신속하고 강력한 사이버 복구 솔루션으로 데이터 보호 계획 강화

본 연구 결과, Dell Technologies PowerProtect Cyber Recovery는 백업 볼트를 물리적으로 격리하고 랜섬웨어에 대한 심층적인 검사를 제공할 수 있는 것으로 나타났다.

백업 볼트를 위한 물리적 에어 갭 격리

데이터가 통과할 수 없는 물리적 장벽 생성

랜섬웨어에 대한 심층 검사

CyberSense는 메타데이터뿐만 아니라 파일 콘텐츠와 데이터베이스를 살펴본다.

2배 더 많은 이상 징후 워크로드 스캔

단일 툴로 더 많은 곳에서 멀웨어 검색

랜섬웨어 공격으로 인한 평균 비용은 2년 동안 거의 20% 증가한 미화 523만 달러로 증가했다.[1] 효율적인 Cyber Recovery 솔루션은 조직이 인시던트로부터 신속하게 복구하고, 데이터 손실을 줄이고, 다운타임을 최소화하며, 프로세스 중에 브랜드 무결성을 유지하도록 하여 이러한 잠재적인 비용을 줄이거나 발생하지 않도록 지원한다. 솔루션은 공격 후 잘못된 데이터를 찾아내고 복원하여 조직이 중요한 데이터와 시스템을 보호하고 비즈니스 위험과 다운타임을 최소화하는 데 도움이 된다.

Dell PowerProtect Cyber Recovery(Cyber Recovery)가 이러한 솔루션이다. 조직은 랜섬웨어, 파괴적인 사이버 공격 및 예기치 않은 이벤트로부터 데이터와 애플리케이션을 보호할 수 있다. 이 보고서는 공개된 데이터를 사용하여 Cyber Recovery와 경쟁 솔루션인 RSC(Rubrik Security Cloud)의 기본적인 데이터 보호 기능을 대조한다. 특히 복구 볼트, 불변성, 워크로드 지원, 스캔 기술, 복구 가능성, 격리를 포함하여 Cyber Recovery 솔루션 고객이 중요하게 여길 수 있는 기능을 살펴보았다.

RSC와 달리 Cyber Recovery는 다중 복사 접근 방식을 사용한다. 즉, 백업을 생성한 후 이러한 백업(또는 일반적으로 선택한 하위 집합)을 격리된 스토리지에 복사하여 보호 및 분석을 수행한다. Cyber Recovery는 PowerProtect Data Domain 어플라이언스의 온프레미스 또는 소프트웨어 정의 Dell APEX Protection Storage for Public Cloud를 통해 클라우드에 위치한 하나 이상의 스토리지 볼트를 비롯한 여러 구성 요소로 구성된다. 이에 비해 RSC는 로컬 볼트 옵션을 제공하지 않는다. 또한 Cyber Recovery에는 랜섬웨어 공격으로 인한 손상 징후를 확인하기 위해 볼트의 데이터, 파일, 데이터베이스 및 이미지를 스캔하는 완전 자동화된 통합 지능형 보안 분석 엔진인 CyberSense도 포함되어 있다. CyberSense 솔루션은 Rubrik 솔루션보다 2배 더 많은 이상 징후 워크로드를 스캔할 수 있으므로 CyberSense 스캐닝 ML(Machine Learning)이 더 많은 데이터에서 멀웨어 또는 기타 위협 행위자 활동의 영향을 탐지할 수 있다. PowerProtect Cyber Recovery가 어떻게 다르게 작동하며 조직에 더 유리할 수 있는지 살펴보도록 한다.

제품 개요

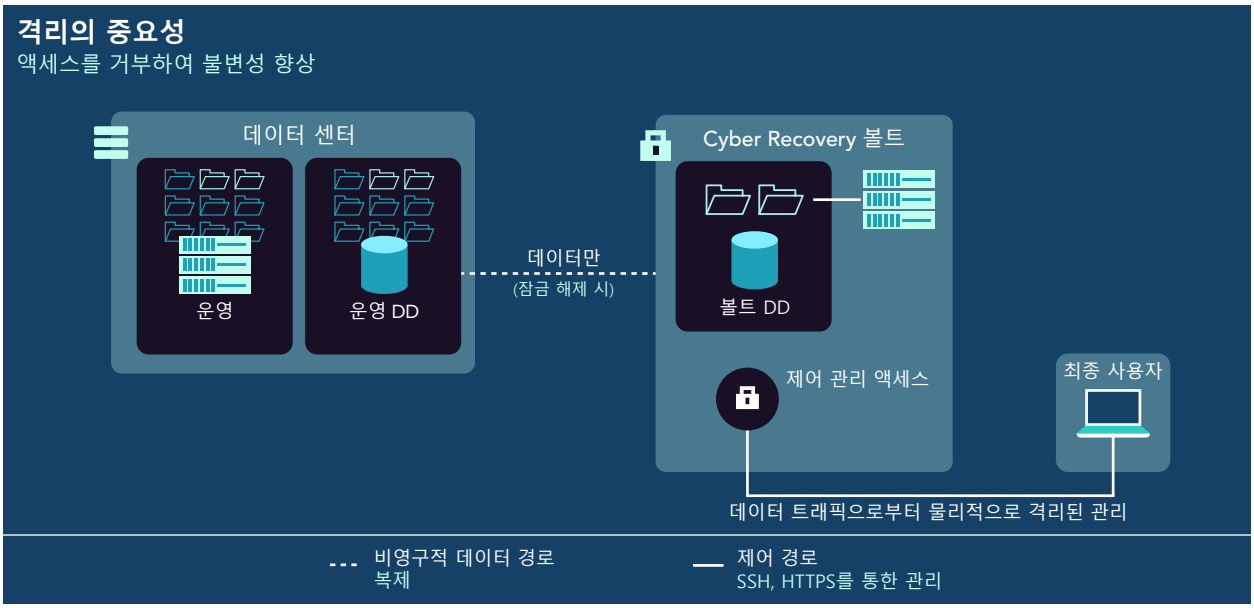
Dell PowerProtect Cyber Recovery 개요

Dell PowerProtect Cyber Recovery는 복제를 위해 볼트에 운영 데이터와 타겟 스토리지 어플라이언스를 저장하는 스토리지 어플라이언스로 구성된다. 또한 동기화를 조정하고, Cyber Recovery 볼트의 PPDD(PowerProtect Data Domain) 시스템에서 여러 데이터 복제본을 관리하고, 복구 프로세스를 감독하고, CyberSense를 통해 분석 프로세스를 감독하는 Cyber Recovery 소프트웨어를 포함한다.

이 솔루션은 MTree 복제를 통해 운영 PPDD MTree에서 볼트 상대방으로 고유한 데이터를 전송하고 설정된 기간 동안 데이터 불변성*을 지원한다. 볼트는 Cyber Recovery 소프트웨어를 포함하는 서버와 백업 애플리케이션과 데이터를 복원하는 구성 요소를 갖추고 있다. 각 Cyber Recovery 볼트에는 일반적으로 이러한 구성 요소가 많이 포함되어 있다. 또한 볼트에는 데이터 분석 소프트웨어가 탑재된 분석/인덱싱 호스트가 포함되어 있어 Cyber Recovery 소프트웨어와 CyberSense를 직접 통합할 수 있다.

*Dell 제품은 중요한 데이터를 보호하려는 고객의 노력을 지원하도록 설계되었다. 다른 전자 제품과 마찬가지로 데이터 보호, 스토리지 및 기타 인프라스트럭처 제품에도 보안 취약성이 발생할 수 있다. 고객은 Dell에서 보안 업데이트를 제공하는 즉시 설치하는 것이 중요하다.

그림 1에는 Dell Cyber Recovery 솔루션 개요가 나와 있다.

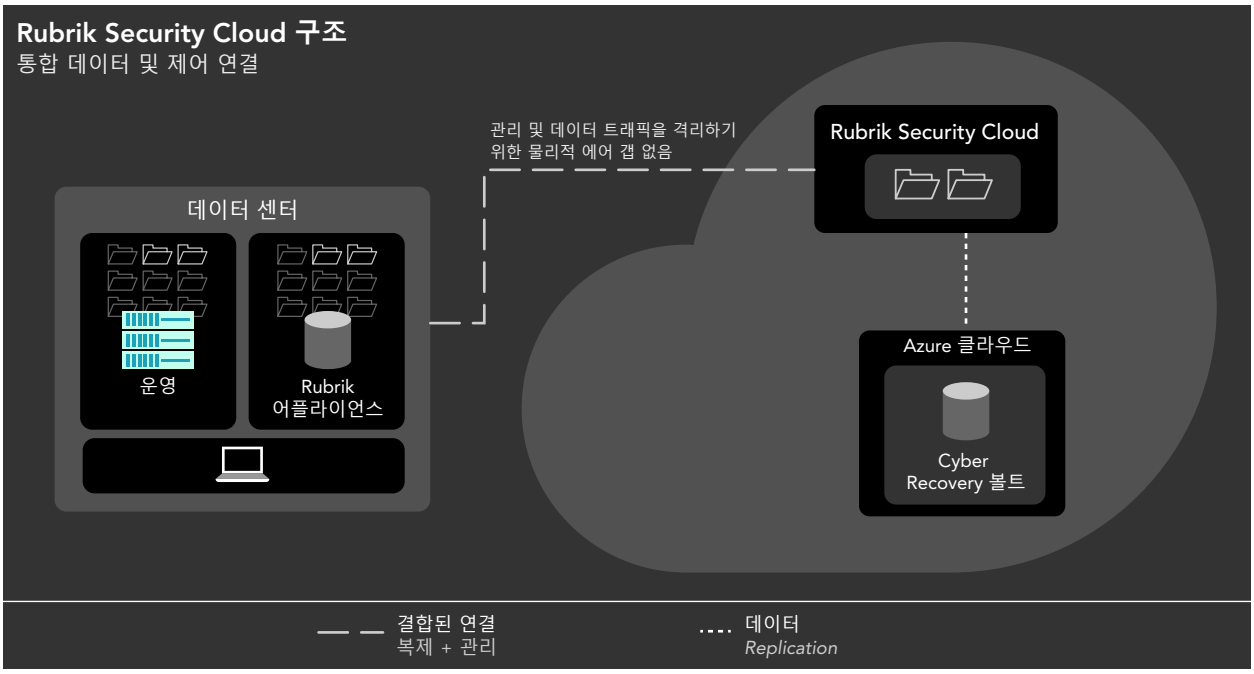


1: Cyber Recovery 볼트의 개략적인 데이터 및 제어 경로 아키텍처이다. 출처: Principled Technologies

Dell PowerProtect Cyber Recovery 솔루션의 주요 구성 요소에 대한 자세한 내용은 Dell PowerProtect Cyber Recovery Solution Guide를 참조하십시오.

Rubrik Security Cloud 개요

Rubrik은 Rubrik Security Cloud를 고객이 '기업 전반, 클라우드, SaaS 애플리케이션에서 데이터를 안전하게 유지하고, 데이터 위험을 모니터링하며, 데이터를 신속하게 복구할 수 있는' SaaS(Software-as-a-Service) 플랫폼으로 설명한다.[4] Rubrik은 "GCP(Google Cloud Platform)에서 실행되는 고가용성 서비스와 인프라스트럭처를 사용하는 보안 마이크로서비스 아키텍처"를 기반으로 솔루션을 구축했다고 말한다.[5] 그림 2는 Rubrik Security Cloud의 일반적인 구조를 보여준다.



2: Rubrik Security Cloud의 일반적인 구조이다. 출처: Principled Technologies

기능 지원

복구 볼트

볼트는 솔루션이 운영 환경 내에서 수행하는 백업의 암호화된 복제본을 보관하는 전용 스토리지이다. 볼트는 운영 백업 솔루션의 일부가 아니며, 각 볼트는 고객이 검증된 백업을 복구할 수 있는 격리된 '백업-백업' 위치의 역할을 한다.

Dell Technologies는 온프레미스, 원격 코로케이션 사이트 또는 퍼블릭 클라우드를 비롯한 여러 볼트 옵션을 제공한다. 온프레미스 볼트는 데이터 센터에 상주하는 운영 에어 갭 PPDD를 활용하며, 이는 백업 솔루션과 동일한 랙 내에서도 가능하다. 에어 갭 솔루션은 보통 프로덕션 환경과 물리적으로 분리되어 있다. 오프사이트 코로케이션 볼트에는 온프레미스 버전과 같은 물리적 볼트에 대한 전용 네트워크 연결이 필요하지만 볼트는 원격 데이터 센터에 지리적으로 분리되어 있다. 또한 Dell은 클라우드 서비스 공급업체인 AWS(Amazon Web Services), Microsoft Azure 및 Google Cloud와 협력하여 퍼블릭 클라우드 내에서 볼트를 제공한다. 퍼블릭 클라우드 볼트는 고객의 요구 사항을 충족하는 구성 유연성을 제공할 수 있다.[6, 7, 8]

Rubrik Cyber Recovery는 Rubrik Security Cloud의 구성 요소이다. SaaS(Software as a Service) 모델을 통해 제공되는 복구 볼트는 Microsoft Azure의 스토리지만 사용한다. 연구에서 확인한 공개된 문서 중 상당수는 Rubrik Cyber Recovery 볼트를 불변성을 제공하는 백업 계층인 Rubrik Cloud Vault와 관계된다.[9'10] 이 볼트는 추가 하드웨어가 필요하지 않으며 Rubrik CDM(Cloud Data Management) 6.02 이상의 모든 버전의 플랫폼에서 사용할 수 있다.

불변성

불변성은 변할 수 없거나 영구적인 상태를 말한다. 불변 백업 및 백업 복제본을 통해 관리자는 할당된 기간이 경과할 때까지 사용자 또는 시스템이 수정하거나 삭제할 수 없는 파일에 대한 영구 기능을 생성할 수 있다. 그러면 파일이 '롤오프'되고 솔루션이 파일을 자동으로 제거한다. 솔루션은 일반적으로 시스템에서 파일을 처리하는 방식을 제어하는 정책 또는 정의를 통해 이 프로세스를 수행한다.[11]

Dell PowerProtect Cyber Recovery 불변성은 Retention Lock 기능을 통해 Retention Lock을 실시하며, 일정 기간 동안 백업 복제본의 삭제 또는 수정 또는 강제 조기 만료를 방지한다. (PPDD는 조직이 Retention Lock을 사용하든 사용하지 않든 추가 전용 파일 시스템으로 작동한다.[12]) Dell 고객은 백업 애플리케이션 대상으로 할당하는 독립적인 보존 설정을 가진 사용자 정의 논리 파티션인 PPDD MTrees를 사용하여 백업을 관리한다.[13] 고객은 거버넌스 및 규정 준수의 두 가지 유형의 보존 잠금 중에서 선택할 수 있다. 규정 준수 잠금은 이 두 가지 중에서 더 엄격하고 안전하다. 고객들은 MTree당 보존 잠금을 설정할 수 있다. 즉, 특정 MTree 내부의 모든 파일은 해당 MTree의 보존 잠금 정의에 따라 동작하고, 파일 당 보존 기간을 설정할 수 있다. 고객이 규정 준수 보존 잠금을 정의하면 사용자 또는 시스템이 이를 제거할 수 없다. 관리자는 덜 엄격한 옵션인 거버넌스 Retention Lock을 되돌릴 수 있다.[14]

Rubrik 솔루션의 불변성은 백업 복제본의 삭제 또는 강제 조기 만료를 방지하기 위해 Retention Lock을 활용한다. PowerProtect Cyber Recovery와 마찬가지로 Rubrik 솔루션은 기존 데이터를 덮어쓰지 않고 파일 시스템에 새 데이터를 추가한다. 이 솔루션은 수신 데이터를 지문으로 처리하고 데이터와 함께 저장한다. **Rubrik 솔루션은 기본적으로 Retention Lock을 활성화하지 않으며** 고객은 Rubrik Support 티켓을 열거나 2인 규칙을 활성화하여 Retention Lock을 허용해야 한다. (Rubrik Cloud Data Management 버전 7.0.1 이전에는 고객이 Rubrik 지원 부서에 문의하여 Retention Lock을 활성화해야 했다. Rubrik 설명서는 고객이 이 작업을 위해 지원 부서에 계속 문의할 수 있는지 여부를 명확하게 안내하지 않는다) 고객이 활성화한 후에는 Retention Lock을 통해 사용자 또는 시스템이 정의된 매개변수 외부의 데이터를 삭제할 수 없다. Rubrik Retention Lock을 사용하려면 시간 동기화를 위해 외부 NTP(Network Time Protocol) 서버가 필요하다. 악성 행위자가 참조 NTP 소스를 조작하여 Retention Lock이 조기에 만료될 수 있기 때문이다.[15]

> *"Rubrik 솔루션은 기본적으로 Retention Lock을 활성화하지않으며 고객은 Rubrik Support 티켓을 열거나 2인 규칙을 활성화하여 Retention Lock을 허용해야 한다."*

라이선스 및 구독

Dell PowerProtect Cyber Recovery는 라이선스가 부여된 솔루션이다. 설치 중에 Dell은 기본적으로 90일 평가판 라이선스를 설치한다. 90일이 지난 후 고객은 새 라이선스를 구입해야 제품을 계속 사용할 수 있다. Dell은 표준(영구) 라이선스와 구독 기반 라이선스를 모두 제공한다.

Rubrik은 Rubrik Cyber Recovery를 RSC(Rubrik Security Cloud)에 통합한다. 고객은 Rubrik Cyber Recovery를 사용하려면 Rubrik Enterprise Edition에 가입해야 한다. 구독 기간은 3년이다.[16, 17] RSC 장애가 발생할 경우 SAP HANA 및 Db2 워크로드에 데이터를 복구하기 위한 타사 툴이 필요하며, 이로 인해 추가 구독 비용이 발생할 수 있다.[18]

관리 액세스

Dell PowerProtect Cyber Recovery 시스템의 관리는 고객이 구축을 위해 선택한 토폴로지에 따라 수행된다. 이 솔루션이 볼트에서 복구를 시작하므로, 관리자들은 볼트의 위치와 관계없이 관리 UI에 로그인하여 작업을 수행할 수 있다. 온프레미스 볼트는 NIST(National Institute of Standards and Technology)에서 권고하는 바와 같이 서비스 거부 공격이나 인터넷 연결을 끊어 데이터를 보호함으로써 사이버 공격으로부터 심각한 손상을 받을 수 있는 인터넷 액세스 없이도 로컬 액세스 권한을 관리자에게 제공한다. 코로케이션 볼트를 사용하면 원격 사이트에서

어플라이언스에 물리적으로 액세스하고 공용 인터넷 외부의 연결을 사용할 수 있다. 클라우드 기반 볼트는 복구를 위해 인터넷 액세스가 필요하므로 사이버 공격이 종료되고 정상적인 네트워크 연결이 재개될 때까지 현장 복구가 지연될 수 있다.

Rubrik Cyber Recovery를 관리하려면 인터넷 액세스가 필요한 Rubrik Security Cloud에 액세스해야 한다. 앞서 언급했듯이 이러한 종류의 연결은 사이버 공격 후 네트워크 기능이 정상으로 돌아올 때까지 현장 복구를 지연시킬 수 있다.

고객이 Rubrik Cyber Recovery 기능을 사용하려면 RSC에 액세스할 수 있어야 하므로 RSC는 단일 장애 지점이 된다. 해당 서비스가 사용 불가능해지면 영향을 받은 고객의 볼트에서 복구할 수 없게 된다. Rubrik은 RSC 서비스 중단 중에 10개의 워크로드를 복구할 수 있지만, 2개의 데이터베이스 워크로드를 복구하려면 타사 툴과 Rubrik Support의 도움이 필요하다.[19' 20] 또한 손상된 관리자 계정이나 RSC 플랫폼에 대한 액세스 권한이 있는 악성 행위자는 단일 볼트가 아닌 전체 자산에 대한 액세스 권한을 얻는다.

Dell Technologies의 Managed Detection and Response에 대한 추가 지원 받기

일부 조직은 사이버 보안을 '혼자 해결하는' 접근 방식에 익숙하지 않을 수 있다. Dell은 이러한 고객에게 위협 및 위험을 모니터링 및 탐지하고 고객과 협력하여 이러한 위험을 완화하는 완전 매니지드 서비스인 MDR(Managed Detection and Response)을 제공한다. Dell에 따르면 이 서비스는 다음을 제공한다.[21]

- Dell이 지원하는 XDR(Extended Detection and Response) 보안 분석 플랫폼의 배포 및 구성에 대한 전문가의 조언을 비롯한 신뢰할 수 있는 지원
- 분기당 최대 40시간의 서비스 관련 보안 구성을 포함한 위협 대응 및 보안 구성
- 24/7 탐지 및 조사(각 고객의 환경에 맞춰 보안 시스템을 회피하는 새로운 위협 또는 이미 알려졌지만 변형된 위협을 발견하는 사전 예방적인 위협 추적 포함)
- 사이버 인시던트에 대한 즉각적인 대응을 가능하게 하는 연간 40시간의 원격 인시던트 대응 지원을 포함하여 조사를 신속하게 시작할 수 있는 초기 대응의 개시

APEX Cyber Recovery Services와 결합된 MDR을 통해 고객은 다양한 옵션 중에서 선택하여 위협과 위험을 모니터링, 탐지 및 완화할 수 있다. 옵션이 존재한다는 사실은 조직의 요구에 맞는 적용 범위나 하이브리드 접근 방식을 확장할 수 있음을 의미한다.

MDR에 대한 자세한 내용은 **https://www.dell.com/en-us/dt/services/managed-services/managed-workplace-services/managed-detection-response.htm**에서 확인 가능하다.

원활한 운영

설정

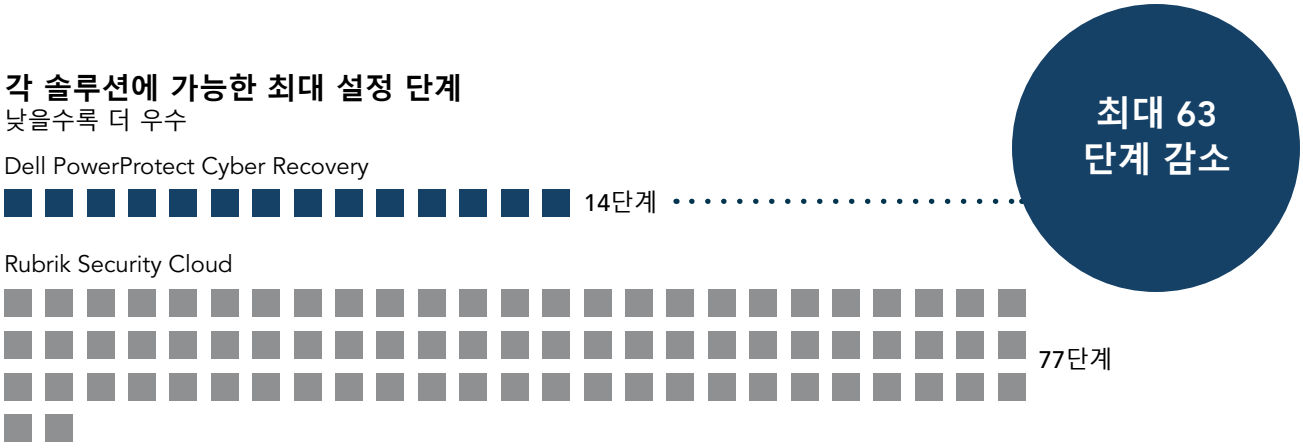
Dell PowerProtect Cyber Recovery 설정은 Linux 시스템에 소프트웨어를 설치하거나®® OVF(Open Virtualization Format) 템플릿에서 VMware vSphere 어플라이언스를 생성하는 작업으로 구성된다. 소프트웨어를 설치하려면 14단계가 필요하지만[22] 대체 vSphere 어플라이언스 배포에는 8단계가 필요하며 5분이 소요된다.[23] 설치 후 관리자는 격리된 환경 내에서 웹 브라우저를 통해 솔루션에 액세스할 수 있다.

고객은 완전히 자동화되고 통합된 지능형 보안 분석 엔진인 CyberSense를 별도로 배포해야 한다.[24] Dell PowerProtect Cyber Recovery에 CyberSense를 설치하는 지침은 공개적으로 제공되지 않는다.[25]

Dell은 DDO(Destruction Detection Objective), DAO(Destruction Assessment Objective), CRP(Cyber Recovery Point), CRT(Cyber Recovery Time), Cyber Recovery 동기화 간격 및 Cyber Recovery 데이터 복제 수를 비롯하여 사용자가 조정할 수 있는 다양한 지표를 보유하고 있다. 또한 보호가 필요한 데이터의 특성을 파악하는 것이 좋다. 이 데이터는 핵심 인프라스트럭처 서비스 또는 기타 애플리케이션에 따라 미션 크리티컬, 비즈니스 크리티컬 또는 애플리케이션 바이너리, 부팅 이미지 및 백업 카탈로그와 같은 일반 데이터일 수 있다. 다양한 옵션을 통해 고객은 백업 환경을 완벽하게 제어하고 데이터 분류를 맞춤 구성할 수 있다. Dell Consulting Services는 추가 지원과 제안을 제공할 수도 있다.[26]

Rubrik 설정도 여러 단계로 구성된다. 클러스터를 생성하기 전에 Rubrik 지원 서비스는 Rubrik CDM을 설치하고 구성해야 한다. 그런 다음 관리자는 최신 또는 원하는 CDM 버전을 다운로드하여 설치한다(15단계).[27] 그런 다음 관리자는 UI 또는 CLI를 사용하여 Rubrik 클러스터를 설정할 수 있다. UI 또는 CLI를 사용하여 클러스터를 설정할 수 있으며, 두 방법 모두 24단계를 거친다.[28] [29] 그런 다음 관리자는 온라인 방법(12 단계)[30] 또는 오프라인 방법(18 단계)을 사용하여 Rubrik 클러스터를 등록할 수 있다.[31] 그런 다음 관리자는 13단계를 거쳐 MFA(Multi-Factor Authentication)를 활성화한다.[32] 마지막으로 관리자는 초기 계정(6단계) 및 다른 계정을 추가한다.[33] 그림 3은 각 Cyber Recovery 솔루션을 설정하는 가능한 최대 단계 수를 보여준다.

Rubrik 고객은 다른 지표를 조정할 수 없으므로 요구 사항을 충족하는 유연성이 떨어질 수 있다. 한 리뷰어는 "대부분의 사용자 인터페이스는 직관적이고 쉽지만, 일부 지역에서는 해당 옵션의 용도 설명이 부족하거나 옵션이 누락되어 있다"라고 주장했다. 그리고 "사용자 경험을 쉽게 만드는 동안 조정 가능 요소가 다수 존재하지 않으며 지원 담당자가 고객 환경을 변경하기 위해서는 지원 터널을 열어야 한다."라고 하였다.[34]



3: Dell PowerProtect Cyber Recovery와 Rubrik Security Cloud를 설정하기 위해 필요한 최대의 단계 수는 얼마나 됩니까? 낮을수록 더 우수. 출처: Principled Technologies

유지 보수

설정 후 일상적인 유지 보수 작업을 수행하기 위한 Dell 및 Rubrik UI가 유사하다는 것을 확인했다. 구성 후 고객은 다음을 수행하도록 Dell PowerProtect Cyber Recovery를 구성할 수 있다[35., 36]

- 스케줄에 따라 수동 사용자 요청에 대한 응답으로 Cyber Recovery 작업 보고서를 자동으로 생성한다.
  - 사용자 또는 스케줄은 정책, 복구 작업, 시스템 백업 또는 정리 작업을 시작할 때 작업을 생성한다.
- 볼트 상태, 스토리지 용량, Cyber Recovery 운영, 복사/동기화 실패 또는 Cyber Recovery 볼트 다운 알림, Cyber Recovery 작업을 모니터링한다.
- 공격을 지속적으로 자동 검사한 다음 심각도 순서대로 CyberSense 알림을 표시하여 파일 수, 호스트, 관련 정책, 탐지된 특정 위협, 공격 시점 등을 파악하여 정리 백업을 찾고 공격 분석에 사용할 손상된 파일 목록을 제공한다.

마찬가지로 고객은 Rubrik이 다음을 수행하도록 구성할 수 있다.[37]

- Rubrik Security Cloud를 자동으로 사용하여 연결된 모든 Rubrik 클러스터의 모든 이벤트를 추적, 모니터링 및 표시한다. 세 가지 이벤트 유형을 제공한다.[38]
  - 위험 - 백업, 아카이브 또는 복제 실패 등 주의가 필요한 이벤트
  - 경고 - 백업, 아카이브 또는 복구가 완료됨
  - 정보 - 참고용
- 솔루션이 마지막으로 스냅샷을 생성한 시간, 이벤트 타임라인, 탐지 시간, 변경된 파일 수, 의심스러운 파일 수, 클러스터 이름, 오브젝트 유형 및 이름을 제공하는 Threat Monitor를 사용하는 신규 및 기존 손상 지표에 대한 스냅샷을 지속적으로 자동 스캔한다.

이상 징후 워크로드 지원

Rubrik Security Cloud Data Threat Analytics와 CyberSense는 모두 여러 워크로드 유형을 검사하지만, 출처에 따르면 CyberSense는 이상 징후 탐지 워크로드를 두 배 더 지원한다. 여기에는 다음과 같은 유형의 워크로드를 스캔하는 작업이 포함된다.

- VM
- 핵심 인프라스트럭처
- 문서, 계약 및 지적 재산이 포함될 수 있는 사용자 파일
- 데이터베이스
- 다른 클라이언트가 수행한 백업

"공개적으로 사용 가능한 데이터에서 지원되는 워크로드 수를 계산하면 CyberSense는 21개의 이상 징후 탐지 워크로드를 지원하지만 Rubrik은 7개를 지원한다."

공개적으로 사용 가능한 데이터에서 지원되는 워크로드 수를 계산하면 CyberSense는 21개의 이상 징후 탐지 워크로드를 지원하지만 Rubrik은 7개를 지원한다. 따라서 공개적으로 제공되는 데이터에 따르면 CyberSense는 Rubrik Security Cloud Data Threat Analytics보다 2배 더 많은 워크로드를 지원하는 것으로 나타나고 있다. 사이버 복구 솔루션이 스캔할 수 있는 데이터가 많을수록 교묘한 멀웨어나 기타 손상을 발견할 가능성이 높아진다.

VM 워크로드 지원

VM 워크로드란 물리적 호스트 서버 또는 클라우드 환경에서 VM이 실행하는 애플리케이션, 서비스 또는 작업을 말한다. 이러한 워크로드는 기능 및 멀웨어에 대한 노출을 증가시킬 수 있는 기타 방법마다 다양할 수 있으므로 VM 스캔이 필수적이다. Rubrik Security Cloud Data Threat Analytics는 이상 징후 탐지, 위협 모니터링, 위협 추적 및 보호된 리소스에 대한 데이터 복구 서비스를 제공하는 클라우드 기반의 보안 솔루션으로,[39] 다음 VM 워크로드의 스캔을 지원한다.[40]

- VMware
- Nutanix® AHV
- Microsoft Hyper-V
- Microsoft Azure

CyberSense는 다음 VM 워크로드의 검사를 지원한다[41. 42, , 43]

- VMware
- AWS(Amazon Web Services)
- Hyper-V에서는 Dell Avamar 나 Dell NetWorker와 같은 백업 솔루션을 사용할 수 있다.

VMware는 "가상화된 워크로드의 80%가 VMware 기술에서 실행된다"고 주장한다.[44] 2024년 1분기에는 클라우드 인프라스트럭처 서비스 시장에서 가장 인기 있는 공급업체인 AWS(Amazon Web Services)가 전체 시장의 31%를 장악했다. Microsoft Azure는 25%의 시장 점유율로 2위를 차지했다.[45]

핵심 인프라스트럭처

핵심 인프라스트럭처는 기술 환경의 운영을 지원하는 기본 구성 요소이자 서비스이다. 핵심 인프라스트럭처 기능은 많은 시스템과 사용자에게 영향을 미칠 수 있으므로 이 수준에서 멀웨어를 탐지하면 공격의 심각도를 줄일 수 있다. Rubrik Security Cloud 문서에는 모든 핵심 인프라스트럭처 스캔에 대한 지원이 언급되어 있지 않는다.[46]

반면 CyberSense는 다음과 같은 핵심 인프라스트럭처의 스캔을 지원한다.[47]

- Active Directory
- DNS
- LDAP

문서, 계약 및 지적 재산이 포함될 수 있는 사용자 파일

Rubrik Security Cloud Data Threat Analytics는 다음 사용자 파일 검사를 지원한다.[48]

- NAS 파일 세트 및 데이터 세트
- Windows 볼륨 그룹
- Linux 및 Windows

CyberSense는 Linux 및 Windows 사용자 파일을 검사할 수 있다.[49]

데이터베이스 스캔

CyberSense 7 대비
RSC 데이터 위협 분석 0

데이터베이스

애플리케이션은 여러 가지 이유로 다양한 유형의 데이터베이스를 사용할 수 있으므로 다양한 데이터베이스에서 멀웨어의 존재를 탐지할 수 있는 능력은 신속한 대응에 매우 중요할 수 있다. Rubrik Security Cloud Data Threat Analytics는 데이터베이스를 백업할 수 있지만 데이터베이스 백업을 검사할 수 있는 공개 문서를 찾지 못했다.

CyberSense는 페이지 수준 스캔을 통해 다음과 같은 데이터베이스를 스캔할 수 있도록 지원한다.[50]

- SQL
- PostgreSQL
- Oracle®
- Epic® Caché
- SAP HANA
- MariaDB/MySQL
- Db2

다른 클라이언트가 수행한 백업

일부 조직은 이중화를 제공하거나 규정을 준수하거나 기타 중요한 이유를 위해 여러 공급업체의 데이터 백업을 보유하고 있을 수 있다. Rubrik Security Cloud 설명서에는 다른 백업 클라이언트에서 수행한 백업 스캔에 대한 지원이 언급되어 있지 않는다.[51]

이 범주에서 명확한 이점을 제공하는 CyberSense는 다음 백업 클라이언트에서 만든 백업 검사를 지원한다.[52' 53' 54]

- DNAS
- SQL
- NetWorker
- Veritas NetBackup
- 교환
- Avamar
- CommVault

스캐닝 기술

Rubrik Security Cloud에는 Data Threat Analytics에서 스캔하는 데 도움이 되는 많은 툴이 포함되어 있다.

- Rubrik Anomaly Detection은 고객이 스냅샷 조사에 연구하고 사용할 수 있도록 의심스러운 파일, 스냅샷 변경 사항[55] 및 이상 징후 세부 정보를 이상 징후 인시던트로 표시한다.[56] 이 소프트웨어는 복구 옵션도 제공한다.[57]
- Rubrik VM Encryption Detection은 VMware vSphere 가상 디스크 파일에 대한 공격을 탐지한다.[58]
- Rubrik Threat Monitoring은 탐지된 위협 및 일치 항목에 대한 정보를 표시한다.[59]
- Rubrik Threat Hunt는 손상 지표에 대한 사용자 개시 스캔 기능이다.[60]
- Rubrik Quarantine은 위협 추적에 표시되는 오브젝트를 격리한다.[61]

Rubrik RSC에는 각 Rubrik 클러스터에 대한 Rubrik Backup Service 커넥터도 있다.

Rubrik 고객은 작업에 적합한 툴을 선택해야 하며, 수동으로 스캔을 시작하거나 여러 툴을 사용하여 작업을 수행해야 할 수 있다. 반면, Dell Technologies는 단일 CyberSense 검사 옵션을 제공하므로 고객은 이를 보다 쉽게 관리하고 관리할 수 있다.

CyberSense는 Rubrik RSC Data Threat Analytics의 표면 전용 검사보다 더 심층적으로 데이터 위협을 감지할 수 있다. CyberSense는 파일의 전체 콘텐츠 검사와 데이터베이스의 페이지 수준 검사를 수행하고 파일의 부분 암호화를 탐지할 수 있다.[62] 이 툴은 수천 개의 데이터 위협에 대해 Index Engines에서 학습한 ML(Machine Learning) 데이터베이스를 사용하며 200개 이상의 분석 지점을 포함하여 데이터 손상을 탐지한다.[63] Rubrik Threat Monitoring 및 Threat Hunt와 달리 CyberSense는 멀웨어 서명을 제공하기 위해 외부 위협 인텔리전스 기관에 의존하지 않는다. 대신 새로운 위협을 발견한다.[64] **또한 CyberSense는 허용되는 파일 변경의 임의의 임계값이나 거짓 음성을 초래할 수 있는 스냅샷 간의 엔트로피 수준에 의존하지 않으며,** ML을 이전 고객 행동의 기준에 맞춰 학습시키지도 않는다.[65, 66, 67]

> *"또한 CyberSense는 허용되는 파일의 임의의 임계값에 의존하지 않는다. 스냅샷 간의 변경 또는 엔트로피 수준으로 인해 거짓 음성이 발생할 수 있다...."*

Rubrik 이상 징후 탐지 소프트웨어는 콘텐츠 분석을 수행하기 전에 메타데이터에만 의존하여 스냅샷이 손상되었는지 확인한다. CyberSense의 지속적인 ML과 비교하는 과정에서 Rubrik 소프트웨어는 서명을 얻은 후 손상을 발견한다. Rubrik 이상 징후 탐지 기능의 경우 고객의 정상 기준을 정의하기 위해서는 동작 모델을 구축해야 한다. 이렇게 하려면 여러 번의 백업이 필요할 수 있다. Rubrik 동작 모델은 공격이 없을 때 파일 시스템에 대한 일반적인 변경 사항의 기준을

생성하기 위해 최소 2개의 백업이 필요하다. 그러나 변경 통계 한 세트만으로는 일반적인 사항을 파악하는 데 충분하지 않을 수 있다. 비즈니스 이벤트는 첫 번째 Rubrik 스냅샷과 두 번째 Rubrik 스냅샷 사이에 발생하지 않은, 더 많거나 더 적은 활동 또는 더 의심스러운 유형의 활동을 트리거할 수 있다. Rubrik 솔루션이 분석하는 백업이 많을수록 행동 모델을 기준에 맞게 더 정확하게 학습시킬 수 있다.[68, 69]

CyberSense는 볼트에 모든 분석 데이터를 보관하고 있다. Rubrik은 파일 시스템 동작 분석 파이프라인에서 고객 파일 시스템 변경 사항에 대한 메타데이터를 클라우드 기반 Polaris 플랫폼으로 전송하여 동작 분석을 수행함으로써 공격 노출 지점을 개방한다.[70]

고객은 Rubrik Threat Monitoring 및 Threat Hunt를 Rubrik Enterprise 에디션의 일부로만 사용할 수 있다.[71] 고객은 RBAC(Role-Based Access Control) 권한으로 Threat Hunt 스캔을 수행해야 하며, 사용자는 어떤 IOC(Indicators of Compromise)를 추적할지 표시해야 한다.[72] 이는 업계 모범 사례에 해당하지 않는다.[73] CyberSense와 마찬가지로 Threat Hunt는 VMware, AHV, Hyper-V, NAS 파일 세트, Linux 및 Windows 서버를 지원한다.[74]

다음 섹션에서는 Rubrik 솔루션이 위협 탐지를 제공하는 방법에 대해 자세히 설명한다.

메타데이터 및 파일 시스템 통계

Rubrik Anomaly Detection ML 동작 모델은 마지막 스냅샷 이후 파일 시스템의 변경 사항(예: 추가, 삭제 또는 이동된 파일 수)을 메타데이터로 기록한다.[75] 그런 다음 ML 모델은 이러한 변경 사항을 학습하여 파일 시스템에 대한 동작 모델 "기준"을 구축한다. Rubrik은 스냅샷에서 너무 많은 변화가 있을 경우 이를 이상한 것으로 표시한다. 동작 분석이 스냅샷에 플래그를 지정하면 솔루션이 파일 콘텐츠 분석을 시작한다.[76] 메타데이터를 모니터링하면 보안 계층이 추가될 수 있지만 이벤트로 인한 다운타임을 방지하거나 줄이는 데 도움이 되는 필수 보호 기능을 제공하지 못할 수 있다.

> *"CyberSense는 기준선이 필요하지 않으며 첫 번째 백업 복제본의 파일 및 데이터베이스 콘텐츠 변경 사항을 모니터링하고 분석한다."*

반대로 **CyberSense는 기준이 필요하지 않는다. 첫 번째 백업 복제본의 파일 및 데이터베이스 콘텐츠 변경 사항을 모니터링하고 분석한다.** CyberSense 접근 방식은 소프트웨어가 파일의 일부나 데이터베이스의 페이지까지도 분석하여 더 세밀한 정보를 제공한다. Rubrik 솔루션과 마찬가지로 CyberSense 스캔에는 메타데이터 속성이 포함되며 ML 엔진에 결과를 제공한다. Rubrik 솔루션과 달리 CyberSense는 메타데이터 검사에만 국한되지 않으며 Index Engine은 서명이나 이전 고객 행동이 아닌 Index Engine에서 문서화한 공격에 대해 ML 엔진을 학습시켰다.[77, 78]

임계값

동작 분석 중에 Rubrik ML은 파일 시스템에서 이상 징후가 발생할 가능성을 결정한다. Rubrik 솔루션은 가능성이 높은 경우 콘텐츠 분석을 수행한다. 이는 "비정상적인 동작"에 대한 행동 모델에서 결정된 임계값일 수 있다. 예를 들어, Rubrik 솔루션은 많은 새 파일이나 수정된 파일을 보거나 임의 또는 암호화 표시기가 증가할 때 비정상적인 동작을 플래그할 수 있다.[79] 콘텐츠 분석 중에 Rubrik Anomaly Detection은 파일 콘텐츠의 변경 사항을 표시하고 파일 시스템의 엔트로피를 계산하여 암호화 확률을 계산한다. 파일 시스템의 엔트로피는 랜섬웨어 공격으로 인해 파일이 암호화될 가능성을 보여 준다. 엔트로피가 이상 징후 임계값을 초과하면 솔루션에서 사용자에게 알림을 보낸다.[80, 81] 데이터 손상을 감지하는 효율성은 임계값 엄격성에 따라 달라진다. 너무 많은 허용은 거짓 음성을 일으켜 안정성에 대한 잘못된 인식을 유발할 수 있다.[82] 고객은 임계값을 적절하게 설정해야 한다.

반면에 (Dell 및 Index Engines에 따르면) CyberSense는 데이터 손상 탐지에서 99.99%의 신뢰도를 제공하기 위해 파일 콘텐츠를 스캔하여 파일의 부분 암호화를 확인한다.[83]

서명 및 파일 확장명

Rubrik Threat Monitoring 및 Threat Hunts는 IOC에 대한 스냅샷을 스캔한다. Rubrik이 모니터링하는 여러 위협 인텔리전스 소스 중 하나가 새로운 IOC를 발견하면 Threat Monitoring은 새로운 멀웨어(멀웨어 시그너처라고도 함)를 식별하기 위한 YARA(Yet Another Ridiculous Acronym) 규칙이 포함된 위협 피드를 모든 Rubrik 클러스터로 푸시한다. 그런 다음 클러스터가 스캔을 시작한다.[84] 최근 WatchGuard 보고서에 따르면 멀웨어의 57.8%가 서명 탐지를 방지한다고 한다. BianLian과 같은 고급 멀웨어는 서명 인식을 회피하는 방법을 사용할 수 있으며 새로운 멀웨어 변종은 원본과 약간 다른 서명을 가질 수 있다. 따라서 위협 인텔리전스를 최신 상태로 유지하는 것이 더 어려울 수 있다.[85]

이에 비해 CyberSense는 200개 이상의 분석을 사용하고 수천 가지 랜섬웨어 변종에 대해 학습된 ML 모델을 제공한다. Index Engines는 CyberSense 메서드가 서명을 다운로드하지 않고도 이전에는 볼 수 없었던 정교한 변형을 탐지할 수 있음을 입증했다.[86] 이는 이벤트 중에 인터넷에 의존하지 않을 때 누릴 수 있는 또 다른 장점이다.

대량 암호화 이벤트

Rubrik 솔루션은 전체 파일 시스템의 엔트로피를 계산하여 대량 암호화 이벤트를 모니터링한다.[87] CyberSense는 훨씬 더 세분화되어 있다. 파일 시스템 또는 각 개별 파일만을 검사하지 않는다. 대신 파일의 내부 내용의 조각을 스캔한다. Index Engines에 따르면 파일의 일부가 아닌 전체 파일에 대해서만 엔트로피를 계산하면 '전체 파일의 극단적인 암호화만 감지'하거나 대량 암호화 이벤트를 감지한다.[88]

복구 성능

설명서에 따르면 Dell PowerProtect Cyber Recovery를 사용한 복구는 Rubrik을 사용한 복구보다 더 쉽고 효율적인 프로세스라고 판단한다. 이 보고서의 이 부분에서는 두 솔루션의 복구 기능과 그 기능을 구현하는 방식을 대조적으로 비교한다.

Rubrik 설명서에는 어떤 복구 기능이 어떤 VM 유형에 대해 작동하는지 기록되어 있다. 유용한 수준의 세분성을 제공하는 것처럼 보일 수 있지만 많은 규정 및 변형으로 인해 복구가 복잡해진다. 예를 들어 Rubrik 고객이 데이터, 파일 및 시스템을 복구해야 하는 경우 복구 계획에 포함할 스냅샷 객체를 선택해야 한다. Rubrik에서는 하나 이상의 복구 계획을 생성한 후 다음과 같은 다양한 복구 가능성 옵션을 제공한다.[89, 90, 91, 92, 93]

- 다운로드 또는 덮어쓰기를 통해 파일을 복구하고 별도의 폴더로 복구하거나, 다른 호스트로 내보내거나, 클러스터링된 서비스로 내보낸다.
- 다운로드 또는 덮어쓰기를 통해 VM용 파일을 복구하고 별도의 폴더로 복구하거나 다른 가상 머신으로 내보낸다.
- 다음과 같은 방법으로 VM 또는 디스크 스냅샷의 완전한 복구를 수행할 수 있다.
  - 라이브 마운트. 스냅샷에서 새 VM을 생성한다.
  - 가상 디스크 마운트. 스냅샷을 기반으로 새로운 가상 디스크를 생성한다.
  - 인스턴트 복구. 현재 VM을 스냅샷에 의해 생성된 새 VM으로 대체한다.
  - 내보내기. 선택한 데이터 저장소의 스냅샷에서 새 VM을 생성한다.
  - VM의 배치 복구
- 라이브 마운트 및 내보내기를 통한 복구 계획용 대량 Cyber Recovery
- Rubrik Security Cloud는 격리된 샌드박스, 원격 사이트 또는 현재 위치로 VM 재해 복구를 위한 애플리케이션 복구를 오케스트레이션했다.

Rubrik Batch Recovery에서는 더 복잡성이 나타난다. 표 1은 하이퍼바이저에 따라 Rubrik이 제공하는 배치 복구 기능을 보여준다.[94]

1: Rubrik은 다양한 하이퍼바이저에 대한 배치 복구 기능을 제공한다. 출처: Rubrik.

VM 생성 옵션				
	라이브 마운트	**라이브 마운트(마이그레이션은 선택 사항)**	**내보내기**	**인스턴트 복구**
vSphere VMs	사용 가능, Rubrik 클러스터를 데이터 저장소로 사용	사용할 수 없음	사용 가능, 복구된 하이퍼바이저의 데이터 저장소 사용	사용 가능, Rubrik 클러스터를 데이터 저장소로 사용
AHV VMs	사용 가능, Rubrik 클러스터를 데이터 저장소로 사용	사용 가능, Rubrik 클러스터를 데이터 저장소로 사용하고 모든 후속 쓰기에 Nutanix 컨테이너 사용	사용 가능, Nutanix 컨테이너를 데이터 저장소로 사용	사용할 수 없음
Hyper-V 가상 머신	사용 가능, Rubrik 클러스터를 데이터 저장소로 사용	사용할 수 없음	사용 가능, 복구된 하이퍼바이저의 데이터 저장소 사용	가용, 현재 VM을 새로 생성된 스냅샷에서 가져온 새로운 VM으로 대체 Rubrik 클러스터를 데이터 저장소로 사용한다.

Rubrik 솔루션의 경우 복구된 데이터 저장소는 일반적으로 운영 환경이 아닌 Rubrik 클러스터에 있으므로 문제가 발생할 수 있다. 다음 섹션에서 이러한 문제를 다룬다("Rubrik limitations"). 반면 PowerProtect는 복구된 데이터를 복구 또는 운영 환경에 배치하여 다운타임을 최소화할 수 있는 더 빠르고 원활한 복구를 제공할 수 있다.

표 2는 vSphere VM 복구에 대한 Rubrik의 추가 정보를 보여준다.[95] 표에서 볼 수 있듯이 대부분의 vSphere 복구 데이터 저장소는 Rubrik 클러스터에 있다.

2: Rubrik이 vSphere VMs에 제공하는 복구 기능 출처: Rubrik.

Rubrik이 vSphere에 제공하는 복구 기능				
Action	**데이터 저장소**	**전원 상태**	**네트워크**	**소스 VM**
파일 복구	해당 사항 없음	적용되지 않음	적용되지 않음	영향 없음
라이브 마운트	로컬 Rubrik 클러스터	켜기 또는 끄기	연결 해제됨	영향 없음
가상 디스크 마운트	로컬 Rubrik 클러스터	켜짐	연결 해제됨	영향 없음
인스턴트 복구	로컬 Rubrik 클러스터	켜짐	연결됨(선택 사항)	전원이 꺼지고 이름이 변경됨
내보내기	하이퍼바이저 데이터 저장소	Off	연결 해제됨	영향 없음
현재 위치 복구	하이퍼바이저 데이터 저장소	켜짐	소스 VM과 동일	현재 위치 복구에서는 스냅샷에서 가져온 가상 디스크 데이터를 소스 VM의 가상 디스크 파일에 덮어쓰는 방식으로, VM의 속성은 변경되지 않는다.

Rubrik 솔루션은 대량 복구를 광범위하게 구현하지 않으며 대량 복구 옵션은 제한적이고 복잡하다. 이 보고서의 "Dell PowerProtect Data Manager offers the equivalent of Rubrik "mass restore"" 섹션에 자세히 설명되어 있듯이 Dell PowerProtect는 효율적이고 단순하다.

대량 복원 해제

Rubrik은 대량 복구를 홍보하고 있다. 이를 통해 대규모로 앱, 파일 또는 사용자를 복구하여 비즈니스 운영을 빠르게 회복할 수 있다.[96] 아울러 많은 대량 복구 옵션을 제공한다. 그러나 Rubrik 솔루션은 일반적으로 복구된 데이터를 운영 환경이 아닌 Rubrik 클러스터에 저장한다.[97] 워크로드는 솔루션이 마이그레이션을 완료할 때까지 Rubrik 시스템의 가용성에 따라 달라진다. 로컬 Rubrik 클러스터는 계층 3 스토리지이므로 고객은 계획된 성능 수준으로 돌아가려면 운영 환경으로 추가 마이그레이션을 수행해야 한다. 시스템이 마이그레이션을 완료하는 동안 이러한 단일 장애 지점과 성능 저하로 인해 Rubrik 솔루션이 워크로드를 운영 환경으로 복원할 때까지 복구가 완료된 것으로 간주할 수 없다.

또한 Dell PowerProtect는 사용자가 복구 UI에서 복구할 여러 VM을 선택할 수 있도록 하여 대량 복구를 제공한다.

Dell PowerProtect Data Manager는 Rubrik "대량 복원"과 동등한 기능을 제공한다.

Rubrik 솔루션과 비교하여, Dell 솔루션은 vSphere VM에 대한 여러 유사한 복구 방법을 제공하고 있다. Dell PowerProtect는 복구 또는 운영 환경에 VM 데이터를 배치할 수 있다. 대부분의 Rubrik 옵션은 데이터를 Rubrik 클러스터에만 배치한다. 표 3은 Dell 복구 옵션을 보여준다.[98, 99, , 100 101]

3: Dell 복구 옵션. 출처: Principled Technologies

Dell 복구 옵션	
유형	**기능 정보**
파일 레벨 복구	감염된 파일만 해당 위치에 복원하거나 롤백하여 복원한다.
라이브 VM	VM을 클러스터에 복원하고 나서 운영 환경으로의 마이그레이션이 진행된다.
신규로 복원	원래 환경 또는 새 환경(예: 클린룸 또는 복구 인프라스트럭처)으로 복원하며, 이 기간 동안 사용자는 대량 복원 또는 대규모 복원을 위해 한 번에 여러 VM을 선택할 수 있다.
액세스/라이브 VM	운영 데이터의 격리된 복제본 생성
복구 오케스트레이션	관리자가 복구를 예약하거나 온디맨드 방식으로 사용할 수 있도록 한다. VM을 운영 또는 복구 환경으로 자동 복구하는 데 우선순위를 둔다.

Rubrik 제한 사항

Rubrik 솔루션은 향후 분석을 위해 멀웨어에 감염된 스냅샷을 격리한다. 그러나 Rubrik 솔루션은 기본적으로 스냅샷을 격리하지 않는다. 그런 다음 고객은 격리된 파일을 직접 수동으로 또는 타사 툴을 사용하여 다운로드하고 포렌식 분석을 수행하여 잠재적으로 멀웨어에 노출될 수 있다.[102, 103]

> *CyberSense는 사용자가 직접 포렌식을 수행할 필요 없이 분석을 수행하며 소프트웨어는 복원 지점 생성을 자동화한다.*

CyberSense는 기본적으로 파일 및 데이터베이스를 분석한다. 사용자는 스냅샷을 수동으로 격리할 필요가 없다. **CyberSense는 사용자가 직접 포렌식을 수행할 필요 없이 분석을 수행하며 소프트웨어는 복원 지점 생성을 자동화한다.**[104]

RSC 전용 관리 모드의 Rubrik RSC는 많은 기능을 담당하는 단일 장애 지점이다. 가장 우려되는 것은 공격으로 인해 사용자 사이트와 RSC 간의 연결 또는 사용자 인터넷 연결에 영향을 주는 RSC 서비스 중단이 발생할 수 있다는 점이다. 이러한 공격 후 솔루션은 Rubrik CDM UI 또는 API 기반 자동화를 통해 사용할 수 있는 제한된 기능 세트를 사용자에게 제공한다. 단, 사용자가 공격 전에 RSC 서비스 계정을 생성한 경우에만 가능하다.[105' 106] 조직은 RSC 없이 MongoDB, Microsoft Exchange, 파일, Hyper-V 스냅샷, 관리형 볼륨에서의 라이브 마운트, NAS 호스트 파일, Oracle, SQL Server, VCD, VMware도 마찬가지이다.[107] RSC 없이 SAP HANA를 복구하려면 Studio 및 Cockpit Cross와 같은 타사 툴과 지원 터널을 통한 Rubrik 지원이 필요하다. RSC 없이 IBM Db2를 복구하려면 IBM의 타사 툴과 Rubrik 지원을 지원 터널을 통해 함께 사용해야 한다.[108]

에어 갭/격리

NIST는 에어 갭을 '두 시스템이 (a) 물리적으로 연결되지 않고 (b) 논리적 연결이 자동화되지 않은 두 시스템 간의 인터페이스(즉, 데이터는 인간의 통제 하에 인터페이스를 통해서만 수동으로 전송됨)'로 정의한다.[109]

에어 갭은 소스에서 타겟으로의 데이터 흐름을 제어하는 데 도움이 될 수 있으며 랜섬웨어 보호 및 사이버 복구 전략의 중요한 구성 요소가 될 수 있다. 공격 또는 이벤트로 인해 운영 백업 시스템이 손상되는 경우 운영 시스템에서 사이버 복구 볼트의 백업으로의 트래픽을 방지할 수 있는 기능이 페일 세이프를 제공할 수 있다.

물리적 격리

영화 미션 임파서블(Mission Imposible)에서 물리적으로 격리된 솔루션의 예시를 본 적이 있을 것이다. 주인공은 외부 네트워크에 연결되지 않은 컴퓨터 시스템의 기밀 데이터에 액세스하기 위해 다른 모든 시설 보안 기능을 우회해야 했다. 물리적 격리는 일반적으로 분리된 전용 물리적 네트워킹의 세그먼트를 사용하여 운영 시스템에서 볼트로 백업 복제본을 전송할 수도 있다. 이러한 운영 에어 갭이 분리되면 데이터가 자동으로 교차할 수 없는 물리적 장벽이 생성되어 악성 행위자가 액세스하기가 더 어려워진다.

조직은 운영 에어 갭 전략을 지원하기 위해 Dell PowerProtect Cyber Recovery를 물리적으로 격리할 수 있다. 이 솔루션은 전용 물리적 연결을 사용하고 백업 솔루션에서 푸시 작업이 아닌 볼트에서 가져오기 작업으로 데이터 복제를 수행한다. 복제/반복 중에는 솔루션이 연결을 활성화하고 데이터를 암호화하여 고정된 선로에 이송한다.[110] 복제를 완료한 후 솔루션은 볼트 측에서 연결을 다시 비활성화한다. 솔루션은 잠금 설정된 보존 정책으로 볼트 복제본을 변경할 수 없도록 하므로 사용자 또는 시스템이 액세스 권한을 얻더라도 볼트 복제본을 수정하거나 삭제할 수 없다. 관리 트래픽이 복제 경로를 통과하지 않으므로 **악성 행위자가 온프레미스 백업 솔루션을 제어하더라도 볼트는 복제 경로를 시작 및 연결 해제하고 데이터 소스에서 단방향 데이터 전용 풀을 사용하여 볼트에 대한 직접 액세스를 제한한다.**[111]

논리적 격리

반면에 논리적 격리는 동일한 물리적 네트워크에 상주할 수 있는 시스템을 사용하지만 논리적 네트워크 분리 및 제어를 생성하여 시스템이 서로 간에 데이터를 전송할 수 없도록 한다. 이 솔루션은 암호화 및 해싱과 같은 추가 보안 구현을 RBAC 및 다단계 인증과 함께 사용하여 권한이 없는 시스템이나 사용자가 다른 시스템 내에 있는 데이터를 읽을 수 없도록 한다.

Rubrik은 논리적 에어 갭 전략을 활용하는 것으로 사이버 복구 기능을 설명한다.[112' 113] 공개된 다수의 Rubrik 자료에서 에어 갭의 필요성에 의문을 제기했다. "Rubrik Security – Air Gap and Immutability"라는 제목의 Rubrik 프레젠테이션은 Rubrik 어플라이언스가 물리적 네트워크에 남아 있더라도 솔루션이 백업에 액세스하거나 편집할 방법이 없기 때문에 기본 솔루션에 에어 갭이 적용되었다고 주장한다.[114] 그러나 인증된 악성 행위자가 어플라이언스 GUI에 계속 액세스할 수 있으며, 이로 인해 복구에 영향을 미칠 수 있다. 이를 완화하기 위해 Rubrik에는 백업이 만료되지 않도록 하는 Retention Lock이 있다. 이는 불변성을 보장한다. Retention Lock이 활성화되면 Rubrik 클러스터가 출고 시 초기화되지 않는다. Rubrik CDM 보안 가이드에 따르면 이 솔루션은 기본적으로 클러스터에서 보존 잠금을 전역적으로 비활성화하며 고객이 Rubrik 지원에 문의하여 활성화해야 한다.[115] Rubrik Support가 Retention Lock을 비활성화할 수 있는지 여부는 공개적으로 사용 가능한 소스에서 명확히 알 수 없으므로 공인된 악성 행위자가 여전히 보안 계층을 우회할 수 있다는 우려가 존재한다.

> *"관리 트래픽이 복제 경로를 통과하지 않으므로 악성 행위자가 온프레미스 백업 솔루션을 제어하더라도 볼트는 복제 경로를 시작 및 연결 해제하고 데이터 소스에서 단방향 데이터 전용 풀을 사용하여 볼트에 대한 직접 액세스를 제한한다."*

결론

조직은 데이터 센터에 대한 수많은 공격 벡터를 적극적으로 고려해야 한다. 좋은 데이터 보호 계획은 모든 데이터, 특히 운영에 필수적인 중요 데이터를 보호하기 위한 것이다. Dell PowerProtect Cyber Recovery 및 Rubrik Secure Cloud에 대해 공개된 정보를 살펴보고 두 솔루션이 데이터 관리, 보호 및 복구에 어떻게 접근하는지 확인했다.

PowerProtect Cyber Recovery는 볼트에서 중요한 데이터의 백업 복제본을 물리적으로 격리하고 사이버 공격 발생 시 복구 가능성을 보장한다. 솔루션은 Rubrik Secure Cloud가 주장할 수 없는 물리적 격리 기능을 갖춘 운영 에어 갭 전략을 사용한다. 이 솔루션은 논리적 격리를 활용한다.

Cyber Recovery는 CyberSense의 ML 기반 분석을 사용하여 볼트에 있는 데이터의 무결성을 평가하고 복구할 클린 백업 데이터를 식별한다. 반면 Rubrik Secure Cloud는 파일에 대한 심층 검사를 수행하는 대신 이상 징후를 찾는 ML 학습 분석 툴을 제공한다.

또한 Cyber Recovery 솔루션은 볼트의 손상되지 않은 데이터를 활용하여 효율적이고 원활한 운영 복귀를 촉진하는 여러 복구 옵션을 제공한다. 대부분의 경우 PowerProtect Cyber Recovery는 Rubrik Secure Cloud가 부족한 기능과 이점을 제공할 수 있으므로 다운타임을 최소화하고 복구 속도를 높이기 위해 심층 분석을 수행할 수 있는 잠재적으로 더 안전한 솔루션을 제공할 수 있다.

---

1. Anastasia Dergacheva and Jesse R. Taylor, "Study Finds Average Cost of Data Breaches Continued to Rise in 2023", 2024년 7월 25일 열람, https://www.morganlewis.com/blogs/sourcingatmorganlewis/2024/03/study-finds-average-cost-of-data-breaches-continued-to-rise-in-2023.
2. Dell, "Dell PowerProtect Cyber Recovery Solution Guide", 2024년 4월 18일 열람, https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/h17670-cyber-recovery-sg.pdf.
3. Dell, "Dell PowerProtect Cyber Recovery Solution Guide"
4. Rubrik, "Rubrik Security Cloud Architecture and Security Implementation", 2024년 4월 18일 열람, https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/wp-rubrik-security-cloud-architecture-and-security-implementation.pdf.
5. Rubrik, "Rubrik Security Cloud Architecture and Security Implementation", 2024년 4월 18일 열람, https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/wp-rubrik-security-cloud-architecture-and-security-implementation.pdf.
6. Rob Emsley, "Public Cloud Vault to Secure, Isolate and Recover Data", 2024년 3월 20일 열람, https://www.dell.com/en-us/blog/public-cloud-vault-to-secure-isolate-and-recover-data/.

7. Brian White, "Dell's PowerProtect Cyber Recovery Expands to Microsoft Azure", 2024년 3월 20일 열람, https://www.dell.com/en-us/blog/dells-powerprotect-cyber-recovery-expands-to-microsoft-azure/.
8. Dell, "Cyber Recovery on Google Cloud Platform", 2024년 3월 20일 열람, https://infohub.delltechnologies.com/en-US/l/dell-powerprotect-cyber-recovery-reference-architecture/cyber-recovery-on-google-cloud-platform/.
9. Chris Mellor, "Up to $5m compensation if Rubrik Cloud Vault recovery busted", 2024년 3월 20일 열람, https://blocksandfiles.com/2022/02/24/up-to-5m-compensation-if-rubrik-cloud-vault-recovery-busted/.
10. Kristina Avrionova, "Frequently Asked Questions about Rubrik Cloud Vault", 2024년 3월 20일 열람, https://www.rubrik.com/blog/company/22/3/faq-about-rubrik-cloud-vault.
11. Chris Wahl, "Recovering Fast from Ransomware Attacks: The Magic of an Immutable Backup Architecture", 2024년 3월 22일 열람, https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/rwp-recovering-fast-from-ransomware-attacks.pdf.
12. Dell, "Data Domain Invulnerability Architecture: Enhancing Data Integrity and Recoverability", 2024년 6월 7일 열람, https://www.delltechnologies.com/asset/en-us/products/data-protection/industry-market/h7219-data-domain-data-invul-arch-wp.pdf.
13. Dell, "Consolidate Governance and Compliance Archive Data", 2024년 4월 4일 열람, https://infohub.delltechnologies.com/en-US/l/dell-powerprotect-data-domain-retention-lock/consolidate-governance-and-compliance-archive-data/.
14. Dell, "Dell PowerProtect Cyber Recovery Solution Guide", 2024년 3월 24일 열람, https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/h17670-cyber-recovery-sg.pdf.
15. Rubrik, "Retention-locked SLA Domain attributes", 2024년 4월 2일 열람, https://docs.rubrik.com/en-us/8.0/ug/cdm/attributes_of_retention_locked_sla_domains.html.
16. Rubrik, "Rubrik Cyber Recovery", 2024년 3월 20일 열람, https://www.rubrik.com/content/dam/rubrik/en/resources/solutions-brief/brf-rubrik-cyber-recovery.pdf.
17. Rubrik, "Rubrik Licensing: Subscribe to Simplicity", 2024년 3월 20일 열람, https://www.rubrik.com/content/dam/rubrik/en/resources/data-sheet/rubrik-licensing-data-sheet.pdf.
18. Rubrik, "Workloads require third-party tools for recovery", 2024년 5월 6일 열람, https://docs.rubrik.com/en-us/saas/saas/workloads_require_third_party_tools_for_recovery.html.
19. Rubrik, "Recoverable workloads during RSC service disruption", 2024년 5월 6일 열람, https://docs.rubrik.com/en-us/saas/saas/recoverable_workloads_during_rsc_service_disruption.html.
20. Rubrik, "Workloads require third-party tools for recovery"
21. Dell, "Strengthen your security posture with Managed Detection and Response", 2024년 4월 2일 열람, https://www.delltechnologies.com/asset/pl-pl/services/managed-services/technical-support/managed-detection-and-response-datasheet.pdf.
22. Dell, "Dell PowerProtect Cyber Recovery 19.13 Installation Guide", 2024년 3월 20일 열람, https://www.dell.com/support/manuals/en-us/cyber-recovery/irs_p_19.13_installation/installing-the-cyber-recovery-software?guid=guid-8718978d-ddd0-4dc0-bca7-fb04a2f3d1fb&lang=en-us.
23. Dell, "Dell PowerProtect Cyber Recovery 19.13 Installation Guide"
24. Dell, "Dell PowerProtect Cyber Recovery 19.13 Installation Guide"
25. Dell, "Installing CyberSense in Dell PowerProtect Cyber Recovery", 2024년 3월 20일 열람, https://infohub.delltechnologies.com/en-US/l/ransomware-protection-secure-your-data-on-dell-powerflex-with-powerprotect-cyber-recovery-1/installing-cybersense-in-dell-powerprotect-cyber-recovery-1/.
26. Dell, "Dell PowerProtect Cyber Recovery Solution Guide"
27. Rubrik, "Downloading and installing Rubrik CDM", 2024년 3월 20일 열람, https://docs.rubrik.com/en-us/saas/install/download_install_cdm_on_appliance_nodes.html.
28. Rubrik, "Setting up a Rubrik cluster using the UI", 2024년 3월 20일 열람, https://docs.rubrik.com/en-us/saas/install/setting_up_ui.html.
29. Rubrik, "Setting up a Rubrik cluster using the CLI", 2024년 3월 20일 열람, https://docs.rubrik.com/en-us/saas/install/setting_up_cli.html.
30. Rubrik, "Registering Rubrik clusters using the online method", 2024년 3월 20일 열람, https://docs.rubrik.com/en-us/saas/install/registering_clusters_online.html.
31. Rubrik, "Registering Rubrik clusters using the offline method", 2024년 4월 2일 열람, https://docs.rubrik.com/en-us/saas/install/registering_clusters_offline.html.
32. Rubrik, "Enabling MFA", 2024년 3월 21일 열람, https://docs.rubrik.com/en-us/saas/install/rsc_enabling_mfa.html.
33. Rubrik, "Adding the initial account", 2024년 3월 21일 열람, https://docs.rubrik.com/en-us/saas/saas/adding_the_initial_account.html.

34. TrustRadius, "Learning Rubrik by putting the pieces together Brik by Brik", 2024년 3월 21일 열람, https://www.trustradius.com/reviews/rubrik-2023-09-20-21-03-04.
35. Dell, "Dell PowerProtect Cyber Recovery Solution Guide"
36. Index Engines, "CyberSense®: How it Works", 2024년 3월 21일 열람, https://www.indexengines.com/how-it-works.
37. Rubrik, "Anomaly event details", 2024년 3월 21일 열람, https://docs.rubrik.com/en-us/saas/saas/anomaly_event_details.html.
38. Rubrik, "Events page", 2024년 3월 21일 열람, https://docs.rubrik.com/en-us/saas/saas/common/events_page.html.
39. Rubrik, "RSC Data Threat Analytics", 2024년 3월 21일 열람, https://docs.rubrik.com/en-us/saas/saas/ri_ransomware_monitoring.html.
40. Rubrik, "RSC Data Threat Analytics"
41. Dell Technologies, "Dell PowerProtect Cyber Recovery: Reference Architecture", 2024년 5월 6일 열람, https://www.delltechnologies.com/asset/en-us/products/data-protection/industry-market/h18661-dell-powerprotect-cyber-recovery-reference-architecture-wp.pdf.
42. Dell Technologies, "Dell EMC Avamar for Hyper-V", 2024년 5월 16일 열람, https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/docu89876.pdf.
43. Dell Technologies, "Dell EMC NetWorker Module for Microsoft for Hyper-V", 2024년 3월 16일 열람, https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/docu92011.pdf.
44. VMware, "Accelerate IT. Innovate with your cloud", 2024년 5월 9일 열람, https://www.vmware.com/files/pdf/VMware-Corporate-Brochure-BR-EN.pdf.
45. Statista, "Cloud infrastructure services vendor market share worldwide from fourth quarter 2017 to first quarter 2024", 2024년 7월 17일, https://www.statista.com/statistics/967365/worldwide-cloud-infrastructure-services-market-share-vendor/.
46. Rubrik, "RSC Data Threat Analytics"
47. Dell Technologies, "CyberSense® for PowerProtect Cyber Recovery", 2024년 6월 27일 열람, https://www.delltechnologies.com/asset/en-gb/products/data-protection/briefs-summaries/h18214-cybersense-for-dellemc-powerprotect-cyber-recovery-solution-brief.pdf.
48. Rubrik, "RSC Data Threat Analytics"
49. Index Engines, "CyberSense® Support Matrix", 2024년 3월 21일 열람, https://www.indexengines.com/csmatrix.
50. Dell Technologies, "CyberSense® for PowerProtect Cyber Recovery"
51. Rubrik, "Keep Your Databases Running in the Face of Any Threat"
52. Index Engines, "CyberSense® Support Matrix"
53. Dell Technologies, "Dell EMC Avamar for Hyper-V"
54. Dell Technologies, "Dell EMC NetWorker Module for Microsoft for Hyper-V"
55. Rubrik, "Anomaly incidents", 2024년 4월 2일 열람, https://docs.rubrik.com/en-us/saas/saas/anomaly_incident.html.
56. Rubrik, "Data Threat Analytics events", 2024년 4월 2일 열람, https://docs.rubrik.com/en-us/saas/saas/ri_events.html.
57. Rubrik, "Viewing Anomaly Detection", 2024년 4월 2일 열람, https://docs.rubrik.com/en-us/saas/saas/viewing_ri_investigations.html.
58. Rubrik, "VM Encryption Detection", 2024년 4월 2일, https://docs.rubrik.com/en-us/saas/saas/vm_encryption_detection.html.
59. Rubrik, "Viewing the Threat Monitoring page", 2024년 4월 2일 열람, https://docs.rubrik.com/en-us/saas/saas/viewing_the_threat_monitoring_page.html.
60. Rubrik, "Initiating a threat hunt", 2024년 4월 2일 열람, https://docs.rubrik.com/en-us/saas/saas/initiating_a_threat_hunt.html.
61. Rubrik, "Quarantining matched files or objects", 2024년 4월 2일 열람, https://docs.rubrik.com/en-us/saas/saas/quarantining_matched_objects_or_files.html.
62. Dell, "CyberSense® for PowerProtect Cyber Recovery"
63. Dell, "CyberSense® for PowerProtect Cyber Recovery"
64. Index Engines, "The Power of CyberSense's Machine Learning", 2024년 4월 2일 열람, https://go.indexengines.com/csmachinelearning.
65. Index Engines, "The Power of CyberSense's Machine Learning"
66. Index Engines, "The Power of CyberSense's Machine Learning"
67. Dell, "CyberSense® for PowerProtect Cyber Recovery"
68. Rubrik, "Anomaly Detection behavioral model", 2024년 5월 20일 열람, https://docs.rubrik.com/en-us/saas/saas/anomaly_detection_behavioral_model.html.
69. Amazon, "Training ML Models", 2024년 4월 2일 열람, https://docs.aws.amazon.com/machine-learning/latest/dg/training-ml-models.html.
70. Rubrik, "Defense in Depth with Polaris Radar", 2024년 3월 21일 열람, https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/Defense-In-Depth-Polaris-Radar-Technical-White-Paper.pdf.
71. Rubrik, "Data Threat Analytics dashboard", 2024년 3월 21일 열람, https://docs.rubrik.com/en-us/saas/saas/ri_dashboard.html.

72. Rubrik, "Initiating a threat hunt", 2024년 3월 21일 열람, https://docs.rubrik.com/en-us/saas/saas/initiating_a_threat_hunt.html.
73. SentinelOne, "What Is A Malware File Signature (And How Does It Work)?", 2024년 4월 4일 열람, https://www.sentinelone.com/blog/what-is-a-malware-file-signature-and-how-does-it-work/.
74. Rubrik, "Threat hunts", 2024년 3월 21일 열람, https://docs.rubrik.com/en-us/saas/saas/ri_threat_hunts.html.
75. Rubrik, "Anomaly Detection features", 2024년 3월 22일 열람, https://docs.rubrik.com/en-us/saas/saas/ri_features.html.
76. Rubrik, "Behavioral model"
77. Index Engines, "The Power of CyberSense's Machine Learning"
78. Dell, "CyberSense® for PowerProtect Cyber Recovery"
79. Rubrik, "Behavioral model"
80. Rubrik, "Anomaly Detection features"
81. Rubrik, "Behavioral model"
82. Dell, "CyberSense® for PowerProtect Cyber Recovery"
83. Morningstar, "Index Engines' CyberSense Announces 99.99% SLA in Detecting Ransomware Corruption, Empowering Smarter Recovery", 2024년 7월 17일 열람, https://www.morningstar.com/news/pr-newswire/20240618ny41171/index-engines-cybersense-announces-9999-sla-in-detecting-ransomware-corruption-empowering-smarter-recovery.
84. Rubrik, "Threat Monitoring", 2024년 3월 22일 열람, https://docs.rubrik.com/en-us/saas/saas/threat_monitoring.html.
85. Index Engines, "The Power of CyberSense's Machine Learning"
86. Index Engines, "The Power of CyberSense's Machine Learning"
87. Rubrik, "Anomaly Detection features", 2024년 3월 22일 열람, https://docs.rubrik.com/en-us/saas/saas/ri_features.html.
88. Index Engines, "The Power of CyberSense's Machine Learning"
89. Rubrik, "Investigating and recovering anomalous files for filesets", 2024년 3월 22일 열람, https://docs.rubrik.com/en-us/saas/saas/investigating_and_recovering_anomalous_files.html.
90. Rubrik, "Investigating and recovering anomalous files for virtual machines", 2024년 3월 22일 열람, https://docs.rubrik.com/en-us/saas/saas/investigating_and_recovering_anomalous_files_for_virtual_machines.html.
91. Rubrik, "Full snapshot recovery of a virtual machine", 2024년 3월 22일 열람, https://docs.rubrik.com/en-us/saas/saas/full_snapshot_recovery_of_a_virtual_machine.html.
92. Rubrik, "Recovery of a batch of virtual machines", 2024년 3월 22일 열람, https://docs.rubrik.com/en-us/saas/saas/ri_batch_recovery_of_vm.html.
93. Rubrik, "Performing bulk recovery for Recovery Plans", 2024년 3월 22일 열람, https://docs.rubrik.com/en-us/saas/saas/performing_bulk_recovery_for_recovery plans.html.
94. Rubrik, "Recovery of a batch of virtual machines", 2024년 4월 04일 열람, https://docs.rubrik.com/en-us/saas/saas/ri_batch_recovery_of_vm.html.
95. Rubrik, "Recovery of virtual machines", 2024년 4월 16일 열람, https://docs.rubrik.com/en-us/saas/saas/vs_recovery_vm.html.
96. 복구된 데이터 저장소는 일반적으로 운영 환경이 아닌 Rubrik 클러스터에 있다.
97. Rubrik, "Recovery of a batch of virtual machines", 2024년 4월 16일 열람, https://docs.rubrik.com/en-us/saas/saas/ri_batch_recovery_of_vm.html.
98. Dell, "Restore plan", 2024년 4월 16일 열람, https://infohub.delltechnologies.com/en-US/l/powerprotect-data-manager-protection-for-vmware-cloud-foundation-on-dell-emc-vxrail-1/restore-plan/.
99. Dell, "PowerProtect Data Manager overview", 2024년 4월 16일 열람, https://infohub.delltechnologies.com/en-US/l/dell-powerprotect-data-manager-deployment-best-practices-1/powerprotect-data-manager-overview-4/.
100. Dell, "PowerProtect Data Manager 19.9 Administration and User Guide", 2024년 4월 16일 열람, https://www.dell.com/support/manuals/en-us/enterprise-copy-data-management/pp-dm_19.9_ag/file-level-restore-of-a-powerprotect-backup-in-the-vsphere-client.
101. Dell, "Recovery Orchestration with PowerProtect Data Manager Overview", 2024년 4월 16일 열람, https://www.youtube.com/watch?v=po2oMnAg_x4.
102. Rubrik, "Quarantine files or objects", 2024년 3월 24일 열람, https://docs.rubrik.com/en-us/saas/saas/quarantine.html.
103. Rubrik, "Downloading quarantined files for forensic analysis", 2024년 3월 24일 열람, https://docs.rubrik.com/en-us/saas/saas/downloading_quarantined_files_for_forensic_analysis.html.
104. Forrester, "The Total Economic Impact™ Of Dell PowerProtect Cyber Recovery", 2024년 4월 16일 열람, https://www.delltechnologies.com/asset/en-us/products/data-protection/industry-market/the-total-economic-impact-dell-powerprotect-cyber-recovery.pdf.

105. Rubrik, "Workload recovery during an RSC service disruption", 2024년 4월 16일 열람, https://docs.rubrik.com/en-us/saas/saas/workload_recovery_during_rsc_outage.html.

106. Rubrik, "Rubrik CDM APIs and service account workflows", 2024년 4월 16일 열람, https://docs.rubrik.com/en-us/saas/saas/rubrik_apis_sa_workflows.html.

107. Rubrik, "Recoverable workloads during RSC service disruption", 2024년 4월 16일 열람, https://docs.rubrik.com/en-us/saas/saas/recoverable_workloads_during_rsc_service_disruption.html.

108. Rubrik, "Workloads require third-party tools for recovery", 2024년 4월 16일 열람, https://docs.rubrik.com/en-us/saas/saas/workloads_require_third_party_tools_for_recovery.html.

109. NIST, "Computer Security Resource Center Glossary: air gap", 2024년 6월 29일 열람, https://csrc.nist.gov/glossary/term/air_gap.

110. Dell, "Dell PowerProtect Cyber Recovery Solution Guide"

111. Dell, "Dell PowerProtect Cyber Recovery: Reference Architecture"

112. Adam Eckerle, "Debunking the Myths about Air Gaps", 2024년 3월 14일 열람, https://www.rubrik.com/blog/technology/2021/11/debunking-the-myths-about-air-gaps.

113. Rubrik, "Air-Gap, Isolated Recovery, and Ransomware - Cost vs. Value", 2024년 3월 14일 열람, https://www.rubrik.com/content/dam/rubrik/en/resources/solutions-brief/Air-Gap-Isolated-Recovery-and-Ransomware-Cost-vs.-Value.pdf.

114. Brian Williams, "Rubrik Air Gap and Immutability", 2024년 3월 14일 열람, https://vimeo.com/561870246.

115. Rubrik, "Retention locks in the Rubrik cluster", 2024년 3월 18일 열람, https://docs.rubrik.com/en-us/9.0/sg/security_guide/retention_locks_in_the_rubrik_cluster.html.

▶ 이 보고서의 원본 영어 버전 확인

이 프로젝트는 Dell Technologies의 의뢰로 진행되었습니다.

Principled Technologies®

Facts matter.®