솔루션 브리프

퓨어스토리지 플래시어레이(FlashArray)의 랜섬웨어 방어

플래시어레이(FlashArray™) 세이프모드(SafeMode™)로 악의적인 공격으로부터 더 빠르게 복구하십시오.

랜섬웨어 공격은 거의 매일 뉴스에 보도됩니다. 이러한 공격은 전 세계 산업에 영향을 미치고 있습니다. 비즈니스에 대한 랜섬웨어 위협은 놀라운 속도로 증가하고 있으며, 그 비용은 2025년까지 전 세계적으로 10조 5천억 달러에 달할 것으로 예상됩니다.[1] 비즈니스가 입는 잠재적인 피해는 운영 중단과 재정적 비용 그 이상으로 확장됩니다. 비즈니스가 공격을 받으면 기사에 나오지 않더라도 평판이 위험에 처합니다.

세이프모드(SafeMode) 스냅샷이 포함된 퓨어스토리지의 플래시어레이(FlashArray)를 사용하면, 사이버 공격으로부터 복구하는 데 필요한 중요 데이터를 보호하고, 공격자의 요구에 굴복하지 않고 비즈니스 서비스를 신속하게 재개할 수 있습니다.

최신 데이터 보호에 대한 퓨어스토리지의 접근 방식은 단순한 보험 정책이 아닙니다. 이는 현대적인 데이터센터의 중요한 구성 요소입니다. 퓨어스토리지의 솔루션은 여러 플랫폼과 기술을 포괄하고, 매우 빠른 복구 역량으로 중요한 데이터와 애플리케이션을 효율적으로 보호하며, 보호된 데이터에서 실질적인 비즈니스 가치를 이끌어낼 수 있도록 합니다. 기본적인 워크로드 가용성을 스냅샷으로 확장하고, 백업 복사본을 클라우드의 장기 아카이브로 확장하는 보호 기술의 연속체라고 할 수 있습니다.

비즈니스 보호를 위한 복구 데이터 보호

공격자의 타깃이 점점 더 정교해지고 있는 상황에서 랜섬웨어로부터 비즈니스를 보호하려면 해커를 능가할 수 있는 신중한 계획이 필요합니다. 랜섬웨어 공격자는 일반적으로 공격이 시작되기 몇 주 전에 취약점을 찾으러 시스템에 침입합니다. 그런 다음 자신의 키로 운영 데이터를 암호화하여 공격을 개시하고 키에 대한 대가를 요구합니다. 동시에 시스템을 공격 전의 암호화되지 않은 상태로 복구하는 데 사용할 수 있는 모든 스냅샷이나 백업 데이터를 암호화하거나 파괴합니다. 세이프모드를 사용하면 이러한 공격으로부터 복구하는 데 필요한 중요한 스냅샷과 백업 데이터를 두 가지 방식으로 보호할 수 있습니다. 첫째, 세이프모드는 상시 가동되는 불변성 역량을 통해 복구 데이터가 손상되거나 암호화되는 것을 방지합니다.

엔터프라이즈 데이터 위협

사이버 범죄자들은 랜섬웨어 공격의 73%에서 데이터 암호화에 성공했습니다.[2]

금융 노출

IT 서비스 제공업체 Cognizant는 랜섬웨어 공격 후 5~7천만 달러의 손실이 야기될 것으로 예상합니다.[3]

생산성 손실

랜섬웨어 공격으로 학생 수가 115,000명에 달하는 볼티모어 카운티 공립학교들이 폐쇄하는 사태가 발생했습니다.[4]

둘째, 세이프모드는 시간 기반의 삭제 정책을 통해 관리자 권한이 있는 사람이라도 복구 데이터를 완전히 삭제할 수 없도록 합니다.

변경 불가능하고 효율적인 스냅샷으로 복구 속도 향상

퓨어스토리지의 플래시어레이는 빠른 복구를 제공하는 스냅샷을 포함해 포괄적인 비즈니스 연속성 및 재해 복구 옵션을 제공합니다. 스냅샷은 특정 시점에서의 데이터에 대한 이미지 수준 뷰로 데이터 보호와 재해 복구를 위한 참조 지점 역할을 합니다. 즉각적인 복구를 위해 데이터베이스 볼륨과 같은 볼륨 이미지의 스냅샷을 만들 수 있습니다. 또는 백업 데이터와 관련 메타데이터 카탈로그의 스냅샷을 만들어 데이터 보호 수준을 높일 수도 있습니다. 모든 스냅샷은 관리자 크리덴셜이 침해되더라도 랜섬웨어 공격자가 손상, 변경 또는 영향을 미칠 수 없는 변경할 수 없는 데이터 복사본입니다.

퓨어스토리지 스냅샷은 모든 플래시어레이 장치에서 무료로 사용할 수 있으며 간단하게 설정할 수 있습니다. 퓨어스토리지 스냅샷의 특징은 다음과 같습니다.

- **변경 불가**: 스냅샷이 생성되면, 관리자 액세스 권한이 있는 사람을 포함해 그 누구도 이를 수정하거나 암호화할 수 없습니다.
- **효율성**: 이전 스냅샷 저장 이후 변경된 블록만 저장되므로 데이터 복제가 불필요해 스토리지 비용이 절감되고 스냅샷 생성 시간이 단축됩니다.
- **완전한 기능**: 스냅샷은 새로운 볼륨입니다. 원본과 동일한 성능으로 다시 마운트, 읽기, 쓰기 또는 스냅샷이 가능합니다.
- **유연성**: 스냅샷에서 볼륨을 복구하고 즉시 롤 포워드 또는 백워드하여 비즈니스 서비스를 복원할 수 있습니다.
- **자동화**: 운영에 대한 확신과 유연성을 제공하는 포괄적인 보호 정책을 통해 스냅샷 생성을 자동화할 수 있습니다.

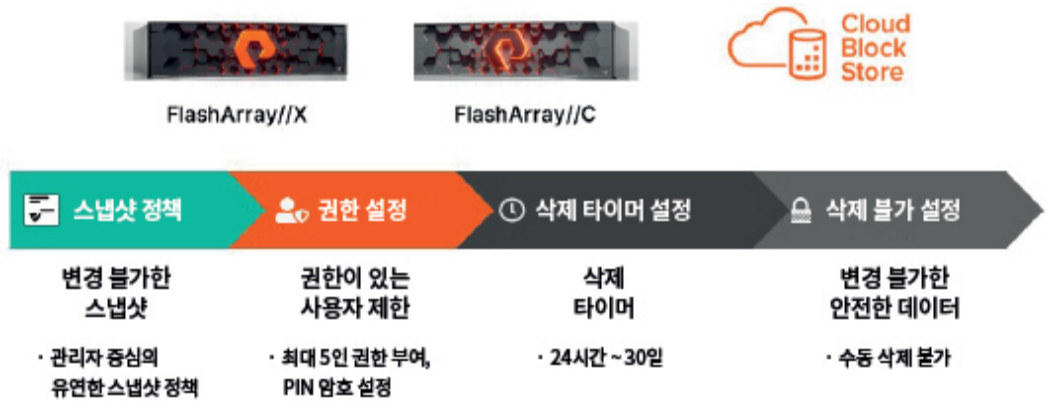

그림 1. 세이프모드는 사이버 공격이 발생하는 동안 암호화와 제거로부터 플래시어레이 스냅샷을 보호합니다.

공격자가 데이터를 제거하지 못하도록 해 스냅샷 보호

공격자는 퓨어스토리지의 세이프모드 스냅샷을 암호화하거나 손상시킬 수 없지만 암호화한 데이터를 복구하지 못하도록 시스템에서 삭제(완전히 파괴)하려는 시도를 할 수 있습니다. 이를 방지하기 위해 플래시어레이는 데이터가 완전히 파괴되지 않도록 정해진 기간 동안 데이터를 잠그는 삭제 타이머를 제공합니다. 삭제 타이머는 관리자 권한을 가진 사람을 포함해 누구도 데이터를 삭제할 수 없도록 만듭니다.

삭제 타이머는 기본적으로 24시간으로 설정되어 있습니다. 그러나 세이프모드를 활성화하면 최대 30일까지 늘릴 수 있습니다. 사용자가 설정할 수 있는 이 타이머는 로컬이든 원격이든 관계없이 플래시어레이에 안전하게 저장된 변경 불가능한 스냅샷을 사용하여 시스템을 롤백할 수 있는 충분한 시간을 제공합니다.

금전적 대가를 지불하지 않고 신속하게 복구

랜섬웨어 공격을 식별하고 무단 침입으로부터 시스템을 보호하며 즉시 복구 절차를 시작할 수 있습니다. 먼저, 세이프모드 보안 스냅샷이 있다는 것을 알고 있다면, 공격자가 암호화하거나 다른 방식으로 손상한 모든 데이터를 삭제할 수 있습니다. 그런 다음 세이프모드 보안 스냅샷으로부터 볼륨을 즉시 복구할 수 있습니다. 대가를 지불할 필요 없이 조직의 평판이 손상되지 않은 상태에서 시스템은 중단되었던 위치로 바로 돌아갈 수 있습니다.

참고 자료

- 플래시어레이(FlashArray) 데이터 보안 및 규정 준수에 대해 보다 자세히 알아보세요.
- 플래시블레이드(FlashBlade)의 랜섬웨어 보호에 대해 자세히 알아보세요.

---

1 사이버 범죄로 인해 2025년까지 전 세계적으로 연간 105억 달러 손실, Cybersecurity Ventures, 2020년 11월

2 2020년 랜섬웨어 현황, Sophos, 2020년 5월

3 15가지 멀웨어 및 바이러스 통계, 동향 및 사실, Safety Detectives

4 랜섬웨어 공격으로 볼티모어 카운티 공립학교 폐쇄, New York Times, 2020년 11월

PS2028-01 03/2021