Microsoft

hypothesis

데이터 보안 인덱스

데이터 보안을 위한 트렌드, 인사이트, 전략

머리말

데이터의 급증으로 정의되는 시대에 조직의 데이터는 생명선에 불과하다는 것이 점점 더 분명해지고 있습니다. 조직에서 생성하고 사용하는 풍부한 데이터는 중요한 운영을 지원하고, 전략적 및 글로벌 의사 결정에 정보를 제공하며, 미래의 가능성을 형성합니다. 데이터는 단순한 리소스가 아니라 현대적인 기업의 핵심입니다.

그러나 데이터에 대한 의존도가 높아짐에 따라 디지털 섀도우의 취약성이 실제로 빠르게 확장되고 있다는 냉혹한 현실이 도래하고 있습니다. 사이버 위협, 데이터 유출, 내부자 위험 인시던트의 발생 빈도는 더 이상 드물지 않습니다. 이러한 현상은 널리 퍼져 있고 점점 더 커지고 있으며, 데이터에 의존하는 조직에 위험을 초래하고 있습니다. 최근 설문 조사에 참여한 의사 결정권자 중 89%는 데이터 보안 태세가 전반적인 성공에 매우 중요하다고 생각한다고 답했습니다.

이 백서에서는 조직의 데이터 보호라는 근본적인 필수 요소에 대해 살펴봅니다. 저희 팀과 저는 이러한 연구 결과를 여러분과 공유하게 된 것을 기쁘게 생각하며, 이를 계기로 데이터 보안을 탁월함을 향해 공동으로 발전시키는 방법에 대한 대화를 시작하기를 바랍니다. 연구를 통해 학습한 내용은 데이터 보안이 얼마나 중요한 시점에 있는지 보여줍니다. 보안 의사 결정권자는 데이터 보안이 데이터 안전에 필수적이라는 데 동의하고 대부분이 자신이 하는 일에 확신을 가지고 있다고 말하지만, 동시에 수많은 데이터 보안 인시던트와 과제를 경험하고 있습니다. 그리고 우리가 인터뷰한 리더 중 80%는 제품군에 가장 적합한 통합 접근 방식이 포인트 솔루션보다 우수하다는 사실을 알고 있었지만, 대부분의 기업은 여전히 데이터를 보호하기 위해 단편화된 다중 도구 시스템을 사용하고 있어 이로 인해 보안 인시던트가 줄어들기는커녕 더 많이 발생하는 경우가 많습니다.

이 최신 보고서를 읽고 공유하여 팀의 미래를 가장 잘 보호할 수 있는 방법에 대한 새로운 대화의 시작으로 삼으시기 바랍니다.

Rudra Mitra
기업 부사장
Microsoft 데이터 보안 및 규정 준수

서문

데이터 침해 및 기타 보안 인시던트를 예방하는 것은 보안 및 위험 의사 결정권자에게 지속적인 관심사이자 모든 사이버 보안 프로그램의 초석이 될 수 있습니다. 조직은 직원 및 고객 정보, 지적 재산, 재무 예측, 운영 데이터를 포함한 광범위한 민감한 데이터를 보호해야 합니다.

현재 데이터 보안 관행 및 트렌드를 이해하고 조직이 데이터 보안을 강화할 수 있는 기회를 식별하기 위해 Microsoft는 독립 연구 기관인 Hypothesis Group에 800명 이상의 데이터 보안 전문가를 대상으로 다국적 설문 조사를 실시하도록 의뢰했습니다. 이 보고서는 데이터 보안을 위한 트렌드, 인사이트, 전략을 포함하여 연구의 5가지 주요 결과를 제시합니다.

주요 조사 결과

1

의사 결정권자는 자신이 보호받고 있다고 생각하지만, 현실은 이들의 인식과 일치하지 않습니다.

대부분의 의사 결정권자는 데이터 보안 솔루션에 만족하고 이를 확신한다고 말하지만, 여전히 연간 평균 59건의 데이터 보안 인시던트가 발생하며 이로 인한 영향을 비용이 많이 소요됩니다.

2

더 많은 도구를 보유한다고 해서 데이터 보안이나 효율성이 향상되는 것은 아닙니다. 오히려 그 반대입니다.

의사 결정권자 중 80%는 포괄적인 통합형 솔루션이 동급 최고의 수동 솔루션보다 우수하다는 데 동의하지만, 도구에 대한 조직의 접근 방식은 평균 10개 이상의 데이터 보안 도구를 사용하며 계속 파편화되고 있습니다. 그러나 가장 많은 도구를 사용하는 사람들은 더 많은 데이터 보안 인시던트를 경험하는데, 이는 도구가 확산될수록 보안이 약해진다는 것을 시사합니다.

3

조직은 특히 비즈니스 데이터에서 외부 및 내부 데이터 보안 인시던트로 인한 스트레스에 계속 시달리고 있습니다.

설문 조사에 참여한 조직 중 50%가 작년에 랜섬웨어 또는 멀웨어 공격을 경험했으며, 많은 의사 결정권자는 조직이 향후 공격을 예방하고 해결할 준비가 완전히 되어 있지 않다고 생각합니다. 내부적으로는 악의적인 내부자가 가장 큰 관심사입니다. 또한 조직은 비즈니스 데이터의 취약성에 대해 매우 우려하고 있습니다. 이는 위험을 포괄적으로 해결하는 보안 플랫폼의 필요성을 다시 한 번 강조합니다.

주요 조사 결과

4

조직은 디지털 트랜스포메이션을 추진하기 위해 클라우드와 AI가 필요하지만, 이는 가장 취약한 데이터 위치이기도 합니다.

클라우드 애플리케이션과 AI 기술은 조직의 협업과 생산성에 필수적인 요소가 되었지만, 이러한 진화로 인해 더욱 역동적이고 다면적인 위험도 발생했습니다. 조직이 AI를 수용함에 따라 책임 있고 안전한 사용을 지원하기 위해 데이터 보안을 강화하는 것이 중요해지고 있습니다.

5

자동화와 AI는 보호력을 강화할 수 있는 유망한 방법입니다.

조직은 팀이 탐지하는데 소요되는 시간을 줄이고 예방에 더 많은 시간을 할애하기를 원합니다. 자동화를 통해 팀은 사전 예방적 조치에 더 집중할 수 있으며, 데이터 보안에 AI를 사용하면 조직이 미래의 위협에 대해 보다 전략적이고 현명해질 수 있습니다.

1

의사 결정권자는 자신이 보호받고 있다고 생각하지만, 현실은 이들의 인식과 일치하지 않습니다.

의사 결정권자는 자신이 보호받고 있다고 생각하지만, 현실은 이들의 인식과 일치하지 않습니다.

표면적으로 의사 결정권자는 데이터 보안 솔루션에 대해 높은 수준의 신뢰와 만족도를 예상하지만, 대부분의 조직은 데이터 보안 제어가 데이터 침해를 방지하는 데 충분하다는 데 동의하고, 대부분의 데이터가 어디에 있는지 알고 있으며, 데이터와 관련된 대부분의 위험을 탐지할 수 있다고 생각합니다.

이와 동시에, 조직은 지난 12개월 동안 평균 59건의 데이터 보안 인시던트를 계속 경험하고 있으며 그 중 5분의 1은 '심각한' 것으로 간주됩니다. 이러한 인시던트의 영향은 평균적으로 만연합니다. 조직은 가장 심각한 데이터 보안 인시던트의 총 재정적 비용이 약 미화 244,000달러라고 추정하며, 이는 연간 인시던트에 최대 미화 1,500만 달러의 비용이 들 수 있음을 의미합니다. 이러한 비용 외에도 의사 결정권자 10명 중 4명은 데이터 보안 인시던트에 대한 복구 운영 비용과 평판 손상으로 인한 비즈니스 손실이 매우 우려된다고 말합니다.

또한 92%는 주로 비용, 통합, 구현 시간 부문에서 문제에 직면해 있는데, 이는 데이터 보안에 대한 추가 투자 능력을 저해하여 보다 예산 친화적이고 노동 효율적인 솔루션의 필요성을 강조합니다.

데이터 보안 준비 상태에 대한 신뢰도는 조직이 경험하고 있는 인시던트의 현실과 다릅니다. 조직이 데이터의 위치를 파악하고 위험을 탐지하는 것이 중요하지만, 이러한 조치는 개별적으로 또는 별도로 조직이 데이터 보안 및 위험 의사 결정자가 밤새 일하게 함으로써 인시던트를 방지하는 데 충분하지 않습니다.

금융 서비스 분야의 한 CISO(최고 정보 보안 책임자)는 "이사회에 '데이터를 보호했지만 안전하게 보호하지 않았을 뿐'이라고 말할 수 없습니다. 우리 은행이 월스트리트 저널의 첫 페이지에 실리지 못하는 것을 보고 싶지는 않습니다."라고 말합니다.

59

지난 12개월 동안의 평균 데이터 보안 인시던트 수

최대 $1,500만

심각한 보안 인시던트로 인한 연간 비용

2

더 많은 도구를 보유한다고 해서 데이터 보안이나 효율성이 향상되는 것은 아닙니다. 오히려 그 반대입니다.

더 많은 도구를 보유한다고 해서 데이터 보안이나 효율성이 향상되는 것은 아닙니다. 오히려 그 반대입니다.

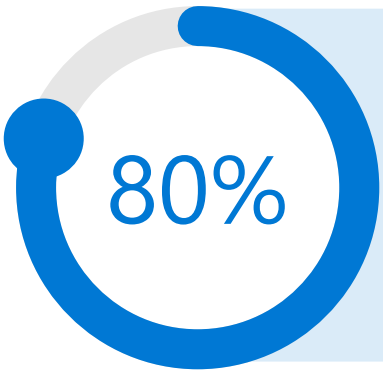
조직은 수년간의 포인트 솔루션 접근 방식으로 인해 사일로화된 데이터 보안 도구로 가시성과 효율성에 격차가 발생했다는 사실을 깨닫고 있습니다. 이러한 트렌드는 현재 데이터 보안을 위한 통합형 솔루션을 갖추고자 하는 욕구로 바뀌고 있으며, 80%는 통합형 솔루션을 갖춘 포괄적인 데이터 보안 플랫폼이 수동으로 통합 및 관리해야 하는 동급 최고의 여러 솔루션을 사용하는 것보다 우수하다는 데 동의했습니다.

그러나 대다수가 통합형 솔루션이 우수하다고 생각하지만, 데이터 보안 도구를 많이 사용하고 이러한 도구는 단편적입니다.

그 결과, 조직은 데이터 손실 방지, 정보 보호, 내부자 위험 관리, SIEM(보안 정보 및 이벤트 관리), 클라우드 액세스 보안 브로커 등을 포함하여 데이터 보안 위험을 해결하기 위해 평균 10개의 데이터 보안 도구를 사용하고 있다고 보고합니다. 직원이 5,000명 이상인 조직의 경우 평균 도구 수가 훨씬 더 많습니다.

더 많은 도구(16개 이상)를 사용하는 사람들이 더 적은 도구를 사용하는 사람들(61% 대 56%)에 비해 데이터 보안 태세에 더 확신을 갖기 때문에 더 많은 도구를 사용하면 잘못된 보안 감각을 갖게 될 수 있습니다.

그러나 연구 결과에 따르면 16개 이상의 도구를 사용하는 조직은 작년에 더 많은 데이터 보안 인시던트(평균 133건)를 경험한 반면, 도구가 적은 조직의 경우 48건의 인시던트가 발생했기 때문에 보안 감각과 모순됩니다.



통합형 솔루션을 갖춘 포괄적인 보안 플랫폼이 수동으로 통합하고 관리해야 하는 동급 최고의 솔루션을 여러 개 사용하는 것보다 우수하다는 데 동의합니다.

2.8배

작년에 더 많은 데이터 보안 인시던트

16개 이상의 도구가 있는 조직의 경우(더 적은 수의 도구를 사용하는 조직과 비교)

더 많은 통합형 솔루션과 더 적은 수의 도구를 통해 더 강력한 데이터 보안에 대한 사례는 동급 최고의 솔루션 또는 더 많은 도구를 선호하는 사람들의 감정과 관행을 볼 때 더욱 강력해집니다.

"꽤 많은 시스템에서 데이터를 어떻게 수집, 집계, 사용해야 할까요? 실제로 작동하려면 다양한 데이터 포인트를 하나의 생태계에 모아야 합니다. 그렇지 않으면 부실한 데이터 보안 버전을 사용하게 됩니다."

IT 부문 부사장
제조/생산

첫째, 다양한 데이터 보안 도구로 인해 가시성이 격차가 발생하고 섀도우 데이터가 늘어날 수 있습니다. 실제로 섀도우 데이터에 대해 우려하는 사람들은 동급 최고의 솔루션을 선호할 가능성이 더 큽니다. 이는 동급 최고의 접근 방식을 사용하는 조직이 데이터 보안 태세에 대한 포괄적인 가시성을 확보하려면 더 많은 노력을 기울여야 하기 때문일 가능성이 큽니다.

둘째, 사일로화된 솔루션을 관리하면 다양한 각 솔루션에는 전담 직원, 엔드포인트 에이전트 설치 및 유지 관리, 다양한 새로운 프로세스가 필요하기 때문에 데이터 보안 팀이 더 복잡해집니다. 직원과 리소스가 필요한 작업 중 하나인 경고 검토 및 심사를 예로 들어 보겠습니다. 경고 수가 증가한다는 것은 격리된 솔루션을 관리할 때 데이터 보안 팀에 추가 노력이 필요하다는 것을 의미합니다. 더 많은 도구를 사용하는 조직은 하루 평균 96개의 데이터 보안 경고를 받는 반면, 더 적은 도구를 사용하는 팀은 44개로 그 절반 미만을 받습니다. 또한 도구가 적은 팀만큼 이러한 경고를 검토할 수 없습니다(68% 대비 61%). 이로 인해 더 많은 도구를 사용하는 조직이 더 적은 양의 도구를 사용하는 조직에 비해 더 사후 대응적인 경우가 많습니다.

마지막으로, 도구가 많을수록 조직은 인사이트와 수정 계획을 통합하기 위해 광범위한 노력을 기울여야 하며 번역 과정에서 정보가 손실될 수 있습니다. 가장 큰 데이터 보안 과제에 대해 물었을 때 데이터 보안 솔루션을 구현하거나 유지 관리하는 비용과 데이터 보안 솔루션을 통합하는 문제가 상위 2개로 꼽혔습니다.

이는 더 길고 느린 프로세스라고 해석됩니다. 16개 이상의 도구를 사용하는 사람들의 37%가 데이터 보안 조사를 완료하는 데 1개월 이상이 필요하다고 보고한 반면, 더 적은 도구를 사용하는 사람들은 21%에 불과했습니다.

"지금 현재, 우리는 기어 다니고 있습니다. 우리가 보유한 모든 시스템에는 고유한 포털, 고유한 도구, 사물을 처리하는 고유한 방법이 있습니다. 각자는 자신이 전문가인 분야에서 자신의 길을 갑니다. 그런 다음 우리 모두는 다시 모여 무슨 일이 일어나고 있는지 결정하고 문제를 바로 해결합니다. 따라서 이 시점에서 약간의 수작업이 필요합니다."라고 제조 및 생산 분야의 인프라 및 운영 이사는 말했습니다.

궁극적으로, 다양한 솔루션을 계속 사용하기로 선택함으로써 조직은 통합형 솔루션이 우수하다는 자신의 의견을 무시하고 시간과 비용을 낭비하는 반대 방향으로 나아가고 있습니다.

더 적은(16개 미만) 데이터 보안 도구와 더 많은(16개 이상) 데이터 보안 도구를 사용하는 사람들을 비교한 결과

	적은 양의 도구	많은 양의 도구
지난 12개월 동안 **데이터 보안 인시던트**의 수	**48**	**133**
심각한 데이터 보안 인시던트 비율	19%	26%
현재 우리의 데이터 보안 전략언 보다 **사후 대응적**	31%	40%
솔루션 **통합** 시 어려움 경험	24%	39%
데이터 보안 팀은 **대응** 시 가장 많은 시간 할애	19%	26%
우리는 데이터 보안 태세에 **확신이 있음**	56%	61%
평균적으로 하루에 **수신**되는 경고 수	44	96
하루에 **검토**할 수 있는 경고 비율	68%	61%
데이터 보안 조사를 완료하는 데 1개월 이상 필요	21%	37%

3

조직은 특히 비즈니스 데이터에서 외부 및 내부 데이터 보안 인시던트로 인한 스트레스에 계속 시달리고 있습니다.

조직은 특히 비즈니스 데이터에서 외부 및 내부 데이터 보안 인시던트로 인한 스트레스에 계속 시달리고 있습니다.

데이터와 상호 작용하는 사람, 데이터 관련 활동, 데이터 처리에 사용되는 디바이스 및 앱을 포함하여 데이터 관련 요소가 지속적으로 진화함에 따라 데이터 보안 인시던트 및 데이터 침해가 언제 어디서나 발생할 수 있습니다. 그리고 이러한 위협은 외부 공격자뿐만 아니라 직원, 계약자, 파트너를 포함한 신뢰할 수 있는 직원 모두를 통해 발생합니다. 악의적이든 우발적이든 모든 플레이어가 데이터 보안 인시던트를 일으킬 수 있는데, 이는 다양한 영역에서 지속적으로 보호해야 함을 의미합니다.

금융 서비스 부문의 IT 담당 부사장은 "보호하고자 하는 것은 항상 변화하고 있습니다. 움직이는 표적입니다. 항상 진화하고, 변화하고, 유연할 것입니다. 보호하고 있는 대상과 대상이 있는 위치는 점점 더 다양해질 것입니다."

데이터 보안 인시던트는 다양한 소스에서 발생할 수 있지만, 멀웨어 또는 랜섬웨어 인시던트의 외부 위협(악성 소프트웨어가 시스템에 침투하여 공격자에게 시스템 또는 네트워크에 대한 무단 액세스를 제공하는 경우)이 가장 일반적이며, 설문 조사에 참여한 조직 중 50%가 작년에 최소 한 번 이상 경험했습니다.

또한 이러한 공격은 조직이 가장 취약하다고 느끼는 부분으로, 41%는 내년에 향후 맬웨어 또는 랜섬웨어 공격을 처리할 준비가 되어 있지 않다고 답했습니다. 이러한 취약성은 동급 최고의 접근 방식을 선호하는 사람들 사이에서 훨씬 더 높으며, 통합 솔루션을 선호하는 사람들은 36%인 것에 비해 44%는 이러한 성격의 공격에 대비할 준비가 되어 있지 않다고 느낍니다.

내부자 위험으로부터 보호하고 예방하는 것 역시 의사 결정권자의 최우선 과제입니다. 35%는 악의적인 내부자 및 손상된 계정에 대한 방어를 강화해야 한다고 답했으며, 3분의 1은 의도하지 않은 내부자 인시던트에 대해 우려하고 있습니다. 악의적인 내부자 인시던트가 데이터 보안 침해의 주요 원인은 아닐 수 있지만, 의사 결정권자가 예방할 준비가 가장 덜 되어 있다고 느끼는 두 번째로 일반적인 유형의 인시던트입니다.

"적어도 한 달에 한 번은 패닉에 빠진 이사로부터 전화를 받습니다... '우리가 사건을 겪었다거나, 내가 사건을 발견했다거나, 위협 팀이 사건을 발견했다'고 말합니다. 이들 중 일부는 의도하지 않았고, 일부는 자신의 특권이 허용하는 것을 알지 못하거나 이해하지 못하는 사람들입니다."

미국 정부 기관 CISO

내부자는 일반적으로 대중이 사용할 수 없는 회사 리소스, 데이터 또는 시스템에 대한 액세스 권한이 부여되었거나 지식을 보유하고 있는 신뢰할 수 있는 개인입니다. 결과적으로 내부자와 관련된 데이터 보안 위험은 더 파악하기 어렵고 탐지하기 어려운 경향이 있습니다. Microsoft의 CISO인 Bret Arsenault는 "궁극적으로 위반이 의도적인지 우발적인지는 중요하지 않습니다. 내부자 위험 프로그램은 모든 회사의 보안 전략의 일부가 되어야 합니다."

데이터 보안 인시던트 요약

데이터 보안 인시던트의 원인	지난 12개월 동안 가장 일반적인 인시던트	향후 12개월 이내에 예방할 준비가 가장 적음
맬웨어 또는 랜섬웨어	50%	41%
손상된 계정	38%	35%
DoS(서비스 거부) 공격	35%	33%
부주의한 내부자	32%	29%
의도하지 않은 내부자	31%	32%
악의적인 내부자	31%	35%
물리적 특성	29%	29%

조직이 선택하는 데이터 보안 솔루션은 고부가가치 비즈니스 데이터, 운영 데이터, 개인 데이터를 비롯한 다양한 민감한 데이터에도 적용되어야 합니다. 지난 12개월 동안 데이터 보안 인시던트가 발생하는 동안 조직 중 74%가 비즈니스 데이터가 노출되었고, 65%는 운영 데이터가 손상되었으며, 58%는 개인 데이터가 취약해지는 것을 경험했습니다. 다양한 유형의 데이터 중에서 지적 재산, IT 및 네트워크 설계, PII가 가장 자주 손상되거나 노출되었습니다.

앞을 내다보자면 조직의 77%는 지적 재산 및 소스 코드와 같은 비즈니스 데이터를 가장 취약한 것으로 인식합니다. 이는 주로 비즈니스 데이터가 경쟁 우위와 수익 창출을 확립하는 데 중요한 역할을 하기 때문입니다. 그러나 기존의 패턴 인식, 정규식 또는 함수 일치 기술이 특정 문자열 형식이나 키워드가 없는 콘텐츠를 효과적으로 식별하지 못할 수 있기 때문에 이러한 데이터를 식별하고 분류하는 것은 어려울 수 있습니다. 따라서 조직은 취약한 민감한 데이터를 검색하고 보호하는 데 도움이 되는 고급 기술이 필요합니다.

향후 12개월 동안 가장 위험한 데이터 유형

77% 비즈니스 데이터		64% 운영 데이터		63% 개인 데이터	
지적 재산	30%	IT 및 네트워크 디자인	29%	PII(개인 및 식별 가능한 정보)	31%
소스 코드	28%	재무제표	18%	인사정보(급여, 이력서 등)	21%
비즈니스 계획	27%	영업 및 수익 보고서	15%	PCI(Payment Card Industry) 데이터	18%
영업 비밀	24%	조달 및 송장	12%	PHI(의료 정보 보호)	18%
파일 통합 및 인수	20%	법률 문서/계약서	12%	개인 인증 정보	17%
건설 사양	18%	제조 공정/배치 파일	11%		

4

조직은 디지털 트랜스포메이션을 추진하기 위해 클라우드와 AI가 필요하지만, 이는 가장 취약한 데이터 위치이기도 합니다.

조직은 디지털 트랜스포메이션을 추진하기 위해 클라우드와 AI가 필요하지만, 이는 가장 취약한 데이터 위치이기도 합니다.

새로운 AI 기술과 결합된 클라우드 애플리케이션 및 플랫폼을 통한 협업은 직원 생산성을 크게 향상시키고 유연한 작업 배치를 지원하여 클라우드 애플리케이션과 AI 기술을 조직에 필수적으로 만듭니다. 평균적으로 조직은 현재 SaaS, PaaS, IaaS를 아우르는 147개의 퍼블릭 클라우드 서비스를 활용하고 있습니다.[1] 그리고 조직 중 66%가 AI 전략을 개발했으며 36%는 이미 AI 전략을 구현했습니다.[2] 그러나 이러한 진화로 인해 다양한 환경에서 데이터 경계를 명확하게 정의하기가 어렵기 때문에 보다 역동적이고 다면적인 위험이 발생했습니다.

1. Measuring Risk and Risk Governance, CSA(Cloud Security Alliance), 2022년
2. Microsoft data security AI research, Hypothesis, 2023년 3월

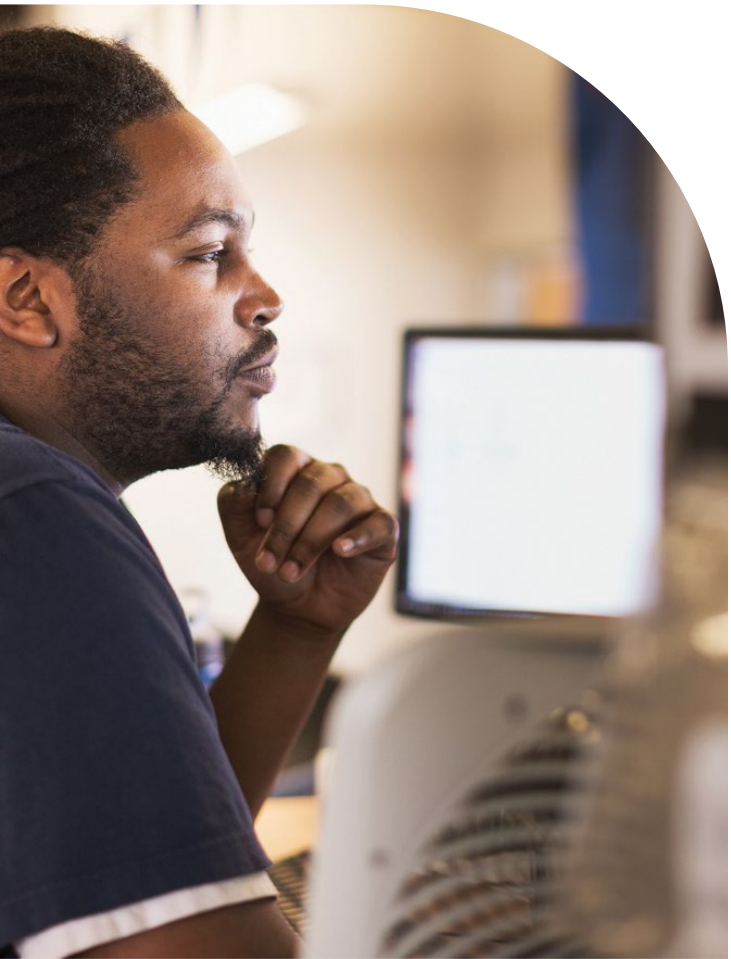
현재 생산성이 높은 데이터 위치에 적합한 데이터 보안 솔루션을 갖추는 것이 훨씬 더 중요해졌습니다. 지난 12개월 동안 조직 중 42%는 클라우드 스토리지에서, 31%는 이메일, 인스턴트 메시징 또는 온라인 미팅 도구에서 보안 인시던트를 경험했다고 보고했습니다. 인시던트는 생산성과 협업이 가장 많이 이루어지는 곳에서 가장 흔하게 발생하는 것처럼 보입니다.

이러한 유형의 인시던트를 관리하려면 리소스가 필요하며, 조직 중 79%는 데이터 보안 팀이 중요한 데이터 보안 책임을 효과적으로 관리하기 위해 더 많은 인력이 필요하다고 보고합니다. 그러나 더 많은 인력이 필요하다고 주장하는 조직 중 대다수(57%)는 동급 최고의 접근 방식을 선호합니다. 이는 더 많은 솔루션을 사용하는 조직이 무수한 사용자 활동 중에서 실제 위험을 식별하는 데 더 많은 어려움을 겪을 수 있음을 강조합니다.

데이터 위치 요약

데이터 위치	지난 12개월 동안 손상됨	대부분 위험함
클라우드 스토리지(예: Box, OneDrive, Google Drive)	42%	54%
이메일/인스턴트 메시징/온라인 미팅 도구	31%	39%
PaaS(Platform-as-a-Service)	29%	34%
IaaS(Infrastructure-as-a-Service)	28%	36%
AI(예: ChatGPT, Bard 등)	27%	38%
SaaS 기반 데이터베이스/데이터 레이크	27%	41%
엔드포인트/디바이스	25%	36%
온-프레미스 리포지토리/파일 공유/데이터베이스	24%	28%
섀도우 데이터	21%	23%
기간 업무 애플리케이션	17%	25%
개발자 도구	16%	23%

조직의 3분의 1 이상이 AI 전략을 구현하고 있으며 더 많은 조직이 AI 전략을 구현하려고 하고 있습니다. AI는 전례 없는 속도로 채택되고 있는데, 이는 과거의 클라우드 및 이메일 채택 때보다 훨씬 빠릅니다. 조직이 AI를 수용함에 따라 책임 있는 사용을 지원하고 위험을 방지하는 것이 중요해지고 있습니다. AI는 다른 위치에 비해 데이터 보안 인시던트가 가장 위험한 위치로 간주되며, 조직 중 27%가 AI 데이터 보안 침해를 경험했습니다. AI 사용을 통한 위험에 대해 조직은 AI와 공유되는 데이터에 대한 제어 부족, AI의 위험한 사용을 탐지하고 완화하기 위한 제어 부족, 생성형 AI 모델 학습 방법에 대한 투명성 부족, AI를 통한 기밀 정보 유출에 중점적으로 우려를 합니다.



"AI는 생산성과 효율성 면에서는 좋지만 잠재적인 보안 및 데이터 위험이 있습니다." 한 보안 의사 결정권자가 말합니다.

AI에 대한 우려 사항이 존재하지만, 특히 시장의 공급업체가 책임 있는 AI 사용을 통해 비즈니스를 강화하는 데 도움이 되는 혁신을 개발하고 있기 때문에 의사 결정권자는 잠재력을 볼 수 있습니다. 그러나 AI를 더욱 효율적으로 활용하기 위해 조직은 AI에서 악의적이거나 위험한 콘텐츠를 탐지하고, AI에 업로드하기 전에 데이터를 암호화, 마스킹 또는 익명화하며, AI에서 생성된 민감한 데이터를 식별하는 것이 가장 중요하다고 보고합니다.

AI에 필요한 상위 5가지 데이터 보안 제어

1. AI에서 **악의적이거나 위험한 콘텐츠 탐지**
2. AI에 업로드하기 전에 **데이터를 암호화, 마스킹 또는 익명화**
3. AI에서 생성한 **민감한 데이터 식별**
4. **민감한 데이터가** AI에 **업로드되지 않도록 방지**
5. AI에서 **모델 또는 데이터 조작 탐지**

5

자동화와 AI는 보호력을 강화할 수 있는 유망한 방법입니다.

자동화와 AI는 보호력을 강화할 수 있는 유망한 방법입니다.

조직의 우선순위나 예산에 따른 제약이 없는 이상적인 세상에서는 조직의 절반이 데이터 보안 관리에 보다 능동적으로 대처하고 민감한 데이터 및 관련 위험을 검색하고 데이터 보안 인시던트를 예방하는 데 더 많은 시간을 할애하기를 원합니다. 그러나 현재 조직의 절반 이상이 인시던트 감지, 대응, 조사와 같은 사후 대응적인 조치에 가장 많은 시간을 할애하고 있습니다. 또한 데이터 보안 인시던트에 대한 이러한 감지 및 대응은 시간이 많이 소요됩니다. 대부분의 조직에서는 데이터 보안 인시던트를 해결하는 데 약 한 달이 걸리며, 일부 조직의 경우 해결하는 데 최대 6개월이 소요될 수 있습니다.

보다 사전 예방적인 조직은 이미 비용이 적게 드는 데이터 보안 인시던트를 경험하고 있고, 한 달 이내에 이러한 인시던트를 조사할 가능성이 더 높으며, 방어 제어가 데이터 침해를 방지하는 데 충분하다고 믿을 가능성이 더 높기 때문에 보다 사전 예방적인 전략을 채택함으로써 누리는 이점은 분명합니다.

조직은 사전 예방적 데이터 보안 조치가 데이터 보안 위험을 줄이는 데 도움이 될 수 있다는 것을 알고 있지만, 이러한 조치를 구현하는 데 진전을 이루지 못하고 있습니다. 예를 들어, 예방에 더 많은 시간을 할당하여 보다 사전 예방적인 방법을 모색하는 사람들은 동급 최고의 솔루션을 선택할 가능성이 더 높으며, 이는 실제로 탐지 신호와 대응 제어를 함께 가져올 때 사후 대응적인 조치를 처리하는 데 더 많은 노력을 요구합니다.

더욱 사전 예방적인 조직과 사후 대응적인 조직 비교 결과

	더욱 사전 예방적	더욱 사후 대응적
지난 12개월 동안 데이터 보안 인시던트의 평균 비용 영향	$207,000	$330,000
평균적으로 한 달 이내에 데이터 보안 조사 완료	80%	68%
우리의 방어 통제는 데이터 유출을 방지하기에 충분	77%	68%

리소스 및 직원이 제한되어 있고 활동 간 노력 할당이 이상적이지 않을 수 있기 때문에 조직은 사전 예방적 활동에 더 많은 시간을 할애할 수 있는 기술을 찾고 있습니다. 자동화는 조직이 데이터 보안에 대한 보다 사전 예방적인 접근 방식을 위해 시간을 할애할 수 있는 한 가지 방법입니다. 설문 조사에 참여한 조직 중 74%는 보안 팀이 수동 검토보다 잠재적인 데이터 보안 인시던트의 영향을 미리 최소화할 수 있는 반자동 또는 완전 자동화된 위험 완화를 선호합니다. 또한 조직은 데이터 보안 보고서 작성, 인시던트 관리 워크플로 자동화, 인시던트 대응 및 조사와 같이 자동화의 이점을 얻을 수 있는 다른 많은 작업에 대해 알고 있습니다. 보안 팀이 자동화하고자 하는 대부분의 주요 작업은 사후 대응적 조치입니다. 이러한 작업을 자동화함으로써 조직은 데이터 보안 팀의 부담을 완화하여 보다 사전 예방적인 자세를 취할 수 있습니다.

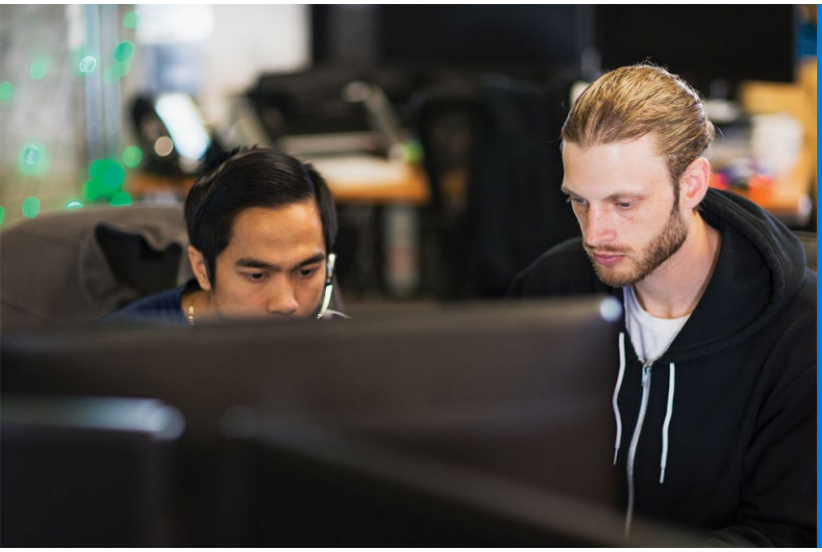
데이터 보안 팀이 자동화/완화하는 것을 선호하는 상위 5개 영역

사후 대응적

1. 인시던트 관리 및 대응을 위한 자동화된 워크플로 생성
2. 데이터 보안 보고서 작성

사후 대응적

3. 데이터 보안 인시던트에 대한 대응 및 억제
4. 조사 중 적절한 팀(예: SOC, 법무, HR)으로 인시던트 라우팅
5. 데이터 보안 인시던트 조사



"수동으로 평가해야 할 위험한 데이터가 너무 많습니다. AI는 팀의 응답 시간을 단축하고 리소스가 부족한 상황에서 데이터를 보호하는 데 도움이 될 수 있습니다."

영국 보안 의사 결정자

데이터 보안에 AI를 사용하면 조직이 미래의 위협에 대해 보다 전략적이고 현명해질 수 있습니다. 이 기술은 감지된 인시던트에 대한 대응 속도를 높여 데이터 보안 전문가가 추가 조사를 할 시간을 벌어줍니다. 자동화와 마찬가지로 조직은 AI가 더 강력한 보안을 제공하여 도움이 될 수 있는 많은 시나리오를 참고함으로써 **팀의 시간을 절약합니다.** AI 사용에 대한 주요 시나리오로는 부적절한 데이터 공유를 자동으로 차단, 중요한 데이터 보안 위험/비정상적인 데이터 활동 감지, 잠재적인 데이터 보안 인시던트 조사 등이 있습니다.

AI 및 자동화의 이점을 활용하고 보다 통합된 솔루션으로 전환함으로써 조직은 보다 사전 예방적인 데이터 보안 전략을 수용하고 보다 안전한 미래를 준비할 수 있습니다.

AI가 사용되는 주요 시나리오

부적절한 데이터 공유 **자동으로 차단**

중요한 데이터 보안 위험/비정상적인 데이터 활동 **감지**

데이터 환경을 더 안전하게 보호하는 **권장 사항**

잠재적인 보안 인시던트 **조사**

데이터 보안 정책 **미세 조정**

최종 권장 사항

- 데이터 보안 태세를 강화하기 위한 통합형 플랫폼 채택
- 심층 방어 접근 방식을 통해 내외부 모두에서 데이터 보안 인시던트로부터 보호
- AI 및 자동화를 통한 데이터 보안 전략 업그레이드

데이터 보안 태세를 강화하기 위한 통합형 플랫폼 채택

이 연구 결과에 따르면 솔루션의 적을수록 보안은 더 강화될 수 있습니다. 직관적이지 않은 것처럼 보일 수 있지만, 조직은 사일로화된 다양한 솔루션으로 인한 잘못된 자신감과 싸워야 합니다. 공급업체를 통합하면 비용을 절감할 뿐만 아니라, 보안을 강화하는 전략적 접근 방식을 제공합니다.

데이터 보안 의사 결정권자는 팀이 새로운 보안 제어를 위한 연구, 계획, 보안 정책 최적화와 같은 전략적 작업에 더 많은 시간을 할애할 수 있도록 지원함으로써 이러한 혁신을 시작할 수 있으며, 의사 결정권자 중 84%가 이를 수행하기를 원한다고 동의합니다. 이러한 프로세스에는 종종 '동급 최고'로 간주되는 다양한 도구와 효과적으로 통합되지 않는 레거시 사일로 솔루션을 교체하는 작업이 포함됩니다.

의사 결정권자는 팀과의 긴밀한 협업을 촉진하여 데이터 보안 프로그램 목표와 KPI(핵심 성과 지표)를 설정할 수 있습니다. 그런 다음 솔루션 요구 사항을 정의하고 협상할 수 없는 기능을 식별하여 진행할 수 있습니다. 이러한 접근 방식을 통해 가장 중요한 목표에 부합하는 도구를 제공할 수 있는 공급업체를 정확히 찾아낼 수 있습니다. 결정적으로, 미래 지향적인 인시던트 방식을 장려하고 팀이 기존 관행이나 고립된 사용 사례에 지나치게 집착하지 않도록 하여 보다 통합된 접근 방식을 위해 필요한 변경 사항을 구현할 수 있도록 합니다.

통합형 데이터 보안 플랫폼은 보안 팀이 다음과 같은 모든 중요한 작업을 원활하게 수행할 수 있도록 지원해야 합니다.

1. 디지털 환경에서 민감한 데이터를 검색하고 보호합니다.
2. 이 데이터와 관련된 중요한 위험을 감지합니다.
3. 합법적인 비즈니스 활동에 영향을 주지 않으면서 중요한 데이터의 무단 사용을 방지합니다.

통합형 데이터 보안 전략을 구현함으로써 조직은 더 높은 수준의 보호를 달성하는 동시에 보안 인프라를 단순화할 수 있습니다.

심층 방어 접근 방식을 통해 내외부 모두에서 데이터 보안 인시던트로부터 보호

데이터 보안 인시던트는 일반적으로 외부 공격자, 악의적인 내부자 또는 의도하지 않은 내부자에 의해 발생합니다. 조직은 외부 위협의 무단 액세스를 방지하고 내부자 도난 또는 우발적인 데이터 노출의 위험을 완화하여 데이터를 보호하기 위한 조치를 취해야 합니다.

이러한 문제를 해결하기 위해 조직은 데이터 보안에 대한 심층 방어 접근 방식을 채택할 수 있습니다. 이러한 전략은 박물관이 귀중한 예술품을 보호하는 것과 유사합니다. 위협 인텔리전스가 장착된 최첨단 보안 카메라는 방문객을 모니터링하고, 티켓팅 시스템은 신원 및 박물관 액세스를 관리하며, 예술 작품에 대한 엄격한 보안 조치는 귀중한 데이터를 보호하는 데이터 보안 제어와 유사하게 작동합니다. 이러한 조치는 외부의 악의적인 행위자로부터 발생하든 이미 조직 환경 내에 있는 개인에서 발생하든 잠재적인 인시던트를 방지합니다.

진화하는 데이터 보안 위험에 대처하려면 이와 같은 심층 방어 전략을 구현하기 위해 조직 전체에서 공동의 노력이 필요합니다. 데이터 보안 팀은 SOC(보안 운영 센터)와 같은 다른 부서와 협업하여 데이터 보안 투자를 최적화할 수 있습니다. 특히, 스스로를 능동적이라고 생각하는 조직 중 66%가 SOC 팀과 상호 작용하는 반면, 그렇지 않은 조직은 54%입니다.

보안 팀 간의 팀워크와 마찬가지로 데이터 보안 솔루션도 XDR(확장된 감지 및 대응) 또는 IAM(ID 및 액세스 관리) 솔루션과 같은 다른 시스템과 원활하게 통합되어 외부 및 내부 소스의 데이터 보안 인시던트를 효과적으로 방지해야 합니다. 이러한 통합을 통해 조직은 보안 인시던트에 대한 포괄적인 조사 및 대응을 수행하고, 영향을 받는 데이터, 행위자, 활동을 철저히 이해하며, 다양한 제어로 대응할 수 있습니다. 결과적으로 이를 통해 정보에 입각한 정확하고 신속한 대응을 통해 잠재적인 보안 인시던트의 영향을 최소화할 수 있습니다.

AI 및 자동화를 통한 데이터 보안 전략 업그레이드

자동화 및 AI는 조직이 데이터 보안에 보다 능동적으로 대처하는 데 도움이 될 수 있습니다. 다음은 조직이 자동화 및 AI 여정을 시작하기 위한 몇 가지 권장 사항입니다.

- 민감한 데이터 검색: AI를 활용하여 민감한 데이터를 식별하고 암호화 및 권한 관리를 포함한 보호 정책을 적용할 수 있습니다. 이는 기존 패턴 인식 기술을 통해 감지하는 데 어려움을 겪을 수 있는 비즈니스 데이터에 특히 유용합니다. 조직은 데이터 컨텍스트 또는 비즈니스 범주에 따라 민감한 콘텐츠를 신속하게 찾을 수 있는 인텔리전스 및 기능으로 알려진 머신 러닝 또는 AI 기반 분류자와 같은 분류 기술을 활용할 수 있습니다. 또는 조직은 정확한 데이터 매칭 기술을 사용하여 운영 또는 개인 데이터를 검색할 수 있습니다.

  또한 산업 규정(예: GDPR, HIPAA 또는 PCI DSS)이 진화하고 데이터 환경이 더욱 역동적으로 변함에 따라 새로운 범주의 민감한 데이터를 식별하기 위해 사용자 맞춤화 및 쉽게 적용 가능한 고급 분류 기술을 보유하는 것이 중요합니다.

- 중요한 데이터 보안 위험 감지: AI의 힘을 활용하여 민감한 데이터와 관련된 중요한 위험을 정확히 찾아내고 리소스를 전략적으로 할당하여 위험이 높은 잠재적인 인시던트를 해결합니다. AI 기술은 충실도가 높은 경고를 생성할 수 있기 때문에 보안 팀은 수많은 오탐 경고를 선별하는 데 소요되는 귀중한 시간을 절약할 수 있습니다. 또한 AI는 특히 악의적인 행위자가 탐지를 회피하려고 할 때 조직이 파악하기 어려운 위험을 식별하는 데 도움이 될 수 있습니다. 이러한 위협 행위자를 능가하려면 컴퓨터 속도를 활용하는 것이 필수적입니다.

- 데이터 보안 인시던트를 동적으로 방지: AI 및 자동화를 사용하여 평가된 위험에 따라 자동으로 예방 및 완화 제어를 조정하여 보다 적응력 있고 사전 예방적인 데이터 보안 전략을 지원합니다. AI 기반 솔루션이 위험을 감지하고 평가하면 자동화된 예방 제어가 신속하게 작동하여 데이터를 보호하고 고위험 영역에 완화 제어를 정확하게 적용할 수 있습니다. 예를 들어, 고위험 사용자가 데이터 반출 의도의 초기 지표를 감지하는 경우 조직은 보다 엄격한 DLP(데이터 손실 방지) 정책을 적용하여 잠재적인 데이터 보안 인시던트에 미리 대비할 수 있습니다.

이 보고서의 인사이트와 권장 사항이 데이터 보안 태세를 강화하고 진화하는 위험으로부터 조직을 강화하는 데 도움이 되기를 바랍니다.

Microsoft 데이터 보안에 대해 자세히 알아보시려면 https://aka.ms/DataSecurityNews에서 확인해 보세요.

자세한 연구 목표, 방법론, 참가자 모집

연구 목표는 다음과 같습니다.

1. 우선순위, 사고 방식, 과제를 포함한 데이터 보안 환경 이해
2. 데이터 보안 인시던트의 원인과 결과를 매핑하고 데이터 보안 팀이 데이터 보안 태세를 강화하기 위해 취할 수 있는 조치 식별
3. 데이터 보안을 위한 AI 사용과 관련된 새로운 전략과 혁신을 포함하여 데이터 보안의 미래 확인

방법론:

2023년 7월 28일부터 8월 9일까지 822명의 데이터 보안 의사 결정권자를 대상으로 15분 동안 다국적 온라인 설문조사가 실시되었습니다.

질문은 데이터 보안 환경, 데이터 보안 팀이 리소스를 할당하는 방법, 데이터 보안 인시던트, 데이터 보안을 위한 AI(인공 지능)에 대한 태도 및 사용에 중점을 두었습니다.

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

데이터 보안에 대한 권한이 있는 CISO 및 인접 의사 결정권자(C-2 이상)

엔터프라이즈급 조직에서 근무(500명 이상의 직원, 다양한 규모)

규제 산업과 비규제 산업의 혼합(교육, 정부 또는 비영리 안됨)

연구를 위해 설문 조사에 참여한 822명의 데이터 보안 의사 결정권자 국가는 다음과 같습니다.

미국	329
영국	322
호주	171