

사이버 위협에 대한 선제적 대응

성숙한 아이덴티티 보안을 통한
복원력 강화

아이덴티티의 수와 유형이 확대됨에 따라
보안 취약점이 늘어나고, 규정 준수에 대한
압박도 증가하고 있으며 사이버 보안 보험료도
인상되고 있습니다.

↑ **30+%**

향후 3-5년간
머신 아이덴티티의
예상 증가율

↑ **14%**

향후 3-5년간
디지털 아이덴티티의
예상 증가율

↑ **77%**

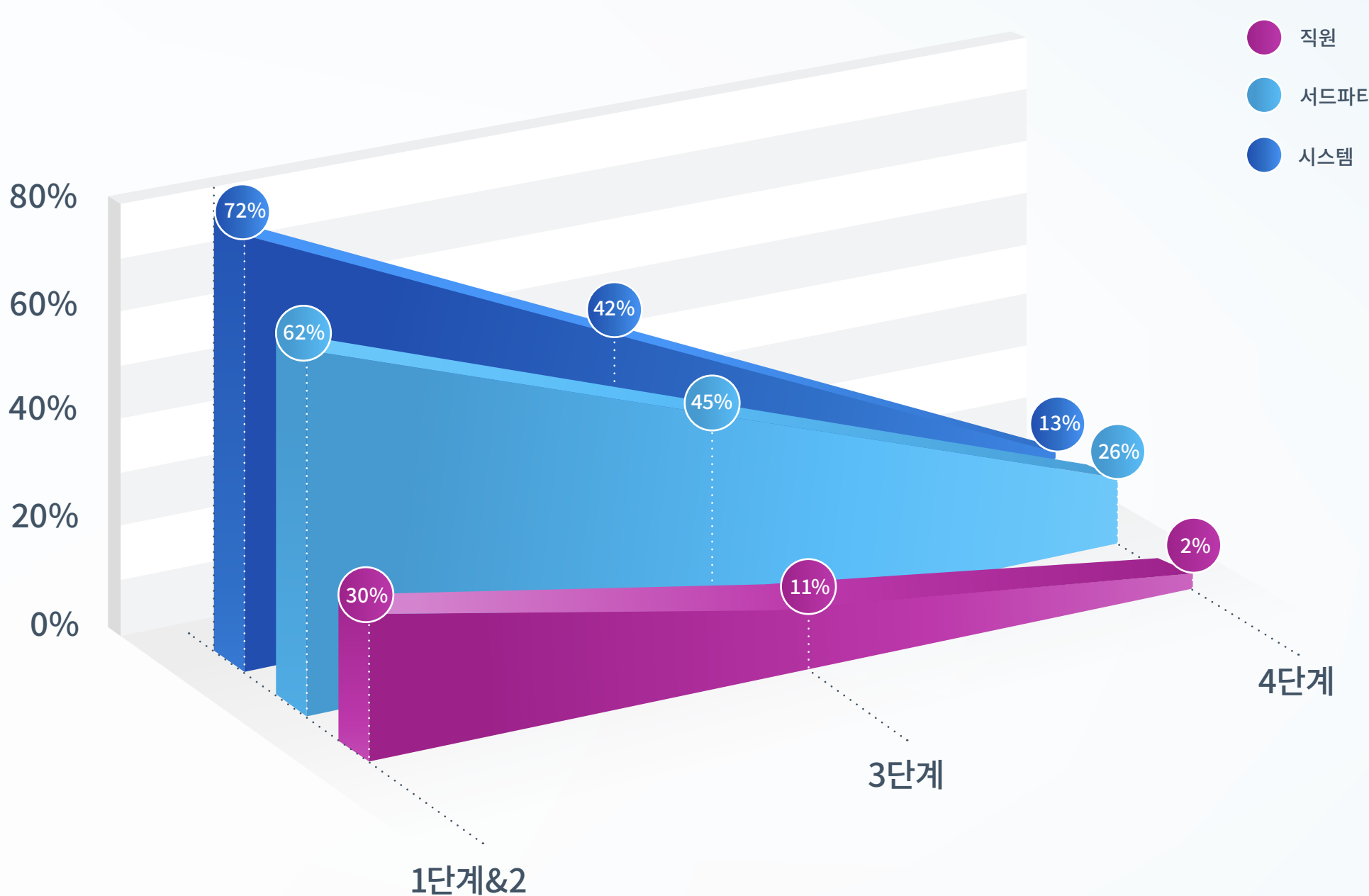
지난 3년간
사이버 보안 보험료
증가율

↑ **7배**

2010년 이후
아이덴티티 관련 규제 증가

최근 실시한 설문에서 약 350명의 IAM 및 보안 의사 결정권자는
미흡한 액세스 관리 체계가 2024년에도 중대한 문제로
남을 것이라고 답했습니다.

아이덴티티 유형별 관리되지 않는 액세스



1단계&2
수동: 기본적인 아이덴티티
프로세스를 수동으로 관리하여
많은 경우 비효율성과
보안 맹점이 발생

3단계
디지털화: 계정 프로비저닝을
자동화하여 정확성을 높이고
수동 워크로드 절감

4단계
고급 도구 및 예측적 사용 사례:
지능형 의사 결정 및 선제적
아이덴티티 관리를 위한
AI 기반 솔루션 구현

머신 아이덴티티는 휴먼 아이덴티티에 비해
최대 10배의 보안 위험을 초래하고 있습니다

보안 위험 및 규정 준수 위반을 방지하기 위해서는
머신에 대한 특별 관리가 필요합니다.

66%

머신 아이덴티티 관리에서
수작업이 더 많이 필요하다고 답한
기업의 비율*

60%

머신 아이덴티티와 관련된
감사 문제를 경험했다고
응답한 기업의 비율*

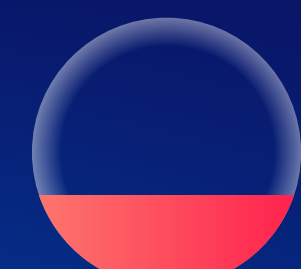
72%

의도적으로 휴먼 상태의
머신 아이덴티티를 유지하고 있다고
답한 기업의 비율*

*머신 아이덴티티의 위기: 수동 프로세스의 문제점과 숨겨진 위험

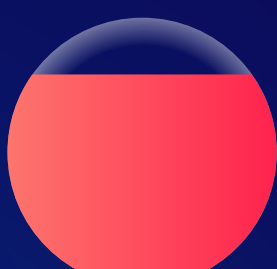
모든 아이덴티티와 액세스를 관리하세요.
성과는 확실합니다.

IAM에 전략적으로 투자하는 조직은 아이덴티티 관련 보안 문제 및
인시던트의 파급을 억제하고 전반적인 사이버 복원력을 높입니다.



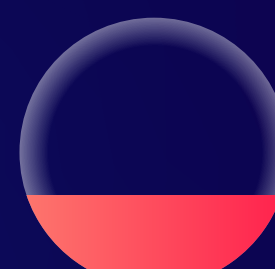
~40%

4단계 이상 조직의 SI를 통한
사이버 공격 탐지 및
대응 속도 향상률



83%

2023년에 아이덴티티 보안에
투자하여 아이덴티티 관련
보안 문제의 발생 빈도가
줄어든 조직의 비율



40%

사이버 위험 관리 개선에
따른 사이버 보안
보험사들의 손실 절감률

수치로 보는 위험 감소 성공 사례

3배

약 6,000개 계정에 대해 적절한 권한을 설정하여
감소된 사이버 보안 위험

12k

아이덴티티 보안을 제공받은
비직원의 수

144k

계정 수정 및 검증을 자동화하여 감소하게 된
잠재적 보안 위험

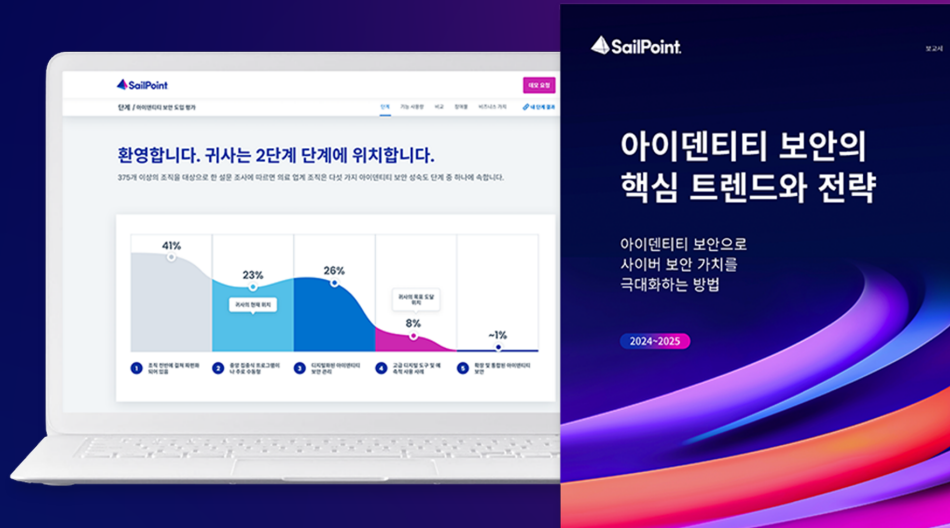
>\$3M+

탄탄한 아이덴티티 보안에 힘입어
랜섬웨어 공격을 예방해 절감한 비용

조직의 현황을 점검하고
사이버 복원력을 높이세요.

아이덴티티 보안의 다섯 가지 단계가 어떤 체계와 평가 기준으로
구성되는지 확인하세요. 성숙한 조직이 어떻게 보안을 강화하고,
운영을 간소화하고, 규정 준수 요건을 충족하는지 살펴보세요.

결과 확인하기



이 문서의 모든 데이터 포인트는 별도로 명시되지 않은 한 아이덴티티 보안의 다섯 가지 단계 보고서에서 가져온 것입니다.