DELL Technologies

# 백업 침투: Dell Technologies와 함께 사이버 보안과 회복탄력성 강화

## 핵심 요약

백업 침투는 모든 부문의 비즈니스에 점점 더 큰 위협이 되고 있으며, 중요한 정보를 보호하도록 설계된 시스템의 취약성을 악용합니다. 이러한 공격은 데이터 복구 시스템을 손상시켜 신뢰를 약화시키고 운영을 위험에 빠뜨립니다. 심각한 재정적 손실부터 장시간의 다운타임 및 평판 손상에 이르기까지 심각한 결과가 발생할 수 있습니다.

Dell Technologies는 Dell Trusted Device, Dell Trusted Infrastructure 및 모든 솔루션에 통합된 광범위한 보안 기능을 포함하여 기밀 데이터를 보호하고 이러한 공격을 방지하기 위한 포괄적인 방어 솔루션을 제공합니다. Dell은 전략적 파트너십과 전문 서비스를 추가하여 조직이 백업 침투 인시던트를 효율적으로 탐지, 차단 및 복구할 수 있는 회복탄력성이 뛰어난 다중 계층 보안 프레임워크를 구축할 수 있도록 지원합니다.

Dell Technologies의 혁신적인 솔루션과 전문가 지원을 구현함으로써, 비즈니스는 인프라스트럭처를 보호하고 운영 연속성을 유지할 수 있도록 더 잘 준비할 수 있습니다.

## 백업 침투의 위협 증가

백업 시스템은 비즈니스 연속성에 필수적이며, 랜섬웨어나 하드웨어 장애와 같은 사이버 이벤트 발생 후 복구에 중요한 역할을 합니다. 안타깝게도 이러한 핵심 요소가 점점 더 사이버 범죄자들의 표적이 되고 있습니다. 백업 침투는 백업 데이터를 손상시키거나 삭제하여 가장 필요한 시점에 접근할 수 없게 만듭니다.

이러한 진화하는 위협에는 사전 예방적 조치가 필요합니다. 백업 시스템을 보호하지 못하면 운영이 위태로워지고 기밀 데이터가 노출됩니다. 소규모 비즈니스부터 다국적 기업에 이르기까지 모든 규모의 기업이 잠재적 공격 대상이며, 특히 의료, 금융, 제조 산업이 위험에 노출되어 있습니다.

Dell Technologies는 백업 환경 강화의 시급성을 인지하고, 이러한 정교한 공격에 대응하기 위한 고급 툴과 지침을 제공합니다.

## 백업 침투 공격

백업 침투는 사이버 범죄자가 백업 시스템의 취약성을 악용하여 중요한 복구 데이터를 손상, 파괴 또는 암호화할 때 발생합니다. 이러한 정교한 공격은 랜섬웨어나 멀웨어 배포와 같은 다른 사고와 동시에 발생하거나 후속적으로 발생할 수 있으며, 이는 운영 및 재정적 피해를 증폭시킵니다.

## 백업 공격의 작동 방식

1. **초기 침해:** 공격자는 피싱, 취약한 자격 증명 또는 패치되지 않은 취약성을 통해 네트워크에 무단으로 액세스합니다.
2. **내부 이동:** 네트워크 내부에 침입한 공격자는 툴을 사용해 탐지되지 않은 채로 이동하며, 백업 리포지토리와 중요 데이터 세트를 표적으로 삼습니다.
3. **백업 손상:** 주요 수법으로는 백업 파일 암호화, 복구 시점 삭제 또는 데이터 손상이 있습니다.

## 일반적인 기법

- **자격 증명 도난은** 관리자 계정을 침해하여 백업 시스템에 대한 전체 액세스를 가능하게 합니다.
- **랜섬웨어 배포는** 라이브 데이터와 백업을 모두 암호화하여 암호 해독 대가를 요구합니다.
- **시차 손상은** 탐지를 피하면서 백업을 점진적으로 손상시켜 복구가 필요할 때 비즈니스를 위험에 빠뜨립니다.

이러한 기법은 위협의 정교함과 심각성을 강조하며, 선제적 조치를 요구합니다.

## 비즈니스에 미치는 영향

### 금전적 손실

백업 침투는 복구 비용과 다운타임을 증폭시켜 대응 비용을 2배 또는 3배로 늘리는 경우가 많습니다. 암호화되거나 손상된 백업에서 복구 작업을 시작하려면 공격자에 대한 대가 지불, 새로운 인프라스트럭처 또는 고비용 컨설턴트가 필요할 수 있습니다.

### 운영 중단

실행 가능한 백업이 없으면 조직은 서비스를 중단하고, 프로젝트를 지연하며, 중요 기능을 정지시키는 등으로 인해 긴 복구 시간에 직면하게 됩니다.

### 평판에 미치는 영향

영구적인 데이터 손실 또는 다운타임이 길어지면 이해 관계자의 신뢰가 저하되어 비즈니스의 장기적인 생존력이 손상될 수 있습니다.

## 실제 사례

글로벌 의료 서비스 공급업체는 랜섬웨어 공격 중에 백업이 손상되었음을 발견했습니다. 랜섬 비용을 지불했음에도 불구하고 3주간의 환자 데이터가 영구 손실되어 수술이 지연되고 소송이 제기되었습니다. 총 복구 비용은 **5천만 달러**를 초과했습니다.

## 우려스러운 통계

최근 연구에 따르면 손상된 백업 시스템의 평균 재정적 손실은 벌금, 다운타임 및 복구 비용을 포함하여 **445만 달러**[1]를 초과하는 것으로 추산됩니다. 특히 이러한 인시던트의 빈도가 증가하고 있으며, 전 세계 보고서에 따르면 백업 관련 위협이 전년 대비 **39%** 증가하고 있습니다.

**57%**
의 백업 대상 공격이 백업 리포지토리에 성공적으로 침투함

출처: 2024: Index Engines

1.

## Dell Technologies로 백업 침투에 대응

Dell Technologies는 백업 침투 공격으로 인해 발생하는 고유한 당면 과제를 해결하는 강력한 툴과 서비스 제품군을 제공하여 비즈니스가 효과적으로 예방, 탐지 및 복구할 수 있도록 지원합니다.

### 서버 및 스토리지 보안 솔루션

Dell의 서버 및 스토리지 솔루션은 백업 대상 공격을 막아내는 탁월한 회복탄력성을 제공합니다. 내장된 기능을 통해 백업의 보안을 유지하고 스냅샷이 손상되지 않도록 보장합니다.

- **변경 불가능 백업/스냅샷은** 변조 불가능 복원 시점을 생성합니다.
- **에어 갭 복구는** 라이브 네트워크에서 데이터를 격리하여 손상을 방지합니다.

[1] Ponemon - Cost of a Data Breach Report 2024

### Dell Data Protection 어플라이언스 강화

Dell Data Protection 어플라이언스에는 펌웨어 무결성을 위한 Dell SafeBIOS와 백업 공격으로부터 보호하는 보안 암호화를 위한 SafeData 등의 기능이 내장되어 있습니다. 또한 이러한 솔루션은 MFA(Multi-Factor Authentication), RBAC(Roles-Based Access Control) 및 이중 인증 등의 기능을 통해 위협 행위자를 차단합니다.

### CrowdStrike를 사용한 지능형 공격 탐지

CrowdStrike와 Dell Data Protection의 통합은 다양한 고급 기능을 통해 데이터 보호 환경의 보안 및 모니터링을 강화하는 데 중점을 두고 있습니다.

1. **엔드포인트 및 Data Protection:** Dell은 CrowdStrike의 엔드포인트 보안과 EDR/XDR(Extended Detection and Response)을 Data Protection Solutions와 통합합니다. 여기에는 Dell PowerProtect Data Manager 및 PowerProtect Data Domain의 텔레메트리 수집과 CrowdStrike Falcon 콘솔 및 차세대 SIEM 소프트웨어의 보안 통찰력이 포함됩니다.
2. **모니터링 및 대응:** Dell의 MDR(Managed Detection and Response) 서비스는 고객을 대신하여 CrowdStrike 소프트웨어를 관리하고, 로그를 수집하며, IoC(Indicator of Compromise) 또는 이상 징후 탐지를 조사합니다. 이러한 통합을 통해 Dell은 지속적인 모니터링을 제공하고 고객의 SOC와 협업하여 위협을 신속하고 효과적으로 해결할 수 있습니다.
3. **실시간 가시성 및 데이터 이동 제어:** CrowdStrike Falcon Data Protection 플랫폼은 다양한 소스와 채널의 데이터 이동에 대한 실시간 가시성을 제공하며, 콘텐츠와 컨텍스트별로 데이터를 분류합니다. 이를 통해 콘텐츠와 컨텍스트 분석을 결합하여 데이터 도용을 방지하고 데이터 보호 정책을 효과적으로 시행할 수 있습니다.
4. **통합 관리 및 배포 간소화:** 통합을 통해 단일 플랫폼과 에이전트에서 엔드포인트와 데이터 보호를 모두 관리하여 복잡성과 운영 오버헤드를 줄일 수 있습니다. 이는 CrowdStrike Falcon 플랫폼의 가벼운 클라우드 네이티브적 접근 방식으로 촉진되어 신속 배포와 중단 최소화를 가능하게 합니다.

CrowdStrike와 Dell Data Protection의 통합은 고급 EDR/XDR 기능, 실시간 모니터링 및 포괄적인 데이터 관리를 활용하여 데이터 보호 환경의 전반적인 보안과 회복탄력성을 향상합니다.

어느 선도적인 금융 기관은 최근 PowerProtect Cyber Recovery를 배포하여 침해 발생 시 공격자가 중요 백업 90%에 접근하지 못하도록 방지함으로써 랜섬 비용 지불 없이 원활히 복원 작업을 진행할 수 있었습니다.

### 백업 무결성을 위한 Dell PowerProtect 솔루션

Dell PowerProtect는 불변성, 격리 및 압축을 활용하여 백업 시스템 손상을 방지하는 포괄적인 백업 보호 기능을 제공합니다. PowerProtect는 랜섬웨어 탐지 툴과 통합되어 의심스러운 변경 사항이 발견될 경우 즉각적인 조치를 위한 알림을 제공합니다.

## 다중 계층 보안 접근 방식

데이터를 보호하려면 조율된 다각적 보안 전략이 필요합니다. Dell은 비즈니스가 회복탄력성이 뛰어난 백업 환경을 구축하기 위한 업계 모범 사례를 구현할 수 있도록 지원합니다.

### 방어 기능을 강화하기 위한 주요 단계

- **제로 트러스트 원칙 도입:** 모든 사용자, 디바이스 및 프로세스를 지속적으로 검증하여 무단 액세스에 대한 위험을 줄입니다.
- **모든 백업 암호화:** 전송 중과 저장 중 데이터가 손상되더라도 읽을 수 없도록 보장합니다.
- **직원 교육:** 직원들이 초기 침해로 이어지는 피싱 시도 및 기타 소셜 엔지니어링 전략을 인식할 수 있도록 교육합니다.
- **정기적인 취약성 테스트:** 조직은 정기적인 테스트를 통해 공격자가 취약한 영역을 악용하기 전에 취약한 영역을 식별하고 패치할 수 있습니다.

Dell Technologies는 이러한 관행을 첨단 솔루션과 결합하여 새로운 당면 과제를 해결할 수 있는 강력하고 대응력이 뛰어난 인프라스트럭처를 구축합니다.

## 보안을 강화하는 전략적 파트너십

Dell Technologies는 Microsoft, CrowdStrike, Secureworks와 같은 사이버 보안 선도 기업과 협력하고 있습니다. 각 파트너십을 통해 Dell의 솔루션이 더욱 향상되어 고객에게 지능형 Threat Intelligence, 엔드포인트 모니터링, 포괄적인 대응 전략 등 탁월한 보호 기능을 제공합니다.

## Dell Professional Services 활용

Dell Technologies의 Professional Services는 비즈니스가 복잡한 사이버 보안 문제를 효과적으로 해결할 수 있도록 전문 지식과 지침을 제공합니다. 인시던트 대응 계획 수립부터 제로 트러스트 아키텍처 구현에 이르기까지, Dell Technologies 전문가들은 클라이언트 환경이 백업 침투와 같은 최신 위협에 대한 회복탄력성을 유지하도록 보장합니다.

## Dell과 함께 비즈니스 회복탄력성 구축

Dell Technologies를 채택하면 비즈니스는 운영 연속성을 유지하면서 정교한 공격자에 대비할 수 있습니다. Dell Technologies는 혁신, 파트너십 및 전문 지식을 통해 조직이 가장 심각한 백업 침투 공격도 예방, 탐지 및 복구할 수 있도록 지원합니다.

## 다음 단계 진행

지금 바로 Dell Technologies에 문의하여 비즈니스를 안전하게 보호하십시오. Dell Technologies와 함께라면 고객의 중요한 자산을 보호하고, 평판을 보호하며, 회복탄력적인 미래를 구축할 수 있습니다.

Dell Technologies는 디지털 시대에 대한 신뢰를 높여 조직이 안전하게 운영하고 성공하는 데 필요한 툴, 지식 및 지원을 제공하기 위해 최선을 다하고 있습니다.

백업 회복탄력성은 Dell Technologies와 함께 시작됩니다. 지금 바로 조치를 취하여 미래를 대비는 운영을 구축하고 사이버보안 태세에 대한 신뢰를 구축하십시오.

**Dell.com/SecuritySolutions**에서 오늘날의 주요 사이버 보안 과제를 해결하는 방법을 알아보십시오.

자세한 정보:
Dell의 솔루션

Dell Technologies
전문가에게 문의

추가 리소스_보기

#HashTag로 대화에
참여하기



DELL Technologies