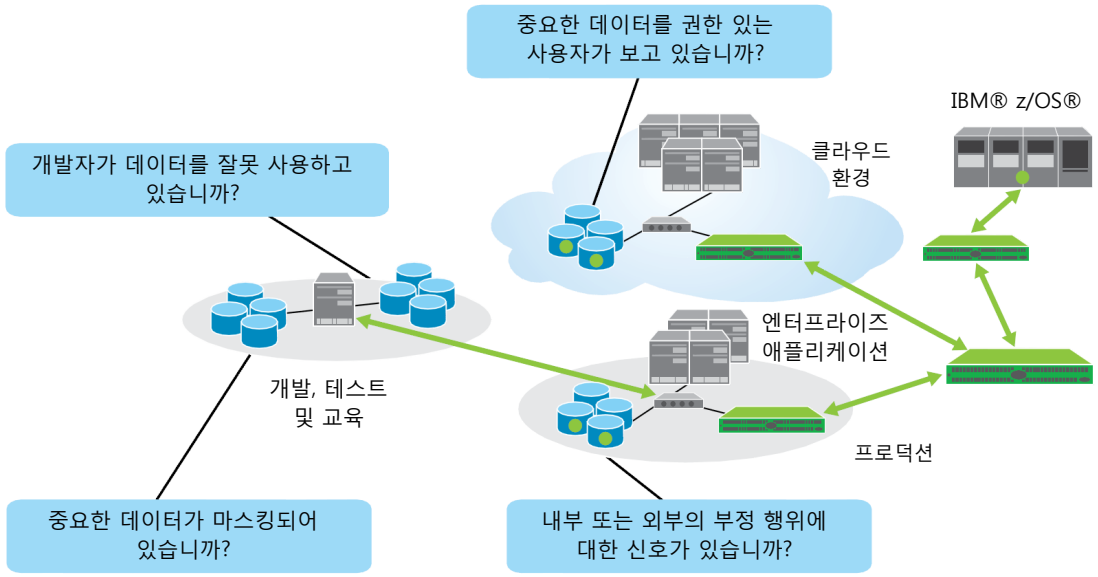


그림 1. 기업은 데이터의 상주 위치(테스트, 프로덕션, 사내 및 클라우드)에 관계없이 데이터를 보호해야 합니다.

그렇다면, 보안 및 거버넌스 전문가가 심각하게 우려하는 이유는 무엇이며, 어떤 위험이 있을까요? 사내 및 클라우드의 보안 해결을 시급하게 만드는 여러 요인은 무엇일까요?

간과할 수 없는 클라우드 보안 문제

70%의 응답자가 클라우드 컴퓨팅 배치에 보안 문제가 있다고 응답

클라우드 컴퓨팅의 상위 5가지 보안 문제
데이터 보안: 41%
액세스 및 통제: 35%
감사 및 규정 준수: 32%
데이터 관리: 26%
보안 모델/도구 세트: 18%

출처: IOG Enterprise, 2013; 451 Research, "Cloud Computing - Wave 6," 2014.

규정 준수

데이터가 상주하는 위치에 관계없이, 중요한 데이터 유형을 식별하고 사내 및 클라우드에서 이러한 데이터의 사용을 위한 일관성 있는 정책을 수립하는 것이 중요합니다. **데이터가 어디에 있는지, 어떤 영역의 정보가 존재하는지, 그리고 데이터가 전사적으로 어떻게 연관되어 있는지 파악해야 합니다.**

이러한 지식은 해당 데이터의 보안 및 보호와 SOX(Sarbanes-Oxley Act), PCI DSS(Payment Card Industry Data Security Standard), FISMA(Federal Information Security Management Act), HITECH(Health Information Technology for Economic and Clinical Health) 같은 규정의 준수를 명시하기 위한 적절한 정책을 정의하는 데 도움이 됩니다. 준수해야 하는 규정의 수와 종류가 계속 증가하고 있지만, 기업은 데이터가 클라우드로 이동해도 규정 준수 능력을 유지해야 합니다.

데이터 침해

중요한 데이터에 대한 위협은 어디에나 존재합니다. 악의적인 해커들은 중요한 데이터에 손쉽게 액세스하는 방법을 끊임없이 찾습니다. 불만을 품은 직원이 거래 기밀이나 고객 데이터를 의도적으로 공개할 수도 있습니다. 정책이 준수되지 않거나 권한이 올바르게 설정되지 않은 경우 실수로 데이터가 노출될 수 있습니다. 그리고 방화벽과 IPS 장치 같은 기존의 경계 방어는 더 이상 충분한 억제 수단이 되지 못합니다.

실제, 가상 및 클라우드 환경에서 내부와 외부의 공격으로부터 데이터를 보호해야 합니다. 최선의 방법은 오류를 방지하고 액세스 권한의 남용을 방지하기 위해 사용자에게 "가능한 최소한의 권한"을 부여하는 것입니다. **클라우드 내부에서 발생하는 상황과 권한 있는 사용자의 행동을 파악하도록 도와주는 데이터 보안 솔루션을 이용하여 다각적인 방어책을 마련하십시오.**

개인정보 보호

또 다른 과제는 중요한 정보에 대한 액세스에 정당한 업무적 사유가 있는지 확인하는 것입니다. 예를 들어 의사는 증상과 예후에 대한 중요한 정보를 필요로 하지만, 청구 담당자는 환자의 보험 번호와 청구 주소를 필요로 합니다. 비즈니스 요구사항을 충족하고 데이터가 "필요한 경우에만 제공되는(need-to-know)" 방식으로 관리되는지 확인하는 동시에 적절한 보호를 제공하기는 매우 어렵습니다. **중요한 정보가 구조화된 데이터베이스와 비구조화된 파일 시스템에 모두 존재하며, 따라서 모든 인스턴스의 액세스를 모니터링해야 한다는 점을 명심하십시오.**

생산성

보안과 개인정보 보호는 비즈니스 운영을 방해하는 것이 아니라 향상시켜야 합니다. **관련 정책은 사용자 생산성에 부정적인 영향을 미치지 않도록 클라우드 환경에서 일상적인 운영 및 업무에 완벽하게 적용되어야 합니다.** 예를 들면 애플리케이션 테스팅을 위해 많은 사설 클라우드가 사용되고 있습니다. 중요한 데이터를 마스킹하면 테스트 결과에 영향을 미치지 않고 이러한 환경에서 노출된 데이터의 보안 위험을 완화할 수 있습니다.

취약성

데이터베이스 취약성은 무수히 많으며, 해커들은 아주 작은 가능성이라도 이용하려고 합니다. 모든 각도에서 취약성을 파악하고 이를 해결하는 방법을 개발해야 합니다. **일반적인 데이터베이스 취약성으로는 오래된 패치, 잘못된 구성 및 기본 시스템 설정이 있습니다.** 데이터베이스 서버가 가상화되면 이러한 취약성의 복잡성이 증가합니다.

오늘날 기업들은 엔터프라이즈 데이터를 보호하고 규정 준수를 보장하기 위해 다양한 보안 기술을 마련하고 있습니다. 기업이 클라우드를 도입하면 데이터 보안의 확장성이 문제가 됩니다. 가장 일반적인 데이터 보안 솔루션 중 하나인 암호화는 이러한 확장성 문제로 인해 어려움을 겪을 수 있습니다. 일부 암호화 방식은 특정 하드웨어 또는 네트워크 리소스에만 적용되며 클라우드 환경에서는 네트워크 또는 인프라에 대한 종속성이 허용되지 않습니다.

또는 애플리케이션 테스팅 또는 개발을 위해 클라우드를 사용하고, 여기에서 새로운 데이터베이스가 정기적으로 생성되고 폐기될 수 있습니다. 데이터베이스가 동적으로 생성되므로 그 안의 데이터를 보호해야 합니다. 클라우드 환경을 위한 확장 가능한 데이터 보안 접근법을 이용하면, 새로 생성된 데이터베이스가 자동으로 발견되고 그 안에 포함된 데이터가 자동으로 분류, 보호 및 모니터링됩니다.

마지막으로, 데이터 마스킹 루틴과 데이터베이스 활동 모니터링 스크립트처럼 데이터 보안을 위해 내부에서 개발한 도구를 사용하는 경우를 생각해 보겠습니다. 이러한 도구가 가상 데이터베이스에서 작동하게 하려면 코딩을 변경해야 합니까? 내부에서 개발한 솔루션을 업데이트하려면 상당한 투자를 해야 할 것입니다. 이상적으로는, 보안 프로세스 및 절차가 수동 개입 없이 수행되어야 하며 따라서 새로운 데이터베이스가 추가되어도 기존 도구를 수정할 필요가 없어야 합니다.

요약하면, 데이터 보안을 하이브리드 환경의 구조에 직접 구현해야 합니다. 어떻게 하면 이 작업을 체계적이고 종합적으로 수행할 수 있을까요?

데이터 보안에 대한 전체론적 접근법

전체론적 데이터 보안 전략은 조직 전체의 데이터에 대하여 데이터의 위치에 관계없이 데이터 활용의 모든 단계에서 완벽한 보호를 구현합니다. 이러한 전략에는 하이브리드 환경에서 보안 제어를 중앙 집중화하고, 데이터 관리자가 보안 관리자 또는 감사자가 되지 않도록 책임을 분리하는 조치가 포함되어야 합니다.

하이브리드 환경의 견고한 데이터 보안 전략에 포함되는 몇 가지 핵심 요소는 다음과 같습니다.

중요한 데이터의 위치 파악.
초기에 대부분의 기업은 모든 중요한 정보가 어디에서 사용되는지 알 수 있다고 생각했습니다. 하지만 인프라 복잡성이 증가한 결과 이제는 새로운 데이터베이스, 웨어하우스 또는 애플리케이션 중 어느 곳에 아주 중요한 데이터가 실수로 로드되었는지 알기가 어려워졌습니다. 식별되지 않은 중요한 데이터가 이름이 잘못 지정된 데이터베이스 테이블 또는 샌드박스 환경에 숨어 있는 경우가 많으며, 이로 인해 엄청난 위험이 발생합니다. IaaS(Infrastructure-as-a-service) 클라우드 데이터베이스 내에서도 중요한 데이터를 발견하고 분류하는 데 도움을 주는 검색 유형 도구를 사용해 보십시오.

중요한 데이터의 보호. 데이터가 구조화되어 있든 비구조화되어 있든, 온라인이든 오프라인이든, 중요한 데이터를 보호하는 단 하나의 최선의 방법은 없습니다. 비즈니스 요구사항과 보안 요소를 바탕으로 여러 가지 옵션을 고려해야 합니다. 적절한 솔루션을 선택하려면 먼저 다음과 같은 질문에 답해 보십시오.

- 어떤 종류의(비구조화 또는 구조화) 데이터를 보호해야 합니까? 두 가지 데이터의 요구사항을 모두 충족하는 솔루션이 있습니까?
- 중요한 데이터가 클라우드 내에 있어야 합니까? 그렇다면 사내 및 클라우드 환경에 모두 상주합니까? 그러한 환경에서 데이터를 공유해야 합니까?
- 데이터를 클라우드로 전송하기 전에 데이터의 민감성을 제거할 수 있습니까? 경우에 따라 실제 같아 보이지만 허구인 결과를 제공하기 위해 데이터를 마스킹할 수 있습니다.
- 준수해야 하는 암호화 기준이 있습니까? 특정한 암호화 기준을 요구하는 규정이 많습니다.
- 솔루션을 현재의 요구사항에서 하이브리드 또는 빅 데이터 환경의 미래 요구사항에 맞게 확장할 수 있습니까? 하드웨어 암호화 또는 내부 개발 솔루션이 이와 관련된 문제에 직면할 수 있습니다.

데이터 액세스의 안전하고 지속적인 모니터링.
마스킹과 암호화 같은 비식별화(de-identification) 기술은 데이터를 보호하는 검증된 방식이지만, 승인된 또는 권한 있는 사용자와 관련된 제한이 있습니다. 예를 들어 암호화가 보안의 유일한 원천인 경우, 권한 있는 사용자는 특별한 문제 없이 이미 중요한 정보에 대한 액세스(키)를 가지고 있습니다. 이러한 위험을 완화하려면 권한 있는 사용자를 포함하여 의심스러운 동작을 실시간으로 식별하고 중단시키기 위한 데이터 자산 자체에 대한 실시간 모니터링이 필요합니다. 이러한 방식을 사용하면 권한 있는 사용자가 중요한 데이터에 원활하게 액세스할 수 있는 동시에, 비정상적인 사용이 발생하면 보안 정책을 적용할 수 있습니다.

감사를 통과하기 위한 규정 준수의 증명.
규정 준수 의무를 충족하는 일은 어렵고 시간이 많이 소요됩니다. 감사 실패나 벌금 부과를 방지하려면 적용 가능한 규정의 가장 엄격한 요건을 충족하는 전체론적인 솔루션을 모색해야 합니다. 이러한 솔루션은 비즈니스 및 변화하는 규정의 성장에 대응하여 확장할 수 있어야 합니다. 또한 규정 준수 프로세스의 간소화를 위해 감사 보고 기능과 사인오프 기능을 사용하십시오.

이와 함께 관리자에게 비정상적인 네트워크 활동과 같이 의심스러운 동작을 경고하는 방법이 필요합니다. 게다가 클라우드 또는 하이브리드 환경의 데이터 보안 프로세스는 클라우드의 데이터를 지속적으로 추적하고 애플리케이션, 데이터베이스, 웨어하우스 및 파일 공유 전반에서 데이터를 액세스하는 사람이 누구인지에 대한 통찰을 제공해야 합니다.

데이터 보안을 위한 IBM 솔루션

데이터 보안 솔루션을 선택할 때는 확장이 가능하고 IT 인프라 전반에 통합되어 실제, 가상 및 클라우드 환경을 악의적인 외부 공격, 사기, 무단 액세스 및 내부 보안 위반으로부터 보호할 수 있는 솔루션을 선택하십시오. 이러한 솔루션은 특별한 설치, 구성 또는 추가 비용 없이 하이브리드 환경에서 작동해야 합니다.

이러한 접근 방식은 데이터 보안 및 개인정보 보호를 위한 효율적인 플랫폼을 제공하고, 고도로 전문화된 데이터 보안 리소스의 필요성을 줄여 비용 관리를 도와주고, 보안 및 개인정보 보호를 위한 셀프 서비스 옵션으로 민첩성과 유연성을 확장할 수 있게 해줍니다.

IBM Security와 **IBM Information Integration and Governance** 솔루션은 다음과 같은 기능을 통해 클라우드 보안 전략을 지원합니다.

- 가상화된 데이터베이스 활동 모니터링, 데이터베이스 취약성 평가, 데이터 교정(redaction) 및 데이터 암호화
- 클라우드 내의 데이터의 자동 검색 및 분류
- 클라우드 리소스에 대하여 최소 권한의 액세스 모델을 보장하는 정적 및 동적 데이터 마스킹
- 클라우드의 규정 준수를 증명하기 위해 여러 규정에 맞게 사용자 정의된 감사 및 규정 준수 보고서
- 실제, 가상, 클라우드 환경을 포함한 서로 다른 환경 간에 중앙화 및 자동화된 보안 제어

다음 단계: 클라우드 거버넌스 논의의 지속

클라우드 기반의 데이터 및 처리 서비스는 비즈니스 사용자가 간과할 수 없는 다양한 기회를 제공하고, IT는 내부 및 사내 트랜잭션 및 보고 시스템의 무결성을 유지 관리하는 일을 담당합니다. 하이브리드 환경을 위한 거버넌스 전략의 계획은 나중에 고려할 일이 아니라 지금 바로 착수해야 할 일입니다.

이 전자책은 성공적인 하이브리드 환경 거버넌스를 위한 네 가지 핵심 중 하나인 '하이브리드 환경의 데이터 보안'을 설명합니다. **다른 핵심을 살펴보려면 이 시리즈의 다른 전자책을 다운로드하여 참조하십시오.**

- The truth about information governance and the cloud(정보 거버넌스 및 클라우드에 대한 진실)
- Make sense of your data(데이터의 이해)
- Developing a data integration and lifecycle management strategy for a hybrid environment (하이브리드 환경을 위한 데이터 통합 및 라이프사이클 관리 전략 개발)
- Prepare and maintain your data(데이터의 준비 및 유지 관리)

IBM 거버넌스 사고 리더십과 지원 기술에 대한 자세한 정보는 다음 사이트를 방문하십시오.

- **ibm.com**/software/data/information-integration-governance
- **ibm.com**/analytics/us/en/technology/agile/

또한 IBM 글로벌 파이낸싱은 기업이 비즈니스의 성장에 필요한 기술을 획득하도록 지원하기 위해 다양한 상환 옵션을 제공합니다. IBM은 IT 제품 및 서비스의 획득에서 처분에 이르기까지 라이프사이클 전반의 관리를 제공합니다. 자세한 정보는 다음 사이트를 방문하십시오.
ibm.com/financing/kr

한국아이비엠주식회사

(07326) 서울시 영등포구 국제금융로 10
서울국제금융센터 3 빌딩 (Three IFC)

Produced in the United States of America
Printed in Republic of Korea

September 2016