퓨어스토리지와 Veeam을 통한 랜섬웨어 방어

퓨어스토리지 플래시어레이//C(FlashArray//C) 및 세이프모드(SafeMode) 스냅샷을 통한 Veeam 소프트웨어 데이터 보호

랜섬웨어 공격은 기업과 IT 리더들이 지속적으로 해결해야하는 우선 과제입니다. 여기에는 그럴 만한 이유가 있습니다. 랜섬웨어는 조직의 생명줄과도 같은 데이터에 대한 액세스를 마비시킬 수 있기 때문입니다. 점점 더 복잡해지고 빈번하게 발생하고 있는 위협들은 심각한 결과를 초래할 수 있습니다. 제대로 대비하지 않으면 데이터를 복호화하기 위해 공격자에게 대가를 지불해야만 합니다.

데이터를 보호하기 위해 기업들은 매년 수백만 달러를 지출하고 있으며, 사람의 실수가 멀웨어 공격의 주요 원인입니다. 이러한 상황에서 많은 기업들은 정교하게 설계된 백업 및 복구 전략의 전략적 가치를 여전히 과소평가하고 있습니다.

Cybersecurity Ventures에 따르면 2021년 랜섬웨어로 인한 피해 비용은 200억 달러에 이를 것으로 예상됩니다. 이는 2015년 대비 57배 이상 증가한 수치입니다.

CrowdStrike의 연구원들은 '맹수 사냥,' 즉 다운타임에 특히 민감한 대규모 조직을 겨냥한 공격이 늘고 있다고 밝혔습니다.

"쉽게 사용할 수 있고 안정적인 복구가 가능하기 때문에 Veeam을 선택했습니다. CryptoLocker 바이러스 공격을 받았을 때, 정말 쉽고 안정적으로 Veeam을 사용할 수 있었습니다. Veeam 덕분에, 필요할 때 언제든지 데이터를 사용할 수 있다는 확신을 갖게 되었습니다."

Bob Eadie, Bedford School
IT 시스템 관리자

랜섬웨어 방어를 위한 Veeam 및 퓨어스토리지 모범 사례

조직은 3-2-1 데이터 보호 원칙 등 데이터 보호를 위한 일반적인 모범 사례를 도입하고 리스크 평가를 수행하여 위협에 대비할 수 있습니다. 3-2-1 원칙은 **3개**의 데이터 복사본을 **2가지** 유형의 미디어로 생성한 후 **1개** 복사본을 오프사이트에 보관하는 것입니다. 이외에도 백업 환경이 '에어 갭(air gap)' 상태가 되어야 합니다. 즉, 백업 데이터를 겨냥한 공격을 차단할 수 있도록 백업 환경을 오프라인으로 운영하거나 백업에 쓰기가 불가능하도록 만들어야 합니다. 정기적인 위험 평가를 수행하는 것도 잠재적인 위험을 선제적으로 식별하기 위한 전체적인 데이터 보호 전략의 일부가 되어야 합니다. 또한, 위험 평가의 일부로, 데이터가 복구 가능하고 쉽고 빠르게 복원될 수 있는지 확인할 수 있어야 합니다.

Veeam 랜섬웨어 모범 사례 솔루션

Veeam®은 랜섬웨어를 방지해주지는 않지만, Veeam Availability Suite™ 고유의 고급 기능과 3-2-1 데이터 보호 원칙을 따르는 랜섬웨어용 Veeam 솔루션을 통해, 기업이 랜섬웨어에 감염된 중요한 데이터를 손상되지 않은 상태로 빠르고 효과적으로 복구할 수 있도록 합니다.

3개의 데이터 복사본: 1차 또는 운영 데이터 이외에도, 데이터의 백업 복사본과 백업 데이터의 복사본이 있어야 합니다. 그리고 이러한 복사본들은 다른 물리적 장치에 저장되어 있는 것이 이상적입니다.

2가지 유형의 미디어: 같은 데이터 센터에 있는 드라이브가 손상되지 않도록 하려면 여러 형태의 미디어를 사용해야 합니다. Veeam은 기본적으로 디스크, 테이프, 백업 어플라이언스, 클라우드 등 다양한 미디어 유형의 백업을 지원합니다.

PURESTORAGE®

1개의 오프사이트 복사본: Veeam의 고급 백업 및 복제 기능은 Veeam Cloud Connect를 사용해 오프사이트, 테이프 또는 클라우드에 있는 두 번째 위치에서 이미지 기반 복제 및 백업 복사본을 쉽게 확보할 수 있도록 해줍니다. Veeam은 빠르고 안전한 복제 및 백업 복사본을 제공할 수 있도록 WAN 가속화 및 암호화를 제공합니다.

위험 평가: Veeam Availability Suite에는 Veeam 백업 인프라를 위한 강력한 모니터링, 보고 및 용량 계획 툴인 Veeam ONE™이 포함되어 있습니다. 이 툴에는 즉각적으로 사용할 수 있는 보고 기능이 포함되어, 백업 평가를 통해 보호 상태를 확인해주고 잠재적인 랜섬웨어 활동에 대한 경고를 제공합니다.

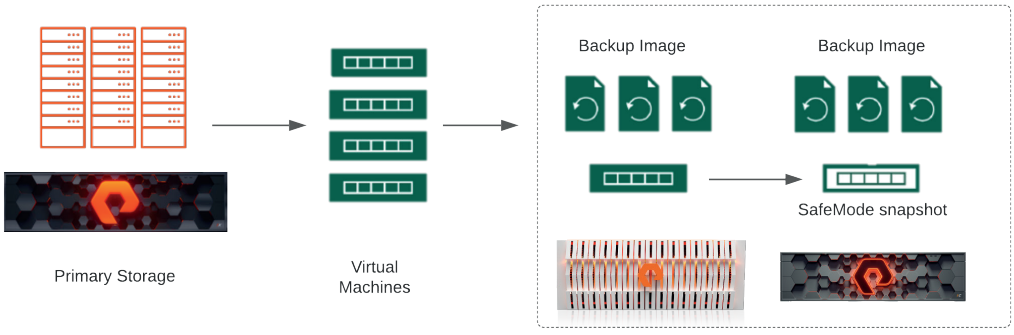
불충분한 기존의 데이터 보호

백업은 자연 재해 또는 인적 재해 복구, 데이터 손상 또는 우발적인 삭제 등 흔히 발생할 수 있는 상황에서 중요한 데이터를 보호합니다. 그러나 랜섬웨어 공격은 디스크나 테이프 같은 레거시 아키텍처에 구축된 기존 데이터 보호 인프라에 큰 부담을 줄 수 있습니다. 첫째, 복구 SLA를 충족하는 데 이미 어려움을 겪고 있다면, 랜섬웨어 공격으로 인해 계획되지 않은 추가적인 다운타임이 발생해 상황이 악화될 수 있습니다. 둘째, 백업 시스템에 에어 갭이 없다면 손상된 데이터의 복구를 고려하기 전에 먼저 백업 솔루션을 다시 설치하고 재설정해야 할 수도 있습니다.

세이프모드(SafeMode) 스냅샷을 통한 데이터 보호 강화

백업 환경에 에어 갭을 생성하면 백업 데이터를 랜섬웨어 공격으로부터 보호할 수 있습니다. 퓨어스토리지의 플래시어레이(FlashArray)와 플래시블레이드(FlashBlade) 시스템은 랜섬웨어 공격을 예방하는 새로운 접근 방식으로 추가적인 보호 계층을 제공합니다. 퓨리티(Purity) 운영 환경에 내장된 세이프모드 스냅샷 기능을 사용하면, 전체 백업을 수행한 후, 백업 데이터와 관련 메타데이터 카탈로그의 변경 불가능한 읽기 전용 스냅샷을 생성할 수 있습니다. 이러한 스냅샷에서 직접 데이터를 복구할 수 있으므로, 랜섬웨어나 악의적인 관리자의 공격으로부터 데이터를 보호할 수 있습니다. Veeam과 함께 퓨어스토리지의 올플래시 솔루션을 구현하면 다음과 같은 혜택을 얻을 수 있습니다.

- **강력한 보호:** 랜섬웨어는 세이프모드로 생성된 스냅샷을 삭제, 수정 또는 암호화할 수 없습니다. 또한, 권한을 부여 받은 지정된 담당자가 퓨어스토리지 기술 지원 팀과 직접 협력할 때에만 기능을 설정하거나 정책을 수정하고 스냅샷을 수동으로 삭제할 수 있습니다.
- **유연성:** 스냅샷 주기와 삭제 일정을 사용자가 지정할 수 있습니다.
- **신속한 복원:** 데이터와 함께 확장되는 대규모 병렬 아키텍처와 유연한 성능을 활용하여 백업 및 복구를 가속화할 수 있습니다.
- **투자 보호:** 퓨어스토리지의 플래시블레이드와 플래시어레이에는 세이프모드 스냅샷 기능이 내장되어 있기 때문에 추가 비용이 들지 않습니다.



PURESTORAGE®

퓨어스토리지의 기존 서브스크립션이나 유지보수 지원 계약에는 지속적인 개선이 포함됩니다.

Veeam & 퓨어스토리지가 랜섬웨어 복구를 지원하는 방법

랜섬웨어 공격으로부터 신속한 복구: 빠른 가상머신 및 세분화된 복구를 통해 암호화된 랜섬웨어 데이터베이스, 애플리케이션, 파일 및 운영 체제를 오버라이드합니다.

신속한 복구 및 중단 없는 애플리케이션 성능: 퓨어스토리지 올플래시 어레이와 긴밀하게 통합되어 운영 시스템에 영향을 주지 않고 자주 백업할 수 있습니다. 또한, 퓨어스토리지의 세이프모드 스냅샷을 사용하면 수정하거나 암호화할 수 없는, 변경 불가능한 백업 데이터를 생성할 수 있습니다.

복구 지점 테스트 및 검색: Veeam DataLabs™를 사용해 가장 최근의 양호한 복구 지점을 빠르고 쉽게 찾을 수 있습니다.

요약

퓨어스토리지와 Veeam의 모범 사례 솔루션은 조직이 랜섬웨어로부터 신속하게 복구하는 것은 물론, 일상적인 작업에 엔터프라이즈급 데이터 가용성을 제공할 수 있도록 지원합니다.

더 알아보기

www.veeam.com/purestorage-flash-solutions.html