

8

IaaS, PaaS 및 SaaS용 백업 서비스의 이점



8가지 이점

	1. 시간 및 비용 절약	4
	2. 간단한 데이터 보호 및 안정적인 복구	5
	3. 빠르고 원활한 설정	6
	4. 포괄적이고 고속이며 확장 가능한 서비스	7
	5. 확장 가능한 스토리지 및 보존	8
	6. 보안, 불변성 및 복원력 있는 아키텍처	9
	7. 규정 준수 준비 완료, 신뢰할 수 있는 데이터 무결성	10
	8. 귀하의 워크로드에 맞게 목적에 맞춰 설계된 컨텍스트 인식 복구	11

소개

가장 중요한 비즈니스 데이터는 이제 사용자가 제어하지 않는 SaaS 및 클라우드 플랫폼에 저장되어 있습니다. Microsoft 365는 직원들이 협업하는 공간이고, Entra ID는 누가 접근할 수 있는지 결정하며, Salesforce는 영업 파이프라인과 수익 기록을 저장하고, Azure와 AWS는 이 모든 것의 기반이 되는 인프라를 운영합니다. 이러한 플랫폼은 생산적이고 빠르며 서로 긴밀하게 연결되어 있습니다. 이러한 연결성 때문에 플랫폼이 취약해집니다.

이제 사용자 신원이 주요 공격 표면입니다. Microsoft는 초당 수천 건의 자격 증명 기반 공격을 기록합니다. 공격자가 신뢰할 수 있는 자격 증명으로 환경 내에서 이동하게 되면, 연결된 모든 시스템에서 데이터를 몰래 수정, 삭제 또는 반출할 수 있습니다. 침해가 발견될 때쯤이면, 기본 보존 기능은 손상된 상태만을 보존하고, 비즈니스에서 복원해야 하는 정상 버전은 보존하지 않습니다.

공동 책임 모델은 이를 명확히 보여줍니다. SaaS 공급자는 플랫폼을 보호하고, 데이터는 사용자가 직접 보호해야 합니다. 이 때문에 백업 전략은 IT 팀이 책임지는 가장 중대한 결정 중 하나가 됩니다. 그리고 점점 더 적은 인원으로 더 많은 일을 해야 하는 압박이 커지면서, 여러 환경에서 신원 기반의 신뢰할 수 있는 보호를 지속하기 위해 시간, 비용, 그리고 인재를 확보하는 것이 거의 불가능하게 느껴질 수 있습니다.

소프트웨어 기반 단일 워크로드 백업은 예측 가능한 환경과 항목 수준 복원을 위해 설계되었습니다. 특히 수천 개의 객체를 침해 이후에 다시 복구해야 할 때, 협업, 신원, CRM 및 클라우드 인프라 전반에 걸친 복원력이 필요하다면 이러한 도구들은 제대로 작동하지 않습니다. 이러한 도구들은 지속적인 유지관리, 조정 및 인프라 계획이 필요하며, 대규모 환경에서 여전히 완전한 복구를 제공하는 데 어려움이 있습니다. 각 플랫폼마다 다른 포인트 솔루션을 관리하면 도구가 확산되고, 가시성이 조각화되며, 공격자와 규정 준수 감사자가 사용자보다 먼저 발견할 수 있는 빈틈이 생깁니다.

SaaS 제공 백업 서비스는 모델을 바꿔 놓습니다. 공급자는 인프라, 보안 강화, 스토리지, 업데이트 등 전체 스택을 운영합니다. 팀이 환경을 연결하고 데이터 보호를 시작합니다. 복원 지점은 프로덕션 테넌트와 독립적으로 존재하므로 손상된 계정이 접근할 수 없습니다. 복구는 하나의 항목을 수정하거나 사고 후 환경의 상당 부분을 재구성하더라도 동일한 방식으로 작동합니다. 이 서비스가 SaaS, 아이덴티티 및 클라우드 인프라 전반에 걸쳐 보호를 통합하면, 보호 범위와 예측 가능한 비용, 인력이나 도구를 추가하지 않고도 확장할 수 있는 능력을 한 곳에서 볼 수 있습니다.

다음은 이 모델의 8가지 구체적인 장점과, 백업이 아이덴티티 침해라는 위협을 견뎌야 하는 상황에서 이러한 장점이 왜 중요한지에 대한 설명입니다.



1. 시간 및 비용 절약

기존의 자체 관리형 백업 환경에서는 비용을 예측하기가 거의 불가능합니다. 하드웨어 유지 관리, 스토리지 조정, 취약점 패치, 시스템 강화, 그리고 최악의 상황에 대비한 복구 준비에는 전문적인 역량과 상당한 시간이 요구됩니다. 인프라는 만약을 대비하여 과도하게 구축되어야 하므로, 조직은 일상적으로 사용하지 않는 용량에 대해 비용을 지불하고, 성장이 계획을 앞지르면 예상치 못한 비용에 시달리게 됩니다. 비즈니스가 의존하는 모든 SaaS 및 클라우드 플랫폼에 이를 적용하면 낭비가 빠르게 누적됩니다.

공급업체가 인프라, 스토리지, 보안 및 업데이트를 운영하기 때문에 팀은 그럴 필요가 없습니다. IT 팀의 누구나 별도의 전문 교육 없이도 구성 실수에 대한 우려 없이 자신 있게 보호를 구성하고 데이터 복원을 수행할 수 있습니다. 모든 중요 워크로드가 하나의 플랫폼에 존재하면, 조용히 예산과 관심을 소모하는 도구의 난립을 없앨 수 있습니다. 조달 주기가

줄어들고, 관리해야 할 공급업체 관계가 감소하며, 위험이 눈에 띄지 않게 숨어있는 도구 간의 격차가 줄어듭니다.

예측 가능한 구독형 가격 책정이 예측할 수 없는 자본 지출과 긴급 구축을 대체합니다. 일부 SaaS 백업 공급업체는 무제한 또는 탄력적 스토리지를 제공하므로, 데이터가 증가해도 비용이 눈에 띄지 않게 상승하지 않습니다. 보호는 SaaS 및 클라우드 활용 범위에 맞춰 자동으로 확장됩니다. 사용한 만큼만 비용을 지불합니다.

그 결과, 더 간편하게 운영할 수 있고 예산을 더 쉽게 책정할 수 있으며, 팀이 인프라 전문가가 되어야만 작동시키는 것이 아닙니다. 이 모든 것은 복원력 전략의 순효과입니다.

백업은 별도의 업무가 아니라 예산 항목이어야 합니다.

인프라 오버헤드 없이 예측 가능한 SaaS 백업



용량 계획 시 과도
프로비저닝과 갑작스러운
비용을 제거합니다.



특별한 인프라 전문
지식 없이 운영을
간소화할 수 있습니다.



구독형 가격 책정은 예측할
수 없는 자본 및 긴급
비용을 대신합니다.



2. 간단한 데이터 보호 및 안정적인 복구

자체 관리형 백업은 결코 끝나지 않습니다. SaaS와 클라우드 플랫폼은 끊임없이 변화하고 있으며, 백업 시스템도 이에 보조를 맞춰야 합니다: 패치, 성능 조정, 스토리지 확장, 보안 강화. 이러한 업무는 영구적으로 이루어지며, IT가 담당하는 다른 모든 업무와 동일한 팀과 예산을 두고 경쟁하게 됩니다.

SaaS에서 제공하는 백업 서비스는 복원 지점을 프로덕션 환경과 완전히 분리하여 저장하고 운영합니다. 침해된 신원, 잘못된 구성 또는 테넌트 내의 악의적인 변경은 복원 지점에 접근할 수 없습니다. 이러한 분리가 이 섹션의 핵심 논점이며, 그 이유를 명확히 설명할 가치가 있습니다. 공격자가 유효한 자격 증명으로 변경을 수행할 경우, 프로덕션 환경은 더 이상 신뢰할 수 있는 정보 소스가 아닙니다. 백업은 신뢰할 수 있어야 합니다.

이 서비스는 스토리지 확장, 성능 최적화, 취약점 관리, 그리고 지속적인 보안 업데이트를 담당합니다. 팀이 보호 구성, 보존 기간 설정, 복원 실행을 모두 할 수 있는 단일 인터페이스를 보게 됩니다. 삭제된 이메일 하나를 복구하든, 중대한 사고 이후 여러 플랫폼에서 구성과 권한을 재구축하든, 경험은 동일합니다.

쉽게 도입할 수 있습니다. 간편하게 운영되며, 복구가 가장 중요할 때 안정적으로 작동합니다.



3. 빠르고 원활한 설정

백업 소프트웨어를 배포하는 것은 종종 최악의 부분입니다. Server를 구축하고, 스토리지를 구성하며, 네트워크를 설정하고, 전문가와 협력하고, 소프트웨어 라이선스를 정확하게 취득하며, 첫 번째 백업이 실행될 때 모든 것이 실제로 작동하기를 기대합니다. 각 단계마다 위험이 따르며, 모든 단계가 동시에 문제 없이 진행되어야 합니다.

이러한 시스템은 학습 곡선이 있으며, 환경이 바뀔 때마다 다시 설계해야 합니다. 이러한 투자에도 불구하고 기존 백업은 여전히 너무 자주 실패합니다. Veeam의 2025 랜섬웨어 트렌드 보고서에 따르면, 전체 조직의 53%가 사고 후 완전한 생산성을 달성할

만큼 충분히 빠르게 복구하지 못하고 있습니다. 이는 애초에 손상을 일으킨 신원 기반 사고로부터 백업이 분리되어 있지 않았기 때문입니다.

SaaS 기반 백업 서비스는 이러한 모든 과정을 생략합니다. Server를 구축할 필요, 스토리지를 프로비전할 필요 및 용량 계획을 모델링할 필요가 없습니다. 서비스를 SaaS, 신원 및 클라우드 환경에 연결하면 몇 분 안에 데이터 보호를 시작할 수 있습니다. 하나의 플랫폼이 한 번의 배포만으로 모든 워크로드를 지원합니다.

한 번만 구성하고 계속 진행하세요.





4. 포괄적이고 고속이며 확장 가능한 서비스

조직이 백업을 자체적으로 관리할 때는 Server, 스토리지, 소프트웨어를 수동으로 결합해야 합니다. 또한 이러한 시스템이 효과적으로 운영되도록 지속적으로 관리 작업의 광범위한 목록을 수행해야 합니다. 사용자 지정이 이루어져도, 자체 관리형 백업 환경에서는 작은 구성 오류, 사각지대, 그리고 유지관리의 격차가 조용히 누적되어, 복구가 실제로 테스트될 때 복구 능력을 약화시킵니다.

완전 관리형 서비스에서 달라지는 점은 복구 속도입니다. SaaS 백업 플랫폼은 각 워크로드에 맞게 설계된 백업에 최적화된 API를 사용하므로, 자체 하드웨어와 네트워크에 제한될 때는 불가능한 속도로 복원이 실행됩니다. 이것은 대규모 환경에서 가장 중요합니다. 아이덴티티 기반 사고가 SaaS,

아이덴티티, 클라우드 환경 전반에서 동시에 수만 개의 객체를 건드릴 때, 기존 도구는 제대로 작동하지 않습니다. 이 도구들은 항목 단위 복구를 위해 설계되었습니다. 다중 워크로드 재구성은 완전히 다른 문제입니다. SaaS 백업 서비스는 이러한 작업을 공급자 인프라에서 병렬로 처리하므로, 대규모 복원 시 하드웨어를 과도하게 프로비저닝하거나 맞춤형 재해 복구 워크플로를 미리 설계할 필요가 없습니다.

이러한 상황에서는 대규모 복구가 더 이상 계획 단계에 머무르지 않고 신뢰할 수 있는 기능이 됩니다.

백업 공급업체 서비스 제공 방식



사용자 관리형





5. 확장 가능한 스토리지 및 보존

현대 협업과 클라우드 운영은 방대한 양의 데이터를 생성합니다. 파일, 채팅, 버전, 기록, 사용자 계정, 그룹 멤버십. 인시던트 발생 후 복구는 얼마나 많은 이력을 보관했는지와 그 이력이 손상된 환경 외부에 저장되어 있는지에 따라 달라집니다.

SaaS 백업 서비스는 이러한 제한을 해소합니다. 이 플랫폼은 보호되는 모든 워크로드에서 데이터가 증가함에 따라 스토리지를 탄력적으로 확장합니다. 단일 파일을 복원하든, ID 기반 침해로 인해 수개월간의 협업, 신원, 그리고 비즈니스 중요 데이터를 재구성하든, 스토리지 용량이 병목 현상이 되는 일은 없습니다. 많은 패키지에는 무제한 또는 탄력적 스토리지가 포함되어 있어 데이터 증가로 인한 복원력 비용의 압박을 해소합니다.

스토리지 용량은 방정식의 절반에 불과합니다. SaaS 플랫폼은 공격자가 유효한 자격 증명을 사용하여 가한 변경을 포함하여 현재 존재하는 데이터를 그대로 보존합니다. 완전한 복구를 위해서는 침해 이전의 환경을 반영하는 변경되지

않은 이전 버전에 접근할 수 있어야 합니다. 유연한 장기 보존을 통해 조직은 규정 준수, 정보 검색, 내부 관리 감독 또는 전면적인 롤백에 필요한 기록 깊이를 정확하게 유지할 수 있습니다.

해당 데이터가 어디에 있는지도 중요합니다. 글로벌 규정은 데이터가 얼마나 오래 보관되는지, 어디에 저장되는지, 그리고 누가 접근할 수 있는지를 규정합니다. 데이터 레지던시 제어 기능이 내장된 SaaS 백업 서비스를 사용하면, 각 지역마다 별도의 인프라를 구축하지 않고도 지역별 요구 사항에 맞게 스토리지 위치를 조정할 수 있습니다.

이 서비스의 혜택은, 생성한 데이터의 양이나 보호하는 워크로드, 그리고 복구해야 하는 시점이 얼마나 과거이든 상관없이, 언제든지 돌아갈 수 있는 완전한 특정 시점의 환경 버전을 제공한다는 점입니다.

확장 가능하고 규정을 준수하는 데이터 복원력을 위한 탄력적인 SaaS 백업



탄력적인 스토리지는 복구 과정에서 용량 제한을 해제합니다.



장기 보존으로 손상 이전의 깨끗한 데이터 가용성이 보장됩니다.



데이터 위치 관리 기능은 전 세계 규정 준수를 지원합니다.

6. 보안, 불변성 및 복원력 있는 아키텍처

위에서 언급한 모든 이점도 백업이 안전하지 않다면 아무런 의미가 없습니다. 지난 1년 동안 절반 이상의 조직이 SaaS 어플리케이션에서 데이터 손실 또는 손상을 보고한 상황에서, 운영의 간소화는 백업 환경이 직접 구축하는 것만큼 안전하고, 변경이 불가능하며, 신뢰할 수 있을 때만 의미가 있습니다.

데이터는 종단 간, 전송 중, 저장 시 모두 암호화된 상태로, 변경이 불가능하게 저장됩니다. 백업 환경은 자체 인증 도메인에서 운영되며, 프로덕션 ID로부터 완전히 격리되어 있습니다. 공격자가 SaaS 테넌트의 자격 증명을 침해하더라도, 해당 자격 증명을 사용하여 백업 사본에 접근하거나 수정하거나 삭제할 수 없습니다. 물리적 격리는 프로덕션 환경과 복구 데이터 사이의 아키텍처적 경계입니다.

공급자가 전체 스택에서 패치, 취약성 관리 및 모니터링을 담당하므로, 팀의 개입 없이 운영상의 공격 표면이 지속적으로 줄어듭니다. 아키텍처는 제로 트러스트 원칙을 따릅니다. 침해를 가정하고, 영향 범위를 제한하며, 손상된 환경이 건드릴 수 없는 복구 경로를 유지합니다. AI 기반 위협 탐지 기능은 보호된 워크로드에서 대량 삭제, 비정상적인 권한 변경, 이상 데이터 수정과 같은 의심스러운 패턴을 백업 데이터로 전파되기 전에 탐지합니다.

가용성과 내구성은 하나의 아키텍처에 내장되어 있습니다. 백업 데이터는 지리적으로 분산된 내결함성 데이터 센터에 여러 중복 복사본으로 저장됩니다. 지역이 다운되더라도 복구 데이터는 그대로 보존됩니다. 보안 모델은 아키텍처 수준에서 강제됩니다: 불변성, 격리, 암호화 및 중복성. 기본값은 안전합니다.

그리고 이 서비스는 팀이 매번 모든 것을 완벽하게 처리해야만 하는 것에 의존하지 않습니다.





7. 규정 준수 준비 완료, 신뢰할 수 있는 데이터 무결성

자신의 데이터를 신뢰할 수 없을 때 규정 준수는 더 어려워집니다. 침해된 ID에 의해 SaaS 데이터가 변경되거나 삭제되거나 손상된 경우, 사고 이전에 존재했던 것을 증명하는 것이 핵심 과제가 됩니다. 규제 기준은 요청 시 깨끗한 이력 기록을 생성할 수 있다고 가정합니다. 독립적인 백업이 없으면 다음을 할 수 없게 됩니다.

네이티브 관리 감독 도구는 데이터를 현재 상태로 보존합니다. 이들 도구는 과거 상태를 보존하지 않습니다. 정보가 변경되었다면, 설령 정상적인 신원에 의해 이루어졌더라도, 프로덕션 환경에는 더 이상 원본 버전이 남아 있지 않을 수 있습니다. 또한 신원 기반 변경 사항이 SaaS 및 클라우드 플랫폼의 감사 로그에 자연스럽게 녹아들기 때문에, 조직은 무엇이, 언제, 왜 발생했는지 입증하기 어렵습니다.

프로덕션 환경 외부에 저장된 독립적인 특정 시점 복사본은 프로덕션 환경 자체로는 제공할 수 없는 증거를 제공합니다. 감사, eDiscovery, 조사, 규제 검토 중에는 이러한 불변 버전이 공식 기록이 됩니다: 무엇이, 언제, 어떤 상태로 존재했는지.

GDPR, DORA, HIPAA 및 APPI와 같은 규정은 데이터가 저장되는 위치와 접근 권한이 있는 사람에 대해 엄격한 기준을 적용합니다. 레지던시 제어 기능이 내장된 SaaS 백업 서비스는 조직이 백업 데이터의 위치를 정확하게 결정할 수 있게 하여, 각 지역별 규정에 맞추면서도 지역마다 맞춤형 인프라를 구축할 필요가 없습니다.

요구 시 규정 준수를 입증하는 것은 이를 달성하는 것만큼이나 중요합니다. 내장된 보고 및 감사 로깅은 백업 활동, 보존 상태, 복원 이력에 대한 명확하고 내보내기 가능한 기록을 제공합니다. 감사 담당자나 법무팀이 데이터 보호, 보존, 복구 가능성을 증명해야 할 때, 관련 증거가 이미 갖추어져 있습니다.

SaaS 백업 공급자는 정기적으로 타사 감사를 통해(공급자에 따라 SOC 2 Type II, ISO 27001 등) 자사의 보안 및 데이터 처리 관행이 외부 기준에 부합하는지 검증받습니다. 이러한 인증은 귀하의 규정 준수 태세의 일부가 됩니다.

규정 준수는 결코 놀라운 일이 되어서는 안 됩니다.





8. 귀하의 워크로드에 맞게 목적에 맞춰 설계된 컨텍스트 인식 복구

중요 데이터는 한 곳에만 존재하지 않습니다:

- **Microsoft 365는 협업을 가능하게 합니다.**
- **Entra ID는 액세스를 관리합니다.**
- **Salesforce는 고객 정보, 영업 파이프라인 및 운영 기록을 저장합니다.**
- **Azure와 AWS는 모든 것을 하나로 연결하는 인프라를 호스팅합니다.**

각 플랫폼마다 데이터, 권한, 정책이 상호 작용하는 방식에 대해 고유한 아키텍처, API, 그리고 규칙이 있습니다. 이러한 요소들을 상호 교환 가능한 것으로 취급하는 백업은 기껏해야 불완전하고, 최악의 경우 잘못된 복구를 초래할 수 있습니다. 전용 백업은 각 플랫폼의 고유한 개체 모델과 API에 맞춰 보호 체계를 설계함으로써 이 문제를 해결합니다.

Microsoft 365와 Entra ID의 경우, 백업 최적화 API를 사용하여 고객 하드웨어에 배포된 소프트웨어보다 훨씬 빠르게 백업 및 복원을 실행합니다. 더 중요한 것은, 백업이 Exchange 데이터, SharePoint 사이트, OneDrive 콘텐츠, Entra ID 권한, 그룹 멤버십 및 앱 등록 등 여러 개체에 걸친 연결된 맥락을 포괄적으로 캡처한다는

점입니다. 복원은 환경을 본래 상태로 되돌립니다. ID 기반 인시던트가 한 번에 수천 개의 개체에 영향을 미칠 때, 이것이 완전한 롤백과 몇 주에 걸친 수동 조정의 차이입니다.

Salesforce 보호는 플랫폼의 고유한 데이터 모델을 기반으로 하여 레코드, 메타데이터, 첨부 파일 및 이들의 관계를 보존합니다. 연결된 연락처, 영업 기회 또는 사용자 지정 개체 없이 거래처 레코드를 복원하면 해결되는 것보다 더 많은 혼란이 발생합니다. 전용 백업은 이러한 종속성을 캡처하므로 관리자는 자신 있게 복원할 수 있습니다.

Azure 보호에는 가상 머신, 관리형 디스크, 스토리지 계정, 그리고 하이브리드 및 클라우드 네이티브 운영을 지원하는 인프라 계층이 포함됩니다. VM은 관리형 디스크, 네트워크 구성, 그리고 리소스 그룹 멤버십에 의존합니다. 이러한 종속성을 캡처하는 백업은 실제 프로덕션 상태를 반영하는 복원 지점을 생성합니다. 부팅을 시도하기 전까지는 완전해 보이지만 실제로는 완전하지 않은 복원 지점을 생성하는 백업.

네 가지 워크로드 모두에서 원칙은 동일합니다: 권한, 정책, 그룹 멤버십 및 플랫폼 간 종속성이 데이터와 함께 복원되어 환경이 정상적으로 복구됩니다. 필수 컨텍스트가 누락되면 복원이 표면상 완료되어도 실제로는 접근이 끊기고, 워크플로가 실패하며, 신뢰 경계가 복구하기 어려운 방식으로 변경될 수 있습니다.

전용 보호 방식은 각 플랫폼의 API를 정확하게 사용하여, 세밀한 항목 단위 복구가 정밀한 수정에 활용되고, 연결된 시스템에서 사고가 확산될 때 대규모 재구성이 가능합니다.



Veeam Data Cloud와 함께하는 SaaS 데이터 복원력

SaaS 및 클라우드 워크로드에 대한 백업이 서비스 형태로 제공될 때, 기본 원칙이 변화합니다: 더 빠른 보호 시작, 더 간편한 운영, 환경에 맞게 확장되는 스토리지와 보존 및 ID 기반 인시던트나 일상적인 실수에도 견딜 수 있는 복구가 가능합니다.

SaaS, 클라우드, 그리고 ID 환경 전반에서 핵심은 신뢰할 수 있는 독립적인 복원 지점과 비즈니스에 미치는 영향이 가중되기 전에 중요한 것을 재구축할 수 있을 만큼 빠른 복구입니다. Veeam Data Cloud는 세 가지 기능을 통해 이를 제공합니다.

- **복원력 구현.** 정책 자동화, 정책 기반 보호 및 정밀하고 신속한 복구를 통해 운영이 최소한의 중단으로 계속 진행됩니다. 모니터링, 보고 및 분석 결과로 얻은 실행 가능한 인사이트는 보호를 검증하고 이슈 해결을 지원합니다.
- **임베디드 보안.** 물리적 격리, 불변성, 암호화 등 기술로 내장된 사이버 복원력 보호. 위협 인텔리전스는 랜섬웨어 및 관련 위협을 탐지하고 대응하는 데 도움이 됩니다. 공통 RBAC는 애플리케이션 및 역할별로 액세스 권한을 중앙 집중화하고 표준화합니다.
- **운영 우수성.** 예측 가능한 일체형 패키징과 통합된 다중 워크로드 UI/UX는 인프라 오버헤드를 줄이고 사용성을 개선합니다. 규모에 따른 효율성은 전문 지식 격차를 해소하고 운영 부담을 줄이는 데 도움이 됩니다. AI 가속화는 백업, 보안 및 복구 요구 사항을 최적화하면서 시간과 리소스를 확보하는 데 도움이 됩니다.

Veeam Data Cloud는 데이터 복원력을 위한 통합 클라우드 플랫폼으로 자리매김하고 있으며, 서비스 형태의 간편함과 함께 업계를 선도하는 데이터 복원력 기술을 제공합니다. 이 서비스는 클라우드 네이티브 백업 및 스토리지 서비스를 통해 복원력 있는 데이터 보호와 데이터 복구를 다중 클라우드 데이터에 제공하며, 백업 소프트웨어, 인프라, 스토리지가 하나로 패키징된 SaaS 솔루션으로 제공됩니다.

Veeam Software 소개

Veeam®은 데이터 복원력 분야의 글로벌 1위 기업으로, 모든 비즈니스가 장애 발생 시 모든 데이터를 언제 어디서든 필요할 때 자신 있게 관리하며 비즈니스를 빠르게 재개할 수 있어야 한다고 믿습니다. Veeam은 이를 완전한 복원력이라고 부르며, 고객이 이를 달성할 수 있도록 혁신적인 방법을 지속적으로 개발하는 데 열정을 쏟고 있습니다. Veeam 솔루션은 데이터 백업, 데이터 복구, 데이터 이식성, 데이터 보안, 데이터 인텔리전스를 제공함으로써 데이터 복원력을 극대화하도록 설계되었습니다.

Veeam을 통해 IT 및 보안 리더들은 클라우드, 가상 환경, 물리 환경, SaaS, 그리고 Kubernetes 환경 전반에서 애플리케이션과 데이터가 보호되고 항상 사용 가능하다는 사실에 안심할 수 있습니다. 시애틀에 본사를 두고 30여 개국에 지사를 둔 Veeam은 전 세계 55만여 고객, 그리고 Fortune 500대 기업 중 82%가 비즈니스 연속성을 위해 신뢰하는 기업입니다. 혁신적인 복원력은 Veeam에서 시작됩니다. 자세히 알아보려면 www.veeam.com을 방문하거나 LinkedIn [@veeam-software](https://www.linkedin.com/company/veeam-software) 및 X [@veeam](https://twitter.com/veeam)에서 Veeam을 팔로우하세요.

➔ 자세히 알아보기: [veeam.com](http://www.veeam.com)