Microsoft Security

데이터 보안 인덱스

데이터를 안전하게 유지하고 생성형 AI를
탐색하기 위한 트렌드, 인사이트, 전략

2024 보고서

머리말

진화하는 데이터 보안 환경에 대해 2년째 연구를 시작하면서 우리 앞에 놓인 과제와 기회는 그 어느 때보다 심오합니다. 지난 한 해 동안 데이터 보안 인시던트의 심각성이 높아졌습니다. 지금과 같은 데이터 중심 시대에 데이터를 보호하는 데 사용되는 전략과 도구는 빠른 속도로 발전하고 있습니다.

올해에는 생성형 AI(AI)가 데이터 보안 전략에 미치는 역할과 영향과 같은 새로운 내용에 대해 살펴볼 예정입니다.

AI는 더 많은 혁신과 효율성을 실현할 수 있는 전례 없는 기능으로 전 세계에 파장을 일으키고 있습니다. 그러나 이와 같은 엄청난 잠재력으로 인해 조직은 데이터 보안 위험과 이로 인해 데이터 보안 팀의 책임이 어떻게 형성될 수 있는지에 대해서도 우려하고 있습니다. Microsoft에서는 AI가 조직이 데이터 과잉 공유 및 데이터 유출의 영향을 최소화하고 안전한 AI 채택을 위한 프로세스를 만들 수 있도록 기본 데이터 보안 관행을 강화하는 촉진제라고 생각합니다. 반면, AI는 숨겨진 위험과 보호 격차를 식별하고, 보호 정책을 권장하며, 보안 인시던트를 더 빠르게 조사하고 수정하는 데 도움을 줌으로써 조직이 데이터 보안 관행을 개선하는 데 도움이 될 수도 있습니다.

이 연구 보고서의 목표는 데이터 보안 리더에게 실행 가능한 인사이트와 지침을 제공하여 팀이 데이터 보안 전략을 자신 있게 조정하여 AI 사용을 효과적으로 보호하고 데이터 보안 전략에 AI를 통합할 수 있도록 돕는 것입니다. AI는 영향력과 잠재력 면에서 주목할 만하지만, 하이브리드 업무, 클라우드, 모빌리티와 같이 기업 전반을 휩쓸고 있는 최신 혁신의 물결에 불과하며, 최근 몇 년 동안 위험을 완화하고 영향을 극대화하기 위해 AI를 사용하는 데 있어 시대를 초월한 가시성의 필요성이 강조되었습니다. 이러한 학습 내용을 바탕으로 AI에 사용되는 데이터를 적절하게 보호하고 AI를 사용하여 데이터 보안 조치를 강화하면 팀이 미래의 과제를 탐색할 때 생산성, 회복탄력성, 민첩성을 높일 수 있습니다.

Microsoft와 함께 최신 연구 결과를 살펴봄으로써 이러한 인사이트가 데이터 보안 태세를 강화하는 데 도움이 될 뿐만 아니라 AI를 수용하고 포괄적인 데이터 보안 전략을 구축하여 더 많은 혁신을 실현하고 우리 모두를 위한 더 안전한 미래를 보장하는 데 도움이 되기를 바랍니다.

Rudra Mitra
기업 부사장
Microsoft 데이터 보안 및 준수

서문

조직은 매년 평균 156건의 데이터 보안 인시던트를 경험하고 있으며, 이러한 인시던트의 영향은 데이터 보안 의사 결정권자에게 지속적인 관심사로 남아 있습니다. 단일 인시던트는 막대한 재정적 및 평판 손상을 초래할 수 있는데, 특히 공격자가 가능한 모든 취약점을 악용하는 끊임없이 진화하는 위협 환경에서 큰 손상을 초래할 수 있기 때문입니다. 이는 AI의 급속한 채택으로 인해 과장된 것으로, 적절한 보호 및 보안 조치가 없으면 사용자가 실수로 또는 악의적으로 민감한 비즈니스 크리티컬 데이터(직원 및 고객 정보, 지적 재산, 재무 예측 및 운영 데이터 포함)를 위험에 빠뜨릴 수 있습니다. 조직이 이처럼 광범위한 민감한 데이터를 보호할 수 있는 새로운 방법을 모색함에 따라 많은 의사 결정권자가 AI의 급격한 부상에 관심을 기울이고 있습니다.

AI의 과제는 두 가지입니다. 조직 중 2/3가 직원이 승인되지 않은 AI 도구를 사용하고 있다고 인정한다는 점을 감안할 때 직원이 AI 도구를 안전하게 사용하도록 하는 것이 중요합니다. 이와 동시에, AI를 정교한 데이터 보안 전략의 효과적인 도구로 활용할 수 있는 기회도 있습니다.

AI 기반 데이터 보안 솔루션은 이미 실시간으로 위협을 식별 및 대응하고, 데이터 보안 프로그램의 전반적인 속도와 정확성을 개선하며, 데이터 보안 인시던트가 발생하기 전에 예방하는 데 도움이 되는 인사이트를 제공하는 데 중요한 역할을 하고 있습니다. 조직은 AI의 기능을 활용하여 인간이 기계 속도로 처리하고 분석하기 어려울 수 있는 패턴을 식별하고 궁극적으로 점점 더 정교해지는 사이버 공격에 맞서 싸울 수 있도록 AI로 인한 위험을 관리해야 합니다.

2023년, Microsoft는 독립 연구 기관인 Hypothesis에 의뢰하여 800명 이상의 데이터 보안 전문가를 대상으로 다국적 설문 조사를 실시하고 파트너와 고객에게 더 나은 서비스를 제공하고 비즈니스 리더가 자체 데이터 보안 전략을 개발할 수 있도록 지원하기 위해 데이터 보안 인덱스 이니셔티브에 착수했습니다.

2024년, 이 보고서는 1,300명 이상의 데이터 보안 전문가를 대상으로 한 확장된 다국적 설문 조사를 통해 확보한 새로운 인사이트를 활용하여 이전 연구를 기반으로 합니다. 이 데이터는 우리가 조사한 시장 전반에 걸쳐 일관된 인사이트와 트렌드를 보여주지만, 전 세계의 최신 데이터 보안 및 AI 관행과 트렌드에 대한 새로운 교훈을 발견했습니다.

hypothesis Microsoft Security

주요 조사 결과

1

데이터 보안 환경은 여전히 분열되어 있으며 AI 사용과 관련된 기존 위험과 새로운 위험 모두에 걸쳐 응집력 있는 데이터 보안 전략의 필요성이 증가하고 있습니다

조직은 데이터 보안 조치에 대해 높은 수준의 만족도와 확신을 보고합니다. 그러나 데이터 보안 인시던트의 심각성은 특히 조직이 현재 데이터 보안 정책과 AI 애플리케이션의 사용/도입 증가 사이에서 발견하는 격차로 인해 계속 증가하고 있습니다. 이러한 위험과 과제에 직면한 많은 조직은 여전히 전반적인 취약성과 위험을 증가시킬 수 있는 여러 데이터 보안 도구에 의존하고 있습니다.

2

최종 사용자가 AI 앱을 점점 더 많이 채택함에 따라 조직의 가장 민감한 데이터의 무결성이 더 큰 위험에 처해 있어 더 많은 가시성과 새로운 보호 제어가 필요합니다

AI 도구가 일상 업무에 필수가 됨에 따라 조직은 데이터 보안 위험에 대해 우려하고 있습니다. 이들은 방어를 강화해야 할 필요성을 인식하고 AI로 인한 데이터 보안 인시던트를 방지하기 위해 최선을 다하고 있지만, 이러한 도구의 무단 사용은 보다 강력한 가시성의 필요성을 강조합니다.

3

의사 결정권자들은 데이터 보안 노력을 강화할 수 있는 AI의 잠재력에 대해 낙관적으로 생각합니다

조직은 탐지 및 대응 기능을 개선하기 위해 AI를 통합하는 데이터 보안 도구에 적극적으로 투자하고 있습니다. AI는 보호되지 않는 데이터를 탐지하고, 보호 정책을 권장하며, 데이터 보안 인시던트를 더 빠르게 조사하고 해결하는 데 도움이 될 수 있으며, 궁극적으로 데이터 보안 팀이 전략적 작업에 더 많은 시간과 주의를 집중할 수 있도록 합니다. 또한 AI를 사용하면 조직의 전반적인 데이터 보안 전략, 특히 인시던트에 빠르고 정확하게 대응할 수 있는 능력에 대한 확신과 만족도가 높아집니다.

1

데이터 보안 환경은 여전히 분열되어 있으며 AI 사용과 관련된 기존 위험과 새로운 위험 모두에 걸쳐 응집력 있는 데이터 보안 전략의 필요성이 증가하고 있습니다

데이터 보안 관행에 대한 의사 결정권자의 확신과 데이터의 진정한 보호 수준은 단절되어 있습니다

2023년에 보고된 바와 같이 대다수의 의사 결정권자는 데이터 보안 전략에 확신을 가지고 있으며 74%는 2024년 현재 솔루션에 만족한다고 보고했습니다. 이들은 민감한 데이터를 추적하고 관리할 수 있는 능력에 대해 안전하다고 느낍니다. 88%는 대부분의 중요한 정보가 어디에 있는지 알고 있다고 생각하며, 85%는 데이터가 적절하게 분류되고 레이블이 지정되었다고 말합니다. 또한 응답자 중 79%는 데이터 유출을 방지할 수 있다고 확신하며, 76%는 자사의 접근 방식이 사후 대응이 아닌 사전 예방적이라고 설명하여 대다수가 방어 제어 기능을 신뢰합니다.

그러나 인시던트의 심각성이 계속 증가함에 따라 이들의 자신감은 흔들리고 있습니다. **연평균 데이터 보안 인시던트 횟수는 2023년 166건, 2024년 156건 등 높은 수준을 유지하고 있으며, 이러한 인시던트의 심각도는 심각도 높은 인시던트 비율이 20%에서 2024년 27%로 증가했습니다.**

156

데이터 보안 인시던트 횟수

27%

심각하다고 간주되는 인시던트 발생 비율(2023년 20%에서 증가)

63%

하루에 검토된 경고 비율

"소프트웨어 플랫폼이 구축된 위치, 데이터가 저장되는 위치, 해당 데이터에 액세스할 담당자는 AI 도구 및 공급업체의 데이터 보안 및 관리를 복잡하게 만들었습니다. 우리는 100년 이상의 데이터를 보유하고 있기 때문에 사업을 운영하는 모든 관할권의 법적 요구 사항에 따라 보호하고 관리해야 합니다."라고 한 중장비 제조업체의 정보 거버넌스 담당 선임 관리자는 말합니다.

데이터 보안 인시던트의 심각성이 증가함에 따라 결과적으로 경고의 양이 증가했습니다. **조직은 하루 평균 66개의 경고를 받고 있는데, 이는 2023년의 52개에서 증가한 수치입니다.** 이 수치는 조직 규모에 따라 크게 다르며, 중견 기업(500~999명의 직원) 및 대기업 (1,000~4,999명의 직원)은 평균 56개의 경고를 받고 초대형 기업(5,000명 이상의 직원)은 하루 평균 80개의 경고를 받습니다.

엄청난 양의 데이터 보안 경고를 감안할 때 대부분의 조직이 이를 따라잡을 수 없다는 사실은 크게 놀랍지 않습니다. 평균적으로 데이터 보안 팀은 일일 경고 중 63%를 검토합니다. 이러한 경고 중 35%는 거짓 긍정으로 판명되었습니다. 이러한 통제 인식과 운영 현실이 불일치함에 따라 데이터 보안 팀은 적절한 보호 기능이 마련되어 있는지 또는 이를 미세 조정하는 방법을 평가해야 하는 동시에 잠재적으로 심각한 인시던트가 누락될 수 있다는 우려에 압도됩니다.

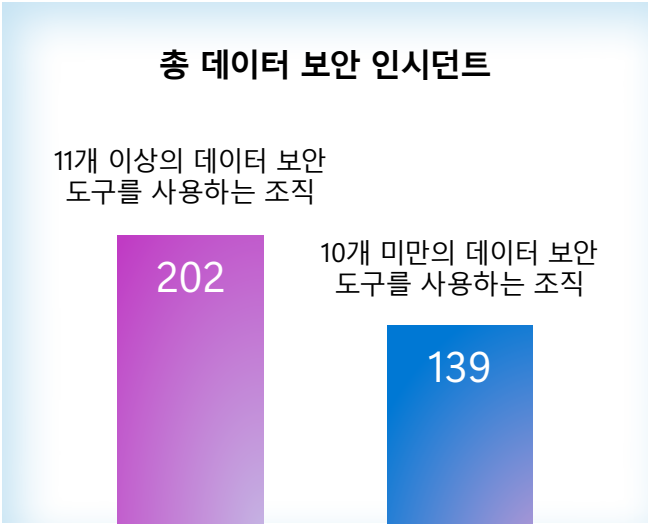
AI 도구 사용과 관련된 기존 및 새로운 데이터 위험에 대처하기 위해 보다 강력하고 응집력 있는 데이터 보안 전략에 대한 필요성이 증가하고 있습니다

사용할 수 있는 도구의 수가 증가하고 있음에도 불구하고 많은 의사 결정권자는 더 많은 것이 항상 더 좋은 것은 아니라는 사실을 계속 인정하고 있습니다. 실제로, 21%는 이질적인 도구로 인해 발생하는 통합되고 포괄적인 가시성(및 위험에 대한 이해 공유)의 부족을 가장 큰 과제/위험으로 꼽았습니다.[1]

대부분의 의사 결정권자(82%)는 완전히 통합된 포괄적 플랫폼이 여러 개의 고립된 도구를 관리하는 것보다 우수하다는 데 동의합니다. **평균적으로 12개의 다양한 데이터 보안 솔루션 사이에서 고군분투하고 있는데, 이로 인해 복잡성이 발생하여 취약성이 증가하고 있습니다.** 이는 특히 규모가 가장 큰 조직에 해당됩니다. 평균적으로 중견 기업은 9개, 대기업은 11개, 초대형 기업은 14개의 도구를 사용합니다.

이 데이터는 사용된 데이터 보안 도구의 수와 데이터 보안 인시던트의 빈도 사이에 강력한 상관 관계가 있음을 보여줍니다. 중견 기업 및 대기업은 연간 평균 89건의 인시던트를 보고하는 반면, 초대형 기업은 연간 248건의 인시던트를 경험합니다. 이처럼 뚜렷한 차이는 대규모 조직이 데이터 보안 조치에 대해 상당한 확신을 표명하더라도 겪게 되는 높은 위험성을 강조합니다.

2024년에 더 많은 데이터 보안 도구(11개 이상)를 사용하는 조직은 평균 202건의 데이터 보안 인시던트를 경험한 반면, 10개 이하의 도구를 사용하는 조직은 139건의 인시던트를 경험했습니다.



단편화된 솔루션은 데이터가 고립되어 있고 이질적인 워크플로로 인해 잠재적 위험에 대한 포괄적인 가시성을 제한할 수 있어 데이터 보안 태세를 이해하기 어렵습니다. 도구가 통합되지 않으면 데이터 보안 팀은 데이터의 상관 관계를 파악하고 위험에 대한 응집력 있는 관점을 설정하는 프로세스를 구축해야 합니다. 이로 인해 사각지대가 발생하고 위험을 효과적으로 탐지하고 완화하는 것이 어려워질 수 있습니다.

AI 애플리케이션 사용으로 인한 데이터 보안 인시던트가 2023년 27%에서 2024년 40%로 거의 두 배로 증가함에 따라 우려가 커지고 있습니다. 이러한 인시던트의 증가는 멀웨어 및 랜섬웨어 공격이 2023년 50%에서 최대 59%로 급증함에 따라 가속화되었습니다. AI 앱 사용으로 인한 공격은 민감한 데이터를 노출시킬 뿐만 아니라, AI 시스템 자체의 기능을 손상시켜 이미 분열된 데이터 보안 환경을 더욱 복잡하게 만듭니다. 간단하게 말하자면, AI 도구 사용과 관련된 기존 위험과 새로운 위험을 모두 해결할 수 있는 더 강력하고 응집력 있는 데이터 보안 전략의 필요성이 점점 더 시급해지고 있습니다.

1. 2024년 9월 Microsoft의 의뢰로 에이전시 MDC Research에서 시행한 데이터 보안, 거버넌스, 규정 준수, 개인 정보 보호 의사 결정권자를 대상으로 한 설문 조사

앞으로 가야 할 길

데이터 보안 인시던트의 심각성이 증가함에 따라 AI가 도움을 제공할 수 있는 기회가 생겼습니다. 최첨단 기술을 사용하는 조직은 AI 기반 데이터 보안을 구현하여 인시던트 우선순위를 지정하고, 데이터 분류를 자동화하며, 현재 보호 정책을 미세 조정하는 방법을 식별하고 있습니다. AI는 인시던트 경고의 잠재적 심각도를 자동으로 종합하여 데이터 보안 팀에 신속한 대응을 위한 실행 가능한 인사이트를 제공하여 오탐에 소요되는 시간을 줄일 수 있습니다. 이를 통해 워크플로를 간소화하고 데이터 보안 팀이 보다 전략적인 데이터 보안 개선 및 사전 예방적 조치에 집중할 수 있습니다.

2

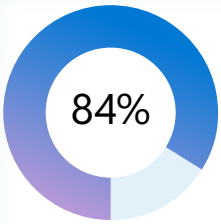
최종 사용자가 AI 앱을 점점 더 많이 채택함에 따라 조직의 가장 민감한 데이터의 무결성이 더 큰 위험에 처해 있어 더 많은 가시성과 새로운 보호 제어가 필요합니다

AI는 빠른 속도로 일상적인 업무를 진행할 때 없어서는 안 될 필수 요소가 되고 있으며, 조직은 이러한 새로운 현실을 수용하고 적극적으로 적응해야 합니다

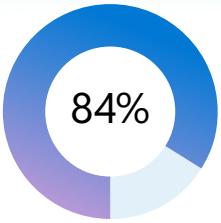
직원들이 AI 도구를 빠르게 채택함에 따라 데이터 보안에 대한 조직의 접근 방식이 크게 변화했습니다. AI는 다른 신흥 기술과 마찬가지로 생산성과 워크플로를 혁신하고 있지만, 기존 위험을 증폭시키거나 민감한 정보를 보호하기 위해 다른 접근 방식을 필요로 하는 새로운 위험을 야기할 수도 있습니다. 그 결과, 기업들은 여전히 빠르게 변화하는 환경에서 발판을 마련하고 있습니다. 운송 부문의 엔지니어링 및 분석 담당 이사는 "AI 측면에서 데이터를 더 주의 깊게 모니터링하고 있습니다. 생산성과 보안, 정확성과 개인정보 보호 사이에 긴장감이 감돌고 있습니다."라고 말합니다.

직원들의 AI 사용 보안에 대한 확신은 여전히 엇갈리고 있습니다. 대다수(84%)는 데이터 입력 관리 및 탐색에 대해 더 확신을 갖고 싶어합니다. 조직 중 22%는 데이터 보안 유지 능력에 대해 매우 확신하고 있지만, 대부분(59%)은 '매우 자신 있다'고 답해 개선의 여지가 있음을 시사합니다. 대부분의 기업(86%)은 AI 도구로 생성된 데이터를 관리하고 발견하는 것에 대해 더 낙관적인 느낌을 갖고 싶다고 인정했습니다.

AI가 일상적인 생산성에 점점 더 중요해짐에 따라 AI 앱의 사용으로 인해 데이터 보안 인시던트에 대한 우려도 높아졌습니다. **조직의 약 3분의 1(31%)이 직원의 AI 사용으로 인해 데이터 보안 인시던트가 증가할 것으로 예상하고 있으며, 84%는 이러한 위험으로부터 보호하기 위해 더 많은 조치를 취해야 한다고 인정합니다.** 이러한 불안감은 특히 규모가 큰 조직에서 높습니다. 중견 기업 중 26%, 대기업 중 29%는 AI 관련 데이터 보안 인시던트가 증가할 것으로 예상하는 반면, 초대형 기업 중 36%에 해당하는 훨씬 더 높은 많은 기업이 AI 관련 데이터 보안 인시던트가 증가할 것으로 예상합니다.



AI 앱 및 도구에 입력된 데이터를 관리하고 발견하는 것에 대해 더 확신을 갖고 싶어하는 비율



직원의 AI 앱 및 도구 사용이 위험하지 않도록 보호하기 위해 더 많은 조치를 취해야 한다는 데 동의하는 비율

무단으로 AI를 사용하는 경우가 만연합니다

응답자 중 40%는 데이터 보안 인시던트로 인해 AI 앱이 이미 침해되거나 손상되었다고 보고했습니다. 다시 말하지만, 다음과 같은 수치는 대규모 조직에서 더 높게 나타납니다. 중견 기업은 36%, 대기업은 38%, 초대형 기업은 44%로 가장 많은 인시던트 발생률을 보고했습니다.

AI를 무단으로 사용하는 경우는 직원이 개인 인증 정보로 로그인하거나 업무 관련 작업을 위해 개인 디바이스를 사용하는 경우 발생하는 경우가 많습니다. **평균적으로 조직 중 65%는 직원이 승인되지 않은 AI 도구를 사용하고 있다고 인정합니다.** 직원이 승인되지 않은 AI 도구를 사용하는 방법은 다음과 같습니다.

- 업무 목적으로 개인 인증 정보로 로그인하는 사용자 53%
- 업무에 AI를 사용할 때 개인 디바이스를 사용하는 사용자 48%
- 개인 목적으로 AI를 사용하기 위해 업무용 개인 인증 정보를 사용하는 사용자 47%

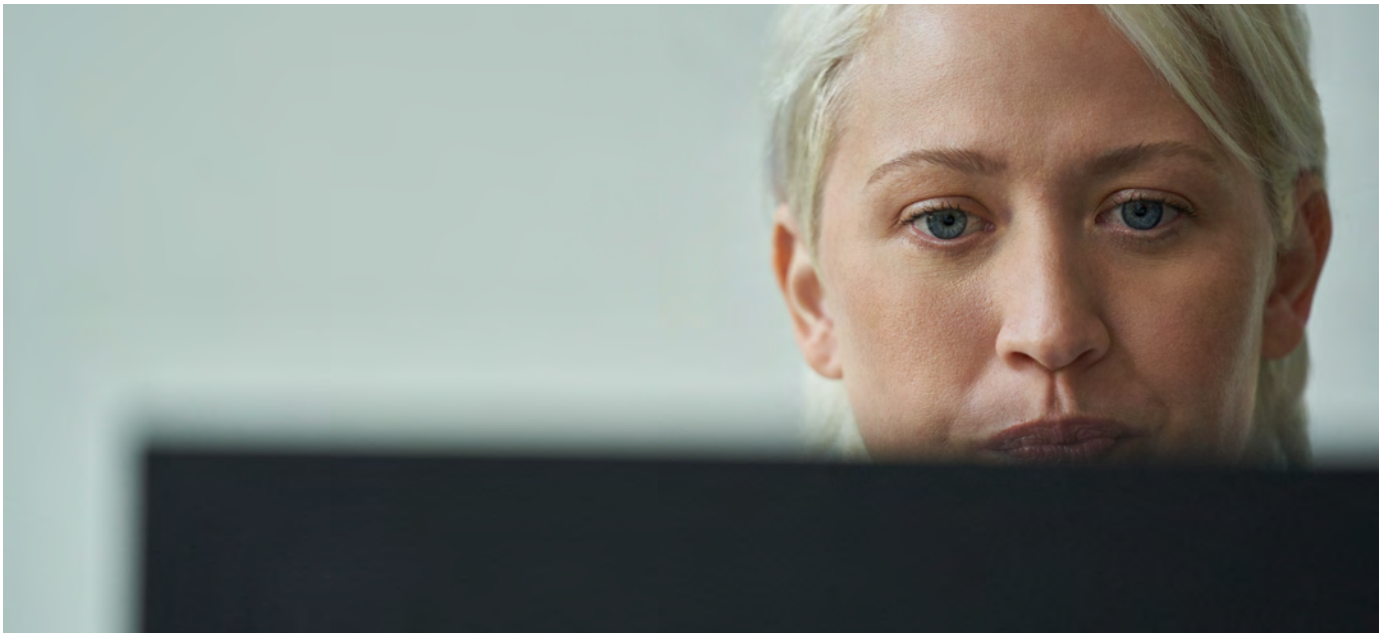
전체 조직 중 절반은 직원이 AI 앱을 안전하지 않은 방식으로 사용할 때 위험을 탐지하고 완화하기 위한 제어 수단이 부족하다는 점에 대해 우려하고 있다고 말합니다. 이러한 수치는 기업 규모에 따라 다르며, 중소기업 중 43%, 대기업 중 50%, 초대형 기업 중 54%가 이러한 위험을 관리할 수 있는 능력에 대해 우려를 표명했습니다.

AI 사용이 증가함에 따라 더 많은 데이터 보안 제어가 필요합니다

AI가 일상 업무에 점점 더 많이 통합됨에 따라 조직은 더 강력한 보호의 필요성을 인식하고 있습니다. **기업 중 96%가 직원의 이러한 도구 사용에 대해 우려하고 있지만, 거의 동일한 비율의 기업이 이러한 우려를 극복하기 위해 솔루션에 투자할 의향이 있습니다.**

"가장 큰 초점은 AI를 어떻게 앞서갈 것인가가 될 것입니다. 보안의 초점은 데이터 크기를 줄이고 데이터를 보다 주의 깊게 모니터링하는 것입니다. AI 측면에서 편향을 식별하기 위해 모델을 더 잘 대표하도록 하려면 더 많은 데이터가 필요합니다. 그렇다면 어떻게 조화를 이룰 수 있을까요?"라고 운송 부문의 엔지니어링, 아키텍처 및 분석 담당 이사는 말합니다. 의사 결정권자의 대다수(87%)는 AI 도구 사용에 대한 보안 관행에 대해 직원을 교육하는 데 시간과 비용을 투자할 준비가 되어 있습니다. **85%가 직원들이 경쟁력을 유지하기 위해 이러한 도구를 사용하는 것이 중요하다고 말하기 때문입니다.**

거의 모든 조직(93%)이 AI 사용에 대한 제어를 개발하거나 구현하는 단계에 있지만, 많은 조직이 아직 초기 단계에 있습니다. 39%만이 AI에 대한 데이터 보안 제어를 완전히 구현했으며, 24%는 정책을 개발했지만 아직 실행에 옮기지 않았습니다. 접객업의 한 데이터 보안 담당 부사장은 "AI에 대한 제어를 조율해야 하지만 조율해야 할 때까지는 AI 사용을 수용하고 있습니다. AI를 통해 더 나은 삶을 살고 효율적으로 일할 수 있습니다."



조직은 AI 앱에서 민감한 데이터가 오용되지 않도록 보호하기 위한 조치를 취하고 있지만, 보다 포괄적인 제어가 필요한 것은 분명합니다. 현재 기업 중 43%는 민감한 데이터가 AI 앱에 업로드되는 것을 방지하는 데 집중하고 있으며, 또 다른 42%는 잠재적인 조사 또는 인시던트 대응을 위해 이러한 앱 내의 모든 활동과 콘텐츠를 기록하고 있습니다. 이와 마찬가지로, 42%는 승인되지 않은 도구에 대한 사용자 액세스를 차단하고 있으며, 이와 동일한 비율은 안전한 AI 사용에 대한 직원 교육에 투자하고 있습니다.

직원이 무단 AI 사용에 관여하는 회사는 특정 유형의 제어에 대한 필요성이 더 높습니다. **AI를 무단으로 사용하는 사용자 중 42%는 AI 쿼리를 기반으로 위험한 사용자를 식별하기 위한 제어가 필요한 반면, 무단으로 사용하지 않는 사용자의 경우 30%가 필요합니다. 또한 무단 AI 사용을 처리하는 조직의 40%는 데이터 수명 주기(예: 보존 및 삭제 프로토콜)를 관리하기 위한 제어가 필요한 반면, 이 문제가 없는 기업의 경우 27%에 불과합니다.**

AI 제어가 필요한 상위 5가지 이유

민감한 데이터가 AI에 업로드되지 않도록 방지	43%
잠재적인 조사 또는 인시던트 대응을 위해 AI 도구에 모든 활동과 콘텐츠 기록	42%
승인되지 않은 AI 도구에 대한 사용자 액세스 권한 차단	42%
안전한 AI 도구 사용에 대한 직원 교육	42%
AI에 대한 쿼리를 기반으로 위험한 사용자 식별	41%

앞으로 가야 할 길

강력한 데이터 보안 태세를 유지하기 위해 팀은 AI 앱에서 데이터를 검색, 보호, 관리하기 위한 완전한 제어 세트가 필요합니다. 다음은 팀이 사용할 수 있는 세 가지 핵심 전략입니다.

AI 앱 사용 및 앱을 통한 데이터 흐름에 대한 가시성 향상: AI 앱을 탐지하고 사용할 수 있는 데이터 보안 도구를 활용합니다. 이러한 도구는 지원되는 데이터 보안 제어 및 규정 준수와 같은 세부 정보를 포함하여 위험 프로필과 함께 사용 중인 AI 앱의 포괄적인 목록에 대한 인사이트를 제공합니다. AI 상호 작용에서 민감한 데이터에 대한 일관된 분류를 제공하고 AI 앱을 통한 데이터 흐름에 대한 트렌드를 표시할 수 있는 도구를 사용합니다.

정책 개발 및 시행: 분석에서 얻은 인사이트를 기반으로 정책을 만듭니다. 이러한 정책에는 승인된 AI 앱에 대한 지침과 승인되지 않은 앱의 직원 사용을 차단하거나 제한하는 절차가 포함될 수 있습니다. 승인된 AI 앱에서도 민감하지 않은 데이터가 통과할 수 있도록 하는 동시에 민감하고 비즈니스 크리티컬한 데이터의 사용을 제한하는 세분화된 정책을 만들 수 있습니다. 데이터 보안을 보장하기 위해 민감한 데이터를 브라우저 기반 AI 도구에 붙여넣는 것과 같은 특정 작업 차단이 이에 포함될 수 있습니다.

정기적으로 위험 평가 및 정책 구체화: 사용 중인 AI 앱의 위험 수준, 민감한 데이터가 이러한 앱을 통해 흐르는 방식에 대한 트렌드, 이러한 앱과 관련된 사용자 활동을 보여주는 보고서를 정기적으로 생성합니다. 이는 전반적인 위험 환경을 평가하고 가장 관련성이 높은 데이터 보안 정책에 대해 정보에 입각한 결정을 내리는 데 도움이 됩니다.

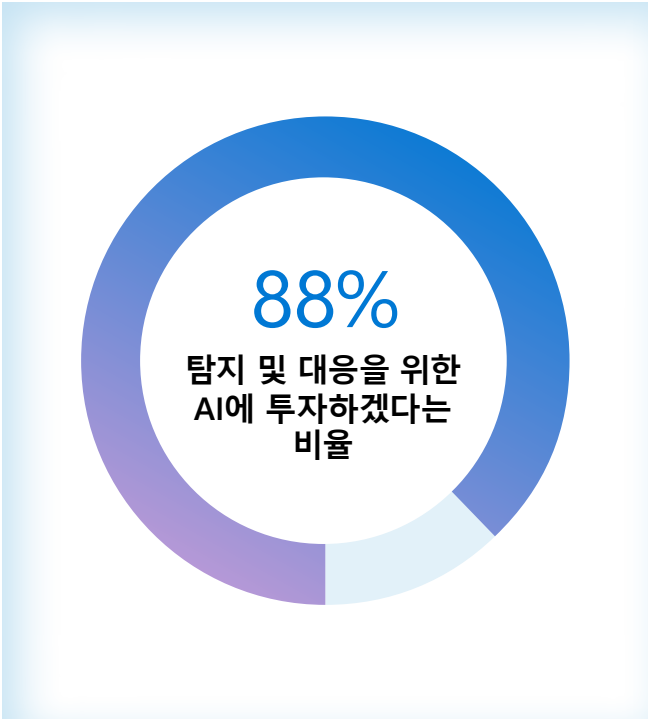
3

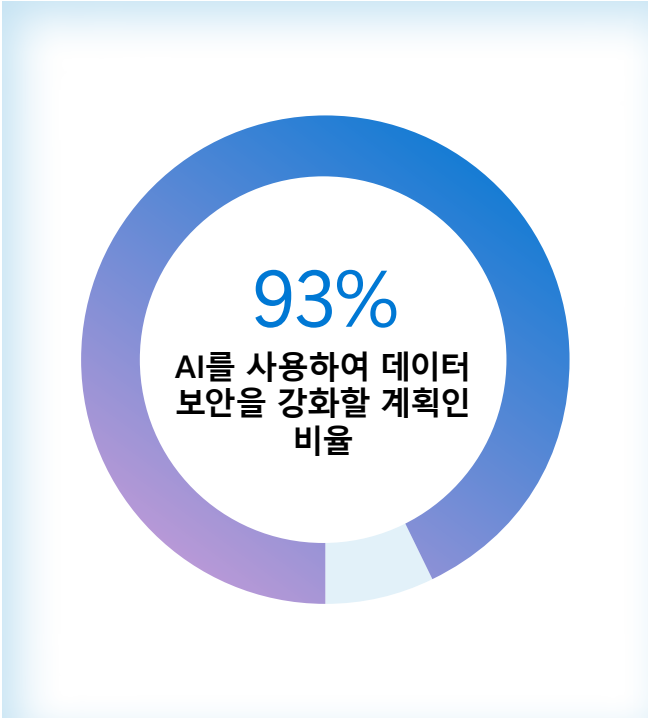
의사 결정권자들은 데이터 보안 노력을 강화할 수 있는 AI의 잠재력에 대해 낙관적으로 생각합니다

데이터 보안 조사는 AI에 크게 의존합니다

조직의 대다수(88%)는 민감한 데이터를 발견하고, 비정상적인 활동을 탐지하며, 위험에 처한 데이터를 자동으로 보호하는 등 탐지 및 대응 노력을 개선하기 위해 이미 AI에 투자하고 있습니다. **조직 중 77%는 AI가 이러한 프로세스를 가속화할 것이라고 믿고 있으며, 76%는 AI가 탐지 및 대응 전략의 정확도를 향상시킬 것이라고 생각합니다.**

의사 결정권자 중 73%가 데이터 보안을 강화하기 위해 AI를 사용하는 것에 대해 우려를 표명한 반면, 50%는 데이터 보안을 강화하기 위해 AI를 사용하는 것을 방해하지 않았다고 답했으며, 23%만이 AI가 이를 방해했다고 답했습니다. 전체적으로 93%라는 압도적인 응답자가 이와 같은 우려에도 불구하고 데이터 보안을 강화하기 위해 AI를 사용할 계획이라고 답했습니다.



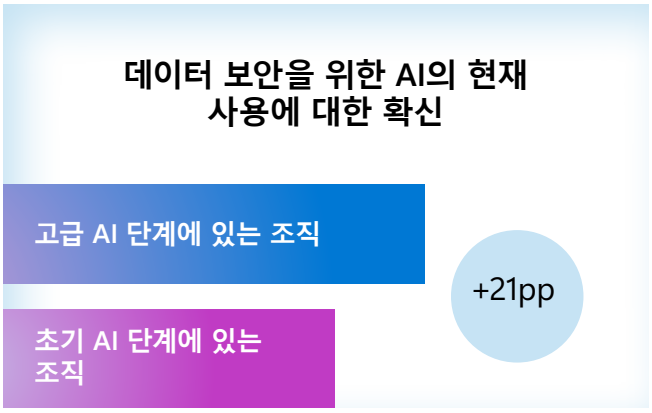


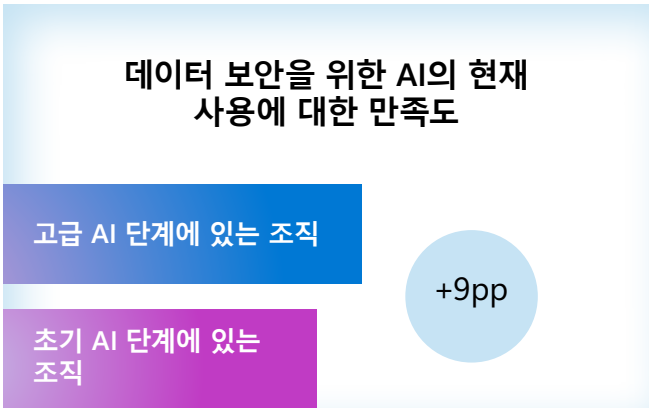
AI를 사용하여 데이터 보안을 강화하면 가시성, 신뢰성, 만족도가 높아집니다

AI를 사용하여 데이터 보안을 강화할 때의 주요 이점 중 하나는 시스템 전반의 가시성을 높여 데이터 저장 위치 및 분류 방법에 대한 의사 결정권자의 주요 우려(20%)를 완화할 수 있다는 점입니다.[1] 데이터 보안 의사 결정권자 중 88%는 AI를 데이터 보안 솔루션에 통합하면 팀이 더 많은 가시성을 확보할 수 있으며, 이를 통해 조직은 그렇지 않은 경우보다 훨씬 더 많은 데이터를 처리하고 분석할 수 있다고 생각합니다. 중간 규모 조직은 주로 데이터 보안 프로세스에서 인적 오류를 최소화하는 것과 같은 단기적인 위험을 줄이는 데 중점을 둡니다. 실제로 중견 기업 중 43%가 인적 오류로 인한 위험을 줄이는 것을 우선시하는 반면, 초대형 기업의 경우 37%에 불과합니다.

이와는 대조적으로, 대기업은 장기적인 위험과 적응력의 필요성을 강조하는 접근 방식이 더 발전되어 있습니다. 이처럼 정교함이 높아짐에 따라 데이터 보안 팀은 진화하는 위험에 더 잘 적응할 수 있으며, 이는 중견 기업의 43%에 비해 초대형 기업의 49%에서 최우선 순위로 두고 있습니다.

전반적으로 데이터 보안을 강화하기 위해 AI를 더 많이 사용하는 조직은 데이터 보안 전략에 대한 확신과 만족도가 훨씬 더 높다고 보고합니다. **AI 구현의 고급 단계에 있는 응답자 중 90%는 데이터 보안을 강화하기 위해 AI를 사용하는 것에 대해 매우 또는 매우 확신한다고 답한 반면, 초기 단계의 응답자는 69%에 불과했습니다. 이와 마찬가지로, AI를 고도로 활용한 조직 중 76%가 데이터 보안 솔루션에 만족을 표명한 반면, 초기 단계에 있는 조직의 67%만이 만족한다고 보고했습니다.**





1. 2024년 9월 Microsoft의 의뢰로 에이전시 MDC Research에서 시행한 데이터 보안, 거버넌스, 규정 준수, 개인 정보 보호 의사 결정권자를 대상으로 한 설문 조사

조직은 AI를 통해 데이터 보안 인시던트의 수를 줄이고 경고 관리를 개선하고 있습니다

AI를 사용하여 데이터 보안 운영을 강화하는 조직은 훨씬 적은 경고를 받는다고 보고합니다. **AI 기반 데이터 보안 도구를 구현한 사람들은 평균적으로 하루에 47개의 경고를 받는 반면, 그렇지 않은 사람들은 79개의 경고를 받습니다. 또한 AI를 사용하는 조직은 일일 경고 중 66%를 검토할 수 있는 반면 AI를 사용하지 않는 조직은 60%만 검토할 수 있습니다.**

뿐만 아니라, 데이터 보안을 강화하기 위해 AI를 사용하는 기업은 위험을 완화하기 위해서도 AI를 사용할 가능성이 더 높습니다(56% vs. 26%). AI를 활용하여 경고를 완화할 수 있는 능력의 증가와 함께 경고의 양이 감소한 것은 전체 데이터 보안 인시던트 수에 극적인 영향을 미친 것으로 보입니다. 데이터 보안을 강화하기 위해 AI를 구현한 조직은 데이터 보안을 강화하기 위해 AI를 사용하지 않는 조직에 비해 데이터 보안 인시던트가 65% 감소했습니다.

AI가 대응에 가장 큰 영향을 미칠 것으로 예상됩니다

탐지 측면에서 의사 결정권자 중 33%는 AI가 비정상적인 활동을 탐지하는 데 도움이 될 것으로 예상하며, 23%는 잠재적인 데이터 보안 인시던트를 조사하는 데 도움이 될 것이라고 생각합니다. 또 다른 22%는 AI가 데이터 환경의 보안을 강화하기 위한 권장 사항을 제공할 수 있는 잠재력에 대해 확인했습니다.

그러나 의사 결정권자들이 AI가 가장 큰 영향을 미칠 것으로 기대하는 분야가 바로 대응입니다. 응답자 중 34%는 AI가 민감한 데이터의 부적절한 공유를 자동으로 차단할 수 있다고 답했으며, 32%는 AI가 위험에 처한 데이터를 보호할 것이라고 답했습니다. 또 다른 26%는 AI가 데이터 보안 위험을 완화하고 적절한 제어를 적용하는 데 도움이 될 것으로 예상했으며, 같은 수치는 AI가 위험한 사용자 행동을 자동으로 플래그 지정할 것으로 예상했습니다.

앞으로 가야 할 길

AI를 데이터 보안 솔루션에 통합하면 팀에 실시간 지침, 요약 기능, 자연어 지원을 제공하여 간과했을 수도 있는 영역을 집중 조명하는 데 도움이 될 수 있습니다. 또한 조사를 가속화하고 데이터 보안 팀 전반의 전문성을 강화할 수 있습니다. 이러한 기능이 미치는 영향은 다음과 같습니다.

경고 요약: 조사는 분석해야 할 소스의 양과 다양한 정책 규칙으로 인해 어려울 수 있습니다. DLP(데이터 손실 방지) 및 IRM(내부자 위험 관리)에 AI를 임베딩함으로써 팀은 소스, 정책 규칙, 사용자 위험 인사이트를 포함한 경고 요약을 신속하게 수신하여 손상된 민감한 데이터와 관련 사용자 위험을 이해할 수 있습니다.

상황별 커뮤니케이션: 조직은 비즈니스 커뮤니케이션과 관련된 규정 요구 사항을 준수해야 하는데, 이를 위해서는 위반에 대한 광범위한 검토가 필요한 경우가 많습니다. AI는 데이터 보안 팀이 규정 및 기업 정책에 따라 콘텐츠를 평가하여 데이터 보안 인시던트를 초래할 수 있는 고위험 커뮤니케이션을 강조하는 데 도움이 될 수 있습니다.

키워드 쿼리에 대한 자연어: 검색은 조사를 진행하는 동안 복잡하고 시간이 많이 걸리는 워크플로일 수 있으며, 이를 진행하려면 일반적으로 키워드 쿼리 언어를 사용해야 합니다. AI를 통해 데이터 보안 팀은 자연어로 검색 프롬프트를 입력하여 검색 시작을 간소화하고 보다 고급 조사를 수행할 수 있습니다.

최종 권장 사항

1 통합형 플랫폼을 채택하여 데이터 보안 인시던트를 방지합니다

완전 통합형 데이터 보안 플랫폼을 채택하면 점점 더 진화하는 환경에서 더 안전하고 간소화된 전략을 제공하여 복잡성을 줄이고 가시성을 높이는 동시에 보호를 강화할 수 있습니다. 통합형 접근 방식은 데이터 보안 제어를 중앙 집중화하고 데이터, 사용자, 활동에 대한 통합된 가시성을 제공하여 데이터 위험에 대한 탐지 및 보호를 강화하고 간소화함으로써 조직이 데이터 보안 태세 관리를 개선하는 데 도움이 될 수 있습니다. 조직 중 82%가 통합형 플랫폼이 우수하다는 데 동의하는 만큼, 통합을 향한 움직임은 유익할 뿐만 아니라 필수적입니다.

2 AI의 내부 사용에 대한 가시성을 높여 생산성에 영향을 미치지 않는 AI를 사용하는 직원에 대한 필요한 제어 평가

AI가 직장에서 점점 더 보편화됨에 따라 기존 위험을 증폭시키고 새로운 위험을 도입할 수 있습니다. 조직은 안전하지 않은 AI 사용을 방지하기 위해 더 많은 조치를 취해야 한다는 사실을 인정합니다. AI 앱에 내장된 제어 및 가시성을 활용하는 것은 생산성을 방해하지 않고 데이터 보안을 유지하는 데 매우 중요합니다. 직원을 대상으로 안전한 AI 사용에 대해 교육하면 조직이 위험한 행동을 최소화하는 동시에 팀이 이러한 강력한 도구를 계속 활용할 수 있도록 할 수 있습니다.

3 AI의 도움으로 데이터 보안 전략 수준 향상

AI를 통해 데이터 보안 팀은 끊임없는 위협과 많은 양의 경고에 대응하는 대신 보다 전략적인 이니셔티브에 집중할 수 있습니다. AI 구현의 고급 단계에 있는 기업은 이제 막 시작하는 기업보다 데이터 보안 솔루션에 대해 더 확신하고 더 만족합니다. 포괄적인 데이터 보안 전략의 일환으로 AI를 배포함으로써 조직은 가시성을 향상시켜 위험을 탐지하고 이에 대응하는 능력을 강화하여 궁극적으로 전반적인 데이터 보안 태세를 강화할 수 있습니다.

연구 목표

연구 목표는 다음과 같습니다.

1. 데이터 보안 인시던트에 대한 우선순위, 마음가짐, 과제, 원인 및 노력 등 데이터 보안 환경에 대해 이해합니다.
2. 새롭게 떠오르고 있는 전략과 혁신 그리고 조직이 미래에 투자하고자 하는 방법 등 데이터 보안에 대한 미래를 살펴봅니다.
3. 데이터 보안을 강화하는 AI 역할과 데이터를 보호하는 데 AI가 수행하는 역할을 파악합니다.

방법론

2024년 8월 5일부터 8월 23일까지 1,376명의 데이터 보안 의사 결정권자를 대상으로 15분 동안 다국적 온라인 설문 조사가 실시되었습니다.

질문은 2023년과 비교하여 데이터 보안 환경과 데이터 보안 인시던트에 집중되었습니다. 또한 올해 설문 조사에는 직원의 AI 사용 보안과 데이터 보안 강화를 위한 AI 사용에 대한 질문이 포함되었습니다.

대상 모집

선별 기준을 충족하기 위해 데이터 보안 의사 결정자는 다음 조건을 갖춰야 했습니다.

- 데이터 보안에 대한 관점을 지닌 CISO 및 인접 의사 결정권자 (C-2 이상)
- 엔터프라이즈급 조직에서 근무 (500명 이상의 직원, 다양한 규모)
- 규제 산업 및 비규제 산업의 혼합 (교육, 정부 기관, 또는 비영리 단체 제외)

연구를 위해 설문 조사에 참여한 1,376명의 데이터 보안 의사 결정권자 국가는 다음과 같습니다.

- 미국: 302
- 영국: 305
- 인도: 301
- 브라질: 158
- 프랑스: 156
- 호주: 154

hypothesis Microsoft Security