



SaaS 데이터를 보호해야 하는 6가지 이유

veeam

SaaS: 오늘날 비즈니스의 핵심 동력

SaaS(서비스형 소프트웨어) 어플리케이션은 이제 엔터프라이즈 운영의 중심에 자리 잡고 있습니다. 이메일, 협업, 고객 참여, 분석, 자동화 등 거의 모든 기능이 유연하고, 확장 가능하며, 비용 효율적이고, 비즈니스 전반과 깊이 연결된 클라우드 플랫폼을 통해 실행됩니다. 도입이 빠르게 가속화된 데에는 그만한 이유가 있습니다. SaaS는 비효율을 줄이고 조직의 민첩성을 높여줍니다.

하지만 이러한 의존성에는 오해가 있습니다. SaaS 데이터는 대부분의 기업이 인식하는 것보다 훨씬 더 취약합니다. 많은 사람들이 그들의 공급자가 완전한 보호를 제공한다고 가정합니다. 실제로 클라우드 서비스는 가동 시간과 가용성에 중점을 두며, 장기 보존이나 신뢰할 수 있는 컨텍스트 기반 복구에는 중점을 두지 않습니다.

네이티브 도구는 이러한 초점을 반영합니다. 짧은 보존 기간, 좁은 복원 범위, 그리고 오늘날 엔터프라이즈가 직면하는 다양한 장애로부터 복구할 수 있는 제한적인 복구 메커니즘만을 제공합니다. 실수로 삭제, 구성 오류 또는 가장 심각한 사고를 초래하는 ID 기반 공격으로부터 방어하지 못합니다. 공격자가 Entra ID 또는 다른 신원 공급자를 통해

접근 권한을 획득하면, 변경 사항이 Microsoft 365와 연결된 SaaS 어플리케이션 전반에 연쇄적으로 발생할 수 있습니다 — 권한을 취소하거나, 구성을 손상시키거나, Teams 구조를 해체하거나, 대규모로 메일박스를 삭제하는 등의 일이 일어날 수 있습니다.

그 결과, SaaS 백업 및 복구가 엔터프라이즈 우선 순위에서 빠르게 부상하고 있습니다. 이러한 변화는 연속성 계획이 일상적인 운영상 문제 해결과 오늘날의 위협 환경을 특징짓는 대규모 장애까지 모두 포괄해야 한다는 인식이 커지고 있음을 반영합니다.

현재 조직의 15%만이 이를 최우선 과제로 여기고 있지만, 이 수치는 2028년까지 75%에 이를 것으로 예상됩니다.

이 전자책은 엔터프라이즈가 이러한 격차를 해소할 수 있도록 설계되었습니다. 실제 위험이 어디에서 발생하는지, 네이티브 도구가 부족한 이유, 그리고 현대적인 SaaS 복원력 전략에 필요한 요소—단일 파일 복원부터 중대 사고 후 전체 ID 연결 환경 재구축에 이르기까지—를 확인할 수 있습니다. 올바른 접근 방식을 통해 SaaS는 가장 중요한 순간에 신뢰할 수 있는 플랫폼이 됩니다.

A woman with dark hair and bangs, wearing a blue denim shirt, and a man with a beard, wearing a blue hoodie over a white shirt, are looking intently at a computer screen. The background is a blurred office environment with other people and computer monitors. The image has a blue and purple color overlay.

SaaS 애플리케이션에 데이터 보호가 필요한 이유는 무엇일까요?

1. 사이버 위협 및 신원 침해

랜섬웨어는 신원 악용, 자동화, 그리고 하이브리드 및 SaaS 생태계 전반에 걸친 신속한 교란을 기반으로 한 조직적인 갈취 모델로 진화했습니다. Coveware by Veeam가 발표한 2025년 3분기 데이터는 이러한 변화를 명확히 보여줍니다. Akira와 Qilin과 같은 높은 공격 빈도의 그룹들이 전체 관측된 공격의 약 65%를 차지했으며, 이들은 모든 규모의 조직에서 대규모로 운영할 수 있도록 해주는 랜섬웨어-서비스형(RaaS) 인프라의 지원을 받고 있습니다.

동시에, 갈취의 경제적 기반이 약화되고 있습니다. 평균 지급액은 2025년 2분기에서 3분기 사이에 66% 감소했으며, 피해자의 23%만이 어떤 형태로든 지급을 했습니다. 이는 역대 최저치입니다. 수익이 감소함에 따라 공격자들은 침해 시 가장 큰 영향력을 발휘할 수 있는 시스템, 즉 신원 공급자(Identity Provider)에 주목하고 있습니다.

신원 침해가 현대 침입 캠페인의 핵심이 되었습니다. 원격 액세스 침해는 3분기 사고의 절반 이상을 차지했으며, 소셜 엔지니어링, 헬프데스크 조작, 기술적 악용 간의 경계는 거의 사라졌습니다. 공격자들은 점점 더 제어를 우회하는 것이 아니라 합법적인 사용자나 지원 담당자에게 프로비전해 달라고 설득하여 접근 권한을 얻고 있습니다. 몇몇 사례에서는 공격 그룹이 자격 증명을 구매하겠다는 제안을 하며 직원들에게 직접 접근했습니다. 이는 한때 표적 스파이 활동에 사용되던 전술이었으나, 이제는 상업적 랜섬웨어 운영의 일부로 확고히 자리 잡았습니다.

일단 인증되면, 공격자는 기존 엔드포인트 멀웨어로는 얻을 수 없는 접근 범위를 확보합니다. 신원 관계를 열거하고, 권한을 상승시키며, Microsoft 365, Entra ID, Azure 및 상호 연결된 SaaS 환경에서 수평 이동합니다. 영향은 단순한 암호화에 그치지 않습니다. 권한이 수정되거나 제거되고, 사서함 및 SharePoint 구조가 삭제되며, Teams 구성이 붕괴되고, 자동화 워크플로가 손상됩니다. 스크립트는 손상을 가속화하여 대규모로 워크로드 전체에 파괴적인 변경을 전파합니다.

엔터프라이즈에게 있어 이러한 후속 신원 기반 중단은 종종 사고에서 가장 중요한 부분이 됩니다. 암호화가 주목을 끌 수 있지만, 신원 계층을 재구성하고, 테넌트를 복구하며, 구성 설정을 복원하고, 통합된 시스템 전반에서 영향 범위를 제한하며 GDPR, NIS2, 주별 개인정보 보호법과 같은 규제 프레임워크에 대응하는 데서 운영 부담이 발생합니다. 몸값을 지불하지 않더라도 복구 비용은 일반적으로 150만 달러를 초과합니다.

하이브리드 및 다중 클라우드 아키텍처는 이러한 문제를 더욱 가중시킵니다. 아이덴티티 시스템은 인증 정책, CI/CD 프로세스, 타사 SaaS 통합, DevOps 워크플로, 기존 애플리케이션 및 원격 액세스 모델을 뒷받침합니다. 공격자가 해당 계층 내에서 의미 있는 제어 권한을 얻으면 기존 보안 경계는 관련성을 잃게 됩니다.

따라서 엔터프라이즈 수준의 복원력은 ID 무결성에 달려 있으며, 이를 위해서는 강력한 관리 감독, 권한 사용에 대한 고충실도 모니터링, ID 손상으로부터 백업 인프라의 격리, 그리고 깨끗한 ID 상태를 재구축하고 SaaS 환경을 정확하게 복원할 수 있는 복구 파이프라인이 필요합니다. 이러한 기능을 갖춘 조직은 침입을 신속하게 억제할 수 있습니다. 그렇지 않은 조직은 연쇄적인 운영 실패에 직면하게 됩니다.

랜섬웨어의 무게 중심이 바뀌었습니다. 아이덴티티의 제어와 그것이 열어주는 시스템의 연쇄가 이제 최신 공격의 범위, 속도, 영향력을 결정합니다.

2. 내부 보안 위협

내부 보안 리스크는 불만을 품은 직원이나 우발적인 실수라는 전통적인 이미지에서 훨씬 더 확장되었습니다. 오늘날 '내부자 위협'에는 신뢰할 수 있는 액세스 권한을 가진 모든 사람이 포함됩니다. 여기에는 직원, 계약자, 침해된 신원, 그리고 조직 내부의 누군가에게 대신 액세스 권한을 부여하도록 설득하는 공격자까지 포함됩니다.



이러한 진화는 최근 위협 트렌드에 명확하게 반영되어 있습니다. 한때 피싱이나 패치되지 않은 VPN과 같은 기회주의적 진입점을 이용하던 랜섬웨어 그룹들은 이제 내부자 영입, 헬프데스크 업무 절차 악용, 그리고 경우에 따라 직원에게 뇌물을 주어 유효한 자격 증명을 획득하는 등 보다 직접적이고 효율적인 방법을 추구하고 있습니다. 한때 예외적 사례에 불과했던 것이 이제는 조용하고 저렴하며, 수익 압박을 받는 공격자들에게 적합한 신뢰할 수 있는 공격 경로가 되었습니다.

악의적인 의도가 없더라도 내부 위협은 일정하게 유지됩니다. 잘못 구성된 권한, 과도하게 공유된 폴더, 부적절하게 동기화된 SaaS 레코드, 또는 선의의 삭제는 Microsoft 365, Salesforce, 또는 모든 상호 연결된 SaaS 환경 전반에 즉시 전파될 수 있습니다. 네이티브 보존은 존재해야 하는 것이 아니라 현재 존재하는 것만 보존하기 때문에 이러한 변경 사항 중 상당수는 한 번 발견되면 되돌릴 수 없습니다.

팀은 분산되어 있고, 접근 방식이 다양하며, 개인 및 회사 장치가 자주 혼용됩니다. 이러한 조건으로 인해 정상적인 행동과 침해된 활동을 구별하기가 더 어려워집니다. 합법적인 사용자로 가장한 공격자, 콜백 피싱에 속은 직원, 또는 강압에 의해 행동하는 자격 증명을 가진 내부자는 신원 신뢰에만 의존하는 SaaS 플랫폼에서는 구분이 어렵습니다. 이렇게 상호 연결된 환경에서는 내부 위협이 이상 현상이 아니라 구조적 특성입니다. 신뢰가 무너지면 경우, 그 영향은 시스템, 신원, 자동화 전반에 걸쳐 빠르게 확산됩니다.

외부 공격자가 신뢰 기반의 접근을 통해 점점 더 침투하는 상황에서, 엔터프라이즈가 반드시 직면해야 할 질문은 조용한 침해가 전면적인 운영 위기로 확대되는 것을 막기 위해 충분한 가시성, 보호 장치 및 복구 경로를 갖추고 있는지 여부입니다.

3. 인적 오류 및 실수로 삭제

SaaS 플랫폼은 일상 업무를 지원하지만, 중요 데이터를 잃는 것이 얼마나 쉬운지와 이를 복구하는 것이 얼마나 어려운지 제대로 인식하는 팀은 드뭅니다. 폴더를 잘못 삭제하거나, 동기화 구성을 잘못하거나, 공유된 기록을 덮어쓰는 등의 단 한 번의 실수로도 핵심 정보가 즉시 사라질 수 있습니다. 많은 사람들은 이러한 플랫폼에서 복구가 간단하다고 생각합니다. 실제로는 그 반대인 경우가 많습니다.

Microsoft 365, Entra ID, 또는 Salesforce와 같은 시스템의 기본 복원 옵션은 짧은 보존 기간, 제한된 휴지통, 그리고 데이터 유형별로 일관성 없는 적용 범위로 인해 제약을 받습니다. 일부 객체는 아예 휴지통에 들어가지도 않고, 다른 것들은 누락된 것을 인지하기도 전에 이미 만료되어 버립니다. 그리고 SaaS 공급자는 환경의 현재 상태만을 보존하고, 과거의 특정 시점 버전은 저장하지 않기 때문에, 우발적인 변경 사항은 발견될 때쯤에는 복구가 불가능해질 수 있습니다.

이러한 단점은 SaaS 애플리케이션이 어떻게 설계되는지 고려해 보면 더욱 분명해집니다. SaaS 애플리케이션은 장기적인 보호가 아니라 협업과 실시간 성능을 위해 최적화되어 있습니다. 동기화 오류는 삭제를 모든 사용자에게 전파할 수 있습니다. 잘못 적용된 권한 변경으로 인해 경고 없이 콘텐츠가 숨겨지거나 변경될 수 있습니다. 그리고 독립적인 백업이 없으면 문제가 발생했을 때 복원할 신뢰할 수 있는 버전이 없습니다.

조직이 핵심 비즈니스 프로세스를 위해 SaaS에 더 많이 의존함에 따라 이러한 눈에 띄지 않는 실패의 영향이 더욱 커지고 있습니다. 한 번의 실수로 삭제로 인해 프로젝트가 중단되거나, 고객 관계가 악화되거나, 감사가 훼손되어서는 안 됩니다. 목적에 맞게 설계된 SaaS 백업은 순간적인 실수가 영구적인 손실로 이어지지 않고, 그저 순간으로 남도록 보장합니다.



4. 법적 위험, 규정 준수 위험 및 규제 위험



법적 및 규제적 압력은 조직이 법에 따라 데이터를 보존, 보호 또는 복구하지 못할 경우 수백만 달러의 벌금, 운영 중단, 평판에 지속적인 손상과 같은 구체적인 결과를 초래합니다.

2025년 이러한 기대치(요구 수준)는 계속해서 더 엄격해졌습니다. 현대의 공격자들은 이제 암호화와 데이터 유출을 동시에 활용하여 운영상 및 규제상 노출을 초래합니다. 그리고 신원 정보 침해가 SaaS 보안 사고의 주요 원인으로 자리잡으면서, 규제 기관들은 복구 능력을 관리 감독의 핵심 요소로 간주하고 있습니다. 공격자가 적법한 자격 증명을 사용해 데이터를 조작할 수 있는 경우에도, 조직은 여전히 깨끗하고 검증 가능한 상태로 복구할 수 있어야 합니다.

NIS2, DORA, 업데이트된 SEC 보고 규정, 그리고 새롭게 등장하는 개인정보 보호 기준과 같은 규정들은 모두 입증 가능한 복원력을 요구합니다. 조직은 공격자가 정상적인 신원 경로를 통해 기록, 권한, 로그, 구성 정보를 변경하거나 삭제했더라도 이를 정확하게 복원할 수 있음을 입증해야 합니다.

기본 보존 및 즉시 백업은 이러한 기대치를 충족할 수 없습니다. 내장 도구는 원치 않거나 악의적인 변경 내용을 포함하여 테넌트의 현재 상태만 보존합니다. 정확한 버전이 사라지면 규정 준수에 필요한 증거도 함께 사라집니다.

이제 규정 준수를 유지하려면 신뢰할 수 있는 데이터 버전을 보존하고 심사 시에도 안정적으로 복원할 수 있는 보호가 필요합니다. 현대적인 SaaS 복원력 전략은 무엇이 변경되었는지 입증하고, 필요한 데이터를 복구하며 신뢰받는 ID 채널 내에서 중단이 발생하더라도 규제 요구사항에 부합할 수 있게 해줍니다.

5. 데이터 손실로 인한 막대한 비용

데이터 손실로 인한 재정적 영향은 단일 파일의 누락에서 비롯되는 경우가 거의 없습니다. 진정한 비용은 정상적인 운영이 느려지거나 중단될 때 나타나며, 대엔터프라이즈의 경우 시간당 수십만 달러의 생산성 손실과 수익 지연이 발생할 수 있습니다. 여기에는 부수적 영향이 포함되지 않습니다. 예를 들어, 중단된 파이프라인, 지연되는 고객 약속, 내부 팀의 집중력 분산, 그리고 리더십이 계획된 이니셔티브가 아닌 위기 관리에 시간을 할애하는 등의 영향이 있습니다. 잠깐의 중단이라도 연쇄적인 운영 지연, 계약 위험 노출, 그리고 고객 신뢰의 장기적 하락을 초래할 수 있습니다.

랜섬웨어 몸값은 전체 경제적 비용의 작은 부분에 불과합니다. 더 큰 비용은 복구 과정 그 자체에서 발생하며, 데이터 재검증, 구성 재구축, 워크플로 복원 및 SaaS 환경의 무결성 확인에 수 시간에서 수 주가 소요될 수 있습니다. 인증 시스템이 영향을 받으면 복구에 필요한 노력이 크게 증가합니다. 단일 손상된 자격 증명 또는 손상된 구성으로 인해 권한이 변경되고, 메일박스가 삭제되며, 자동화가 중단되고, 수십 개의 상호 연결된 애플리케이션에서 워크플로를 손상시킬 수 있습니다.

현대 엔터프라이즈는 설계상 이러한 위험을 증폭시킵니다. ID 계층은 협업 도구, CRM, HR 시스템, 금융 애플리케이션, 그리고 맞춤형 SaaS 통합을 연결합니다. 해당 ID 계층이 손상되면 블라스트 레디우스(blast radius)가 빠르게 확산되어 기술적 장애가 조직 전체의 중단으로 바뀔 수 있습니다. 복구는 단순한 데이터 복원만으로는 충분하지 않으며, 팀은 환경이 의도한 대로 작동하도록 사용자, 시스템, 서비스 간의 관계를 다시 설정해야 합니다.

이러한 수준의 상호의존성을 고려한 복원력 전략이 없다면, 단일 사고로 인한 비용은 금전적 손실뿐만 아니라 시간, 집중력, 신뢰까지도 빠르게 증가하게 됩니다.



6. 비즈니스 연속성 확보

재해가 발생하면 연속성은 분 단위로 측정됩니다. 원인이 랜섬웨어, 지역적 중단, 통합 실패, 또는 SaaS 어플리케이션 전반에 영향을 미치는 아이덴티티 기반 공격이든, 시간은 즉시 가장 중요한 변수가 됩니다. 복구 속도가 중단이 국한된 상태로 유지될지, 아니면 장기적인 운영 장애로 확대될지를 결정합니다.

연속성 위험은 두 가지 수준에서 나타납니다. 실수로 삭제, 구성 오류, 동기화 실패 등 일상적인 문제들이 팀 간에 반복적인 마찰을 일으킵니다. 그리고 광범위한 아이덴티티 침해, 대량 삭제, 변조된 자동화, 또는 전체 사업부에 영향을 미치는 중단 기반 실패와 같은 재해 규모의 이벤트도 있습니다. 두 경우 모두 신속한 복원이 필요하지만, 각각에 요구되는 규모와 정밀성은 매우 다릅니다.

대부분의 팀은 비즈니스가 요구하는 속도로 두 가지 상황 모두에 대응할 준비가 되어 있지 않습니다. 현대의 인시던트는 종종 ID 관계를 재구성하고, 여러 시스템에 걸쳐 데이터를 검증하며, IT, 보안, 규정 준수, 운영 전반에 걸쳐 완화를 조율하는 과정을 포함합니다. 복구 기간이 수 주에 걸쳐 늘어나는 경우가 흔하며, 이는 Gartner에서도 지속적으로 강조하는 부분입니다. 이러한 지연은 실제적인 결과로 이어집니다. 예를 들어, 수익 주기의 차질, 서비스 약속의 불이행, 파트너십의 약화, 그리고 규제 노출의 확대 등이 발생할 수 있습니다.

엔터프라이즈 환경은 서로 긴밀하게 연결되어 있어 가동 중단 시간이 개별적으로 발생하는 경우는 드뭅니다. 단일 ID 침해 또는 통합 실패가 모든 다운스트림 어플리케이션에 영향을 연쇄적으로 확산시킬 수 있습니다. 가용성이 안전, 규정 준수 또는 고객 신뢰와 분리될 수 없는 의료, 금융, 정부, 중요 인프라와 같은 분야에서는 잠깐의 중단만으로도 심각한 운영 위험이 발생합니다.

효과적인 연속성 계획은 이러한 복잡성을 반영해야 합니다. 조직은 빠르고 안정적이며 검증 가능한 깨끗한 복구가 필요합니다. 이는 일상적인 운영을 보호하는 동시에 대규모의 ID 연계 장애로부터 복구할 수 있는 경로를 제공해야 합니다. 손상된 SaaS 데이터가 매 시간마다 비즈니스 전반에 마찰을 가중시키고, 이를 해결하는 데 필요한 노력이 늘어납니다.

이제 엔터프라이즈 연속성은 복구가 발생한 중단을 얼마나 빠르게 수습하고 통제할 수 있는지에 달려 있습니다.



이유에서 준비로

데이터 보호에서 타사 솔루션의 역할

SaaS 플랫폼은 포괄적인 데이터 보호가 아니라 가용성과 확장성을 위해 설계되었습니다. 네이티브 도구는 제한된 복원 지점, 짧은 보존 기간, 그리고 엔터프라이즈 환경의 복잡성 및 규제 요구사항에 부합하지 않는 협소한 범위의 복원 옵션만을 제공합니다. 그 결과, 대규모 환경에서 가장 중요한 정밀 복원, 장기 보존, 변경 불가능한 백업, 테넌트 간 가시성 및 규정 준수에 적합한 보고와 같은 핵심 기능들은 대부분의 공급자가 제공하지 않습니다.

환경이 점점 더 상호 연결됨에 따라 이러한 격차는 더 벌어집니다. 엔터프라이즈는 SaaS 애플리케이션, 신원 기반 접근 모델 및 몇 분 만에 수천 개의 객체를 수정할 수 있는 자동화된 워크플로에 의존합니다. 데이터가 손실되거나 변경될 때—구성 오류, 통합 실패, 신원 침해 또는 표적 공격 등으로 인해—네이티브 도구만으로는 깨끗하고 정상적인 환경을 복원하는 데 필요한 신속성과 정확성을 거의 제공하지 못합니다.

내보내기, 맞춤형 스크립트, 수동 복구 경로를 중첩하면 운영 부담이 증가하고 가시성이 저하됩니다. 복구 소요 시간이 길어지고, 연속성 계획을 지속적으로 유지하는 것이 더욱 어려워집니다.

임시 방편은 근본적인 문제를 해결하기보다 마찰을 가중시킵니다.

SaaS 플랫폼은 없어서는 안 될 존재이지만, 기본 보호 기능은 오늘날 엔터프라이즈가 운영하는 규모, 복잡성 및 규제 감독을 해결하도록 설계된 것이 아닙니다. 특수 목적의 백업 및 복구는 충분한 보존 기간, 무결성 보장, 그리고 복원 정확성을 제공함으로써 이러한 격차를 해소합니다. 이는 팀이 일상적인 실수를 바로잡거나, 영향이 큰 사고에서 복구를 하든 관계없이 현대적 운영 환경에 필요한 기능입니다.

ID 중심의 접근, 자동화, 그리고 밀접하게 연결된 시스템으로 정의되는 세상에서 복원력은 이러한 수준의 연계성을 위해 개발된 도구에 달려 있습니다. 타사 솔루션은 SaaS가 엔터프라이즈 전반에서 그 역할을 계속 확장함에 따라 신뢰성 있는 운영을 위한 체계와 보호 장치를 제공합니다.

SaaS 데이터 보호 실제 적용

엔터프라이즈는 Microsoft 365 및 기타 SaaS 환경을 보호하는 방법을 빠르게 재정의하고 있습니다. 최근 몇 년 동안 대부분의 조직은 오직 네이티브 도구만을 사용해왔으나, 오늘날에는 네이티브 도구만 사용하는 조직이 4곳 중 1곳도 채 되지 않습니다. 나머지 조직들은 SaaS 데이터를 단순한 편의가 아닌 핵심 인프라로 간주하는 통합 정책 중심 보호로 전환하고 있습니다.

이러한 변화는 경험이 이끌고 있습니다. 랜섬웨어 지불률은 사상 최저 수준으로 떨어졌지만 위협 환경은 더욱 심화되고 있습니다. 공격자들은 기존의 방어책을 우회하고 신원 정보 침해, 데이터 유출, 내부자 지원 접근과 같은 방법에 집중하고 있습니다. 이러한 방법들은 Exchange, SharePoint, OneDrive, Teams, 그리고 이들을 연결하는 Entra ID 관계 등 일상적인 업무가 이루어지는 시스템을 직접적으로 겨냥합니다.

네이티브 도구는 작은 이슈는 해결할 수 있지만, 실제 압박 상황에서는 제대로 대응하지 못합니다. 보존 기간이 짧고, 범위가 제한적이며, 손상 후 Microsoft 365 환경을 복구하는데 필요한 신원 컨텍스트가 부족합니다. 실제 공격이 발생하면 복구 시간이 종종 몇 시간까지 늘어나고, 운영상의 영향도 빠르게 커집니다.

이러한 사고를 견뎌낸 엔터프라이즈들은 이제 다음과 같은 기능을 제공하는 플랫폼을 우선시하고 있습니다:



세분성 이벤트와
테넌트 전체
이벤트에 대한
신속한 특정 시점 복구



법적 및 규제
요건을 충족하는
데이터 보존 기간 확장



문제가 확산되기
전에 조기에 문제를
발견하는 이상 탐지



복구 시간 창을
단축하고 운영 부담을
줄여주는 신속한 복원

이러한 중단이 더 빈번해지고 ID 기반으로 변화함에 따라, 이러한 기능은 이제 선택 사항이 아닌 필수입니다. Microsoft 365는 재무, 운영, 고객 참여, 영업 주기, 규제된 프로세스 및 소통의 기반을 뒷받침합니다. 실패하면 비즈니스 운영이 즉시 둔화됩니다. 몸값을 지불하지 않더라도, 엔터프라이즈는 주요 SaaS 또는 아이덴티티 기반 공격에서 복구하는 데 사고당 평균 150만 달러를 지출하고 있습니다.

SaaS 데이터 보호의 격차를 인식하는 것이 첫 단계입니다. Microsoft 365를 고려한 복구 계획을 핵심 재해 복구 전략에 포함시키면 조직은 중단 상황에서도 통제력을 유지할 수 있습니다.

최신 SaaS 데이터 복원력은 어떻게 나타납니까?

SaaS 데이터 보호 환경은 빠르게 변화했습니다. 이제 아이덴티티는 Microsoft 365, Entra ID, Azure, Salesforce 및 확장된 SaaS 에코시스템 전반에 걸쳐 주요 액세스 지점으로 기능하며, 공격자들도 이에 맞춰 적응했습니다. 사회공학, 자격 증명 탈취, 그리고 조작된 헬프데스크 워크플로우가 기존 침입 방법을 능가하여, 신원이 환경에서 가장 많이 공격받는 계층이 되고 있습니다. 이러한 전술이 진화함에 따라, 조직들은 Exchange, SharePoint, OneDrive, Teams 및 연결된 애플리케이션 전반의 데이터가 얼마나 빠르게 유출, 변경 또는 삭제될 수 있는지 인식하고 있습니다.

이러한 현실에서 복구 속도가 결과를 좌우합니다. Microsoft 365의 장애는 각각 다른 접근 방식이 필요한 두 가지 범주로 나뉩니다.



일상적인 운영 복구. 누락된 이메일, 손상된 SharePoint 목록, 삭제된 Teams 채널, 오작동된 권한 등은 일상 업무를 중단시키는 사례로, "실행 취소"처럼 즉각적으로 느껴지는 빠르고 정확한 항목 수준 복원이 필요합니다.



전면적인 재해 복구. 테넌트 침해, 광범위한 계정 도용, 대량삭제, 악성 자동화, 플랫폼 중단 — 이러한 이벤트에서는 깨끗하고 변경할 수 없는 복구 지점, 전체 구성 복원, 그리고 전체 워크로드를 자신 있게 복원할 수 있는 역량이 필요합니다.

복구에 사용되는 기술은 중요합니다. 전통적인 내보내기 API는 소규모의 일상적인 수정에 필요한 정확성을 제공하지만, 데이터 이동 속도가 느립니다. 테라바이트 단위의 데이터를 시간당 처리할 수 있는 백업 최적화 API는 엔터프라이즈 규모에서 신속한 복원을 지원합니다. 최신 복원력 전략은 일상적인 작업을 위한 정밀도와 대규모 복구를 위한 처리량이라는 두 가지 요소 모두에 의존합니다.

한편, 운영 환경은 점점 더 복잡해지고 있습니다. 하이브리드 아키텍처, 분산된 팀, 그리고 확장되는 SaaS 포트폴리오는 더 깊은 상호 의존성을 만듭니다. 보존, 감사 가능성 및 사고 대응에 대한 규정 준수 요구가 더욱 엄격해지고 있습니다. ID 중심의 공격은 네이티브 도구가 해결하도록 설계되지 않은 실패 유형을 드러냅니다.

선도적인 엔터프라이즈들은 복원력 프레임워크를 현대화하고 있습니다. 이들은 지능형 위협 탐지, 이상 징후 인식, ID 컨텍스트 보존, 세분성 역할 기반 제어, 보존 기간 연장 등 고급 기능을 포함한 클라우드 네이티브 접근 방식을 도입하고 있습니다. 이러한 기능들은 일상적인 장애와 ID 중심 공격 모두에 효과적으로 대응할 수 있도록 설계되었습니다.

Veeam Data Cloud와 함께하는 SaaS 데이터 복원력

데이터 보호는 복잡하지 않아야 합니다. Veeam Data Cloud를 통해 업계를 선도하는 혁신, 최신 클라우드 네이티브 기술, 내장된 보안이 통합된 단일 클라우드 플랫폼의 역량으로 데이터가 어디에 있든 안전하게 보호하고, 관리하며, 보안을 유지할 수 있습니다.



진정한 복원력 실현:

인텔리전트 자동화, 정책 중심 보호, 정밀하고 신속한 복구를 통해 중단 없는 비즈니스 운영을 보장합니다.



모든 계층에 보안을

내재화: 통합된 제로 트러스트 아키텍처, 강력한 암호화, 데이터 불변성 및 지능형 위협 탐지 기능을 통해 민감한 데이터를 능동적으로 보호합니다.



운영 우수성 추진:

직관적이면서도 강력한 인터페이스로 운영을 간소화하고 총 소유 비용(TCO)을 크게 절감하며 효율성을 높입니다.

중단이 발생한 후에야 준비 상태를 점검하지 마십시오. Veeam Data Cloud를 선택하고, 데이터 복원력 전략이 효율성, 규정 준수 및 비즈니스 연속성을 주도하는 미래를 자신 있게 맞이하십시오.

현대적인 SaaS 데이터 복원력으로 도약하십시오. [veeam.com](https://www.veeam.com)을 방문하여 Veeam Data Cloud가 최신 데이터 보호 전략을 어떻게 혁신할 수 있는지 확인해보십시오.

추가 리소스:

→ [Microsoft 365 백업 서비스의 8가지 이점](#)

→ [Salesforce 복원력 모범 사례 가이드](#)

→ [Microsoft Entra ID 백업의 6가지 이유](#)

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 만드는 데 전념하고 있습니다.

Veeam 솔루션은 데이터 백업, 데이터 복구, 데이터 자유, 데이터 보안, 데이터 인텔리전스를 제공하여 데이터 복원력을 실현하도록 설계되었습니다. Veeam과 함께라면 IT 및 보안 리더는 애플리케이션과 데이터가 클라우드, 가상 환경, 물리 환경, SaaS, 그리고 Kubernetes 환경 전반에서 안전하게 보호되고 항상 사용 가능하다는 사실에 확신을 갖고 안심할 수 있습니다.

Veeam은 시애틀에 본사를 두고 30개국 이상에 지사를 보유하고 있으며, 전 세계 55만여 고객과 글로벌 2000대 기업의 82%를 포함한 고객들이 비즈니스 연속성을 Veeam에 신뢰하고 있습니다. 혁신적인 복원력은 Veeam에서 시작됩니다.

자세히 알아보려면 www.veeam.com을 방문하거나 LinkedIn에서 [@veeam-software](#) 및 X에서 [@veeam](#)을 팔로우하십시오.