CLOUDFLARE

비즈니스 영향

Zero Trust로 위험을 줄이고 기술 효율성을 개선하는 방법

적은 오버헤드로 – 더 강력한 보호

Zero Trust 우수 관행의 경제적 영향 및 보안 영향 수치화

사이버 위험 감소

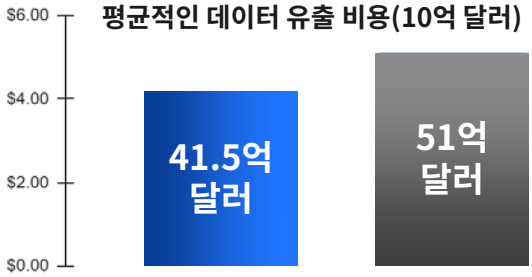
95% 기본 제공 Zero Trust 원칙이 포함된 SASE 아키텍처로 공격 표면이 감소된 비율 [1]

72% 가장 우선적으로 "데이터 보안을 강화하기 위해" Zero Trust를 도입했다고 대답한 IT 리더의 비율 [2]

61% "ID와 위험 상태를 사용한 더 강력한 인증"을 이점으로 꼽은 IT/보안 전문가 비율 [3]

↓ 23% Zero Trust가 배포되지 않았을 때와 비교하여, 배포되었을 때 평균적인 데이터 유출 비용 절감 비율 [4]

평균적인 데이터 유출 비용(10억 달러)



추진 요인

- 모든 요청에 ID 및 컨텍스트 기반 제어를 사용해 과도한 신뢰를 줄임
- 모든 사용자, 애플리케이션, 디바이스의 가시성 개선으로 더욱 신속한 조치
- 위협의 내부망 이동 감소

기술 효율성 개선

700만 달러 Zero Trust를 도입한 5개 조직에서 레거시 보안 비용보다 절감한 평균 금액 [5]

20달러 /FTE 중복되는 보안 서비스를 클라우드 기반 Zero Trust 플랫폼으로 교체할 때 매월 절약되는 비용 [5]

↓ 80% 새로운 인프라를 조달하고 확보하기 위한 노력 절감 [5]

39% 조직에서 사용하는 보안 기술 중, 구식 기술이며 Zero Trust로 현대화할 수 있는 기술의 비율 [6]

사이버 보안 복잡성과 관련된 가장 중요한 결과 [7]

#1 데이터 유출이나 사이버 공격이 성공하여 초래되는 경제적 손해

#2 시장 기회만큼 빠르게 혁신할 수 없음

#3 업무 복원력 부족

추진 요인

- 레거시 포인트 솔루션을 하나의 클라우드 플랫폼에 통합하여 복잡성 감소
- 온프레미스 장비를 통한 백홀링 트래픽이 없어 보안 워크플로 간소화
- 하이브리드 인력 전체에 일관적인 정책

+82 70 4515 6893 | enterprise@cloudflare.com | www.cloudflare.com

REV:PMM-2022NOV

Zero Trust로 조직의 전략적 사고방식이 변화합니다

레거시 IT 보안: 경계가 신뢰를 결정합니다		Zero Trust: 경계 없음, 언제나 확인
보안 경계, 안전한 네트워크 내부 (즉, “성과 해자”)	보호	위험 가정, 영향 감소(암호화, 검사, 마이크로세분화)
경계에서의 로그인만을 기록	가시성	모든 곳에서의 모든 로그인과 요청을 기록
기본 허용 방식, 네트워크 위치에 기반한 정적 액세스	제어	기본 거부 방식, ID 및 컨텍스트에 기반한 최소 권한 액세스

Zero Trust로 사이버 위험을 줄이세요

자문 요청

아직 상담할 준비가 안 되셨나요?

- Zero Trust가 팀 생산성을 개선하는 방법 알아보기: 요약 읽기
- 다른 조직에서 하이브리드 업무를 어떻게 처리하는지 자세히 알아보세요. 요약 읽기
- Zero Trust를 달성하며 벤더에 구애받지 않는 로드맵을 살펴보세요: 백서 읽기

1. Cloudflare 고객 경험 기반
2. “Capterra’s 2022 Zero Trust Survey,” 2022년 8월 (Link)
3. “Global Study on Zero Trust Security for the Cloud,” Ponemon Institute LLC, 2022년 7월 (Link)
4. “데이터 침해 비용 보고서,” IBM, 2022 (Link)
5. “The Total Economic Impact ™ of Zero Trust Solutions from Microsoft,” Forrester Research, 2021년 12월 (Link)
6. “Security Outcomes Study,” Cisco, 2021년 12월 (Link)
7. “2022 Global Digital Trust Insights,” PWC, 2022년 9월 (Link)