

데이터를 보호하세요

랜섬웨어가 백업을
표적으로 삼고 있습니다.

귀사의 백업이 취약할 수도 있습니다.

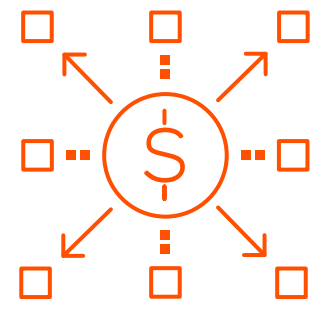
랜섬웨어 공격으로 인한 피해는 2024년까지 두 배 이상 증가해
4,200만 달러(한화 약 545억 원)에 이를 전망입니다.*

규모에 상관없이 어떤 조직, 정부 또는 기업도 랜섬웨어 공격으로부터 안전하지 않습니다.

또한 기존 데이터 복구 솔루션은 필요한 보호를 제공하지 못할 수 있습니다.

이제 사이버 범죄자들은 효과적인 복구 솔루션을 보유한 기업은
대가를 지불하지 않는다는 사실을 깨닫고 데이터 백업을 표적으로 삼고 있습니다.

상황 분석



공격을 받으면 피해가 발생합니다.

랜섬웨어 공격은 비용이 많이 들고, 법적 소송을
야기할 수 있으며, 평판을 손상시킵니다.



랜섬웨어는 단순한 ‘암호화’가 아닙니다.

공격자는 단순히 데이터를 사용할 수 없도록 만들뿐 아니라
다른 기회를 찾기 위해 네트워크를 탐색합니다.



침투에 성공하면 많은 문제가 생길 수 있습니다.

해커는 원하는 것은 무엇이든 삭제할 수 있으며
심지어 ‘변경 불가’로 간주되는 복사본까지 삭제할 수 있습니다.



백업을 보험으로 생각하면 안 됩니다.

백업이 손상되면, 데이터 복구가 지연되고
복구 비용이 증가할 수 있습니다.

해결책



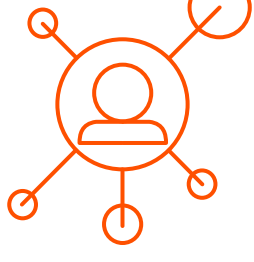
세이프모드(SafeMode)가 해결책이 될 수 있습니다.

퓨어스토리지의 플래시어레이(FlashArray™)와
플래시블레이드(FlashBlade®) 시스템은
세이프모드 기능으로 백업 데이터를 보호할 수 있도록 지원합니다.



데이터에 대한 완벽한 보호를 제공합니다.

관리자의 크리덴셜이 손상된 경우에도
백업을 삭제, 수정 또는 암호화할 수 없습니다.



퓨어스토리지가 상시 대기하고 있습니다.

공격 발생 시, 퓨어스토리지 지원 팀과 협력하여
세이프모드로 보호되는 데이터에 액세스할 수 있습니다.



완전하게 보호됩니다.

세이프모드는 백업 데이터 세트는 물론
백업 메타데이터까지 보호합니다.



평소 사용하던 툴을 활용할 수 있습니다.

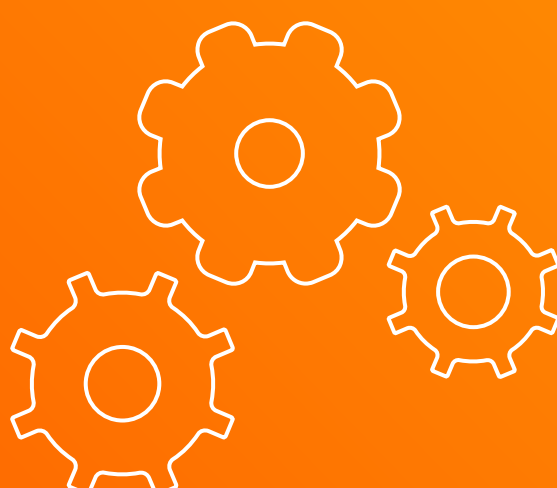
세이프모드는 기존 백업 소프트웨어 또는
데이터베이스 툴과 함께 작동합니다.



투자를 보호할 수 있습니다.

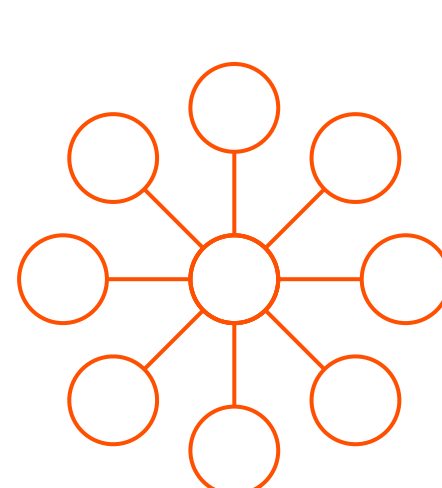
퓨어스토리지의 세이프모드는
플래시블레이드와 플래시어레이에 내장되어 있기 때문에 추가 비용이 들지 않습니다.

혜택



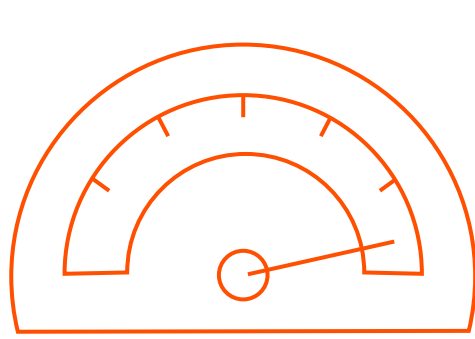
적절한 유형의 보호를 제공합니다.

세이프모드를 사용하면 데이터 복구가
스마트하고 빠르고 쉽습니다.



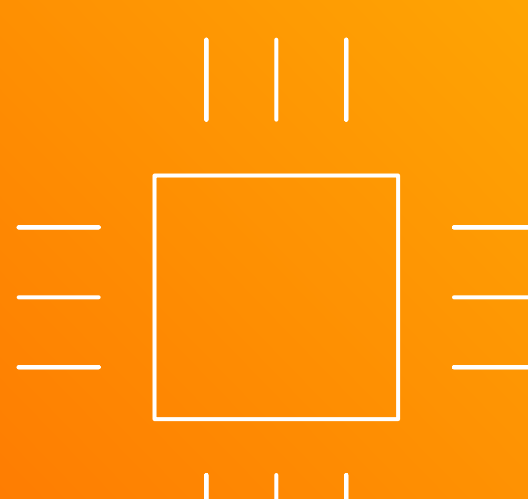
세이프모드는 간단합니다.

설정만 해두고 잊어버리시면 됩니다.
스냅샷 생성과 만료가 자동으로 진행됩니다.



세이프모드는 빠릅니다.

울 플래시 스토리지의
초고속 대용량 복구를 경험할 수 있습니다.



세이프모드는 미래에 대비할 수 있습니다.

향후 모든 기능과 개선 사항이
추가 비용 없이 영구적으로 제공됩니다.

세이프모드로 보안을 유지하세요.

데이터 백업을 안전하게 유지하고
랜섬웨어 공격을 차단할 수 있습니다.

[자세히 보기](#)