랜섬웨어 보호 문서
Ransomware Protection

NetApp
April 01, 2022

목차

랜섬웨어 보호 문서

랜섬웨어 차단의 새로운 기능

랜섬웨어 차단의 새로운 기능에 대해 알아보십시오.

2021년 4월 5일

ONTAP 환경의 보안 강화를 추적하는 새 패널.

새로운 "ONTAP 환경 보호" 패널은 ONTAP 시스템의 특정 설정 상태를 제공하여 에 따른 배포 보안을 추적합니다 "ONTAP 시스템에 대한 NetApp 보안 강화 가이드 를 참조하십시오" 로 이동합니다 "ONTAP의 랜섬웨어 방지 기능" 비정상적인 활동을 사전에 감지하여 경고합니다.

권장사항을 검토한 후 잠재적 문제를 어떤 방식으로 해결할 것인지 결정할 수 있습니다. 다음 단계에 따라 클러스터의 설정을 변경하거나, 변경 사항을 다른 시간으로 연기하거나, 제안을 무시할 수 있습니다. "자세한 내용을 보려면 여기를 클릭하십시오".

클라우드 백업을 사용하여 다양한 범주의 데이터를 보호하는 방법을 보여주는 새로운 패널입니다.

이 새로운 "백업 상태" 패널은 랜섬웨어 공격으로 인해 복구해야 할 경우에 대비하여 가장 중요한 데이터 범주를 포괄적으로 백업하는 방법을 보여줍니다. 이 데이터는 환경에서 Cloud Backup에 의해 백업된 특정 범주의 항목 수를 시각적으로 나타냅니다.

2022년 3월 15일

비즈니스 크리티컬 데이터의 사용 권한 상태를 추적할 수 있는 새 패널입니다

새로운 "비즈니스 크리티컬 데이터 사용 권한 분석" 패널은 비즈니스에 중요한 데이터의 사용 권한 상태를 보여줍니다. 이를 통해 비즈니스 크리티컬 데이터를 얼마나 잘 보호하고 있는지 빠르게 평가할 수 있습니다. "자세한 내용을 보려면 여기를 클릭하십시오".

이제 사용 권한 열기 영역에 OneDrive 및 SharePoint 계정이 포함됩니다

이제 랜섬웨어 보호 대시보드의 개방형 권한 영역에 OneDrive 계정 및 SharePoint 계정에서 스캔되는 파일에 대한 사용 권한이 포함됩니다.

2022년 2월 9일

새로운 랜섬웨어 보호 서비스

새로운 랜섬웨어 보호 서비스를 통해 사이버 보안에 대한 관련 정보를 확인하고 데이터가 사이버 공격에 얼마나 복원되는지 평가할 수 있습니다. 또한 알림 목록과 데이터 보안 개선을 위한 해결 방법도 제공합니다.

"이 새로운 서비스에 대해 자세히 알아보십시오".

시작하십시오

랜섬웨어 차단 에 대해 알아보십시오

랜섬웨어 공격은 비즈니스 시간, 리소스 및 평판에 악영향을 줄 수 있습니다. 랜섬웨어 보호 서비스를 통해 사이버 보안에 대한 관련 정보를 보고 데이터가 사이버 공격에 얼마나 복원되는지 평가할 수 있습니다. 또한 알림 목록과 데이터 보안 개선을 위한 해결 방법도 제공합니다.

"랜섬웨어 차단 의 사용 사례에 대해 알아보십시오".

랜섬웨어 보호 서비스는 현재 베타 버전입니다.

피처

랜섬웨어 차단은 현재 사이버 스토리지 보호 노력을 지원할 수 있는 여러 기능을 제공합니다. 향후 추가 기능이 추가될 예정입니다. 현재 기능은 다음과 같은 경우에 식별합니다.

- 작업 환경의 볼륨은 정기적인 Snapshot 복사본을 만들어 보호되지 않습니다.
- 를 사용하여 클라우드에 백업을 생성하면 작업 환경의 볼륨이 보호되지 않습니다 "클라우드 백업".
- 작업 환경 및 데이터 소스의 데이터는 를 사용하여 스캔되지 않습니다 "클라우드 데이터 감지" 규정 준수 및 개인 정보 보호에 대한 우려 사항을 파악하고 최적화 기회를 찾습니다.
- 작업 환경 또는 데이터 소스에서 암호화된 파일의 비율이 비정상적으로 증가했습니다.

  이는 네트워크에서 랜섬웨어 공격이 시작했다는 것을 나타내는 지표가 될 수 있습니다.
- 파일에서 중요한 데이터가 검색되고 작업 환경 또는 데이터 소스에서 액세스 권한 수준이 너무 높습니다.
- 사용자가 Active Directory 도메인 관리자 그룹에 추가되었습니다.
- 클러스터의 ONTAP 소프트웨어 버전은 오래되었으며 최상의 보호 및 보안 기능을 제공하도록 업데이트해야 합니다.
- ONTAP 시스템에서 NAS 파일 시스템 감사가 설정되지 않았습니다.

  CIFS 감사를 설정하면 시스템 관리자가 폴더 권한 변경, 파일 읽기 또는 쓰기 실패, 파일 생성, 수정 또는 삭제 시기 등의 정보를 추적하는 감사 이벤트가 생성됩니다.
- 온박스 안티 랜섬웨어 기능은 ONTAP 시스템에서 지원되지 않습니다.

  ONTAP의 랜섬웨어 방지 기능은 랜섬웨어 공격을 나타낼 수 있는 비정상적인 활동을 사전에 감지하여 경고합니다.

"랜섬웨어 보호 대시보드에서 이러한 잠재적인 문제를 확인하는 방법을 알아보십시오."

Cloud Volumes ONTAP 시스템을 사용할 경우 작업 환경에서 직접 배포할 수 있는 몇 가지 추가적인 랜섬웨어 보호 기능이 있습니다. "랜섬웨어에 대한 보호를 강화하는 방법을 알아보십시오".

지원되는 작업 환경 및 데이터 소스

"클라우드 데이터 감지" 랜섬웨어 보호 서비스를 이용하려면 사전 요구사항이 있어야 합니다. Data Sense를 설치 및 활성화한 후 랜섬웨어 Protection을 사용하여 다음 유형의 작업 환경 및 데이터 소스에 대한 사이버 공격에 데이터가 얼마나 복원되는지 확인할 수 있습니다.

- 작업 환경: *
- Cloud Volumes ONTAP(AWS, Azure 또는 GCP에 구축)
- 온프레미스 ONTAP 클러스터
- Azure NetApp Files
- ONTAP용 Amazon FSx
- Amazon S3
- 데이터 소스: *
- 비 NetApp 파일 공유
- 오브젝트 스토리지(S3 프로토콜 사용)
- 데이터베이스를 지원합니다
- OneDrive 계정
- SharePoint 계정

또한 랜섬웨어 차단 기능은 글로벌 Active Directory 구성이 있는 경우 모니터링하기도 합니다 "클라우드 데이터 센스에서 구성했습니다".

랜섬웨어 차단의 작동 방식

고수준에서 랜섬웨어 차단은 다음과 같이 작동합니다.

1. 랜섬웨어 방지 기능은 Data Sense, Cloud Backup 및 기타 Cloud Manager 리소스에서 정보를 수집하여 랜섬웨어 보호 대시보드를 채웁니다.
2. 랜섬웨어 보호 대시보드를 사용하여 시스템 보호 수준 개요를 수집합니다.
3. 제공된 보고 툴을 사용하여 사이버 스토리지 보호 노력을 지원할 수 있습니다.

비용

Beta 기간 중에는 랜섬웨어 보호 서비스에 별도의 비용이 들지 않습니다.

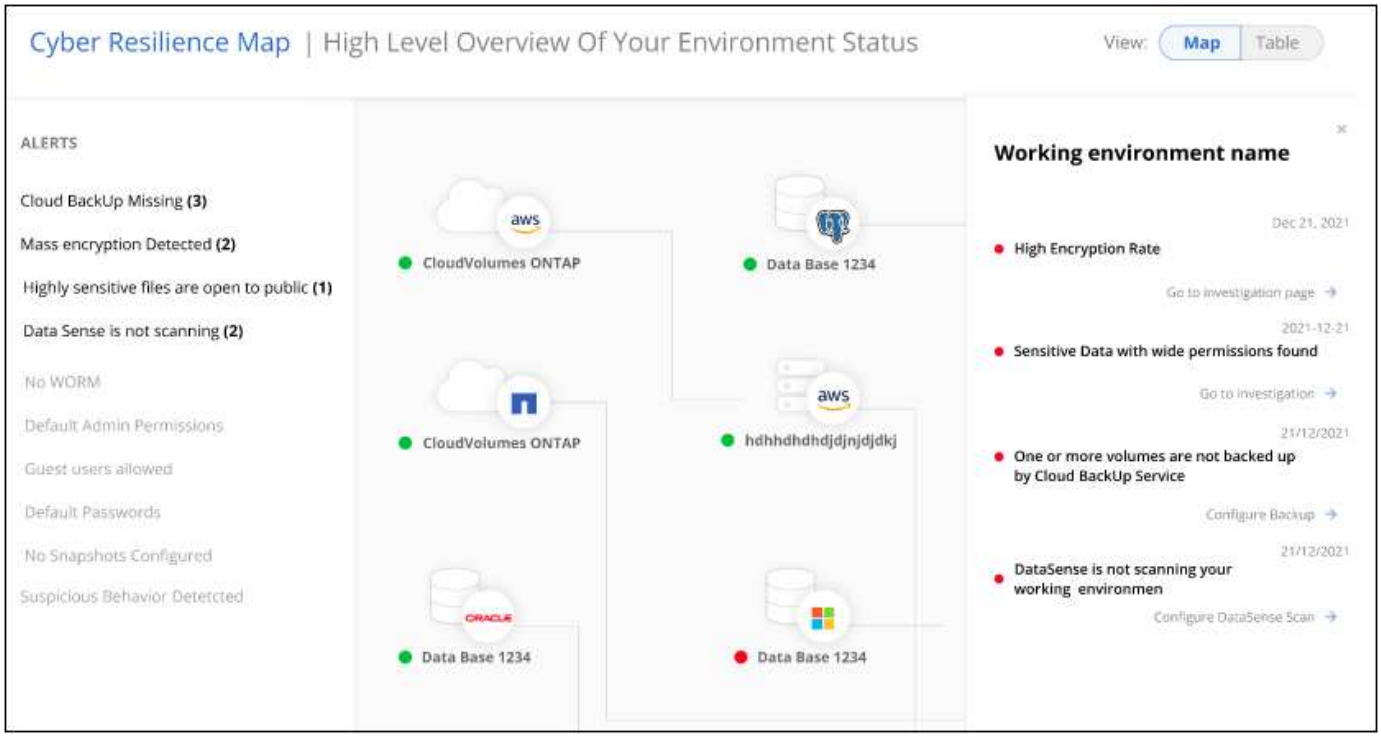
랜섬웨어 차단 기능을 사용하십시오

데이터 원본에 대한 사이버 보안 권장 사항 관리

랜섬웨어 보호 대시보드를 사용하여 모든 작업 환경 및 데이터 소스의 사이버 탄력성에 대한 개요를 볼 수 있습니다. 각 영역을 드릴다운하여 자세한 내용과 가능한 해결 방법을 찾을 수 있습니다.

사이버 복원력 맵

Cyber Resilience Map은 대시보드의 주요 영역입니다. 이를 통해 모든 작업 환경과 데이터 소스를 시각적으로 확인하고 관련 사이버 복원력 정보를 볼 수 있습니다.



이 맵은 다음 세 부분으로 구성됩니다.

왼쪽 패널

모든 데이터 소스에서 서비스가 모니터링 중인 알림 목록을 표시합니다. 또한 사용자 환경에서 활성화된 각 특정 경고의 수도 표시됩니다. 많은 유형의 경고가 있는 경우 이러한 경고를 먼저 해결하기 위한 좋은 이유가 될 수 있습니다.

가운데 패널

모든 데이터 소스, 서비스 및 Active Directory를 그래픽 형식으로 표시합니다. 건강한 환경에는 녹색 표시기가 있고 경고가 있는 환경에는 빨간색 표시기가 있습니다.

오른쪽 패널

빨간색 표시기가 있는 데이터 원본을 클릭하면 이 패널에 해당 데이터 원본에 대한 경고가 표시되고 경고 해결을 위한 권장 사항이 제공됩니다. 가장 최근 경고가 먼저 나열되도록 경고가 정렬됩니다. 많은 권장 사항으로 인해 문제를 해결할 수 있는 다른 Cloud Manager 서비스로 안내됩니다.

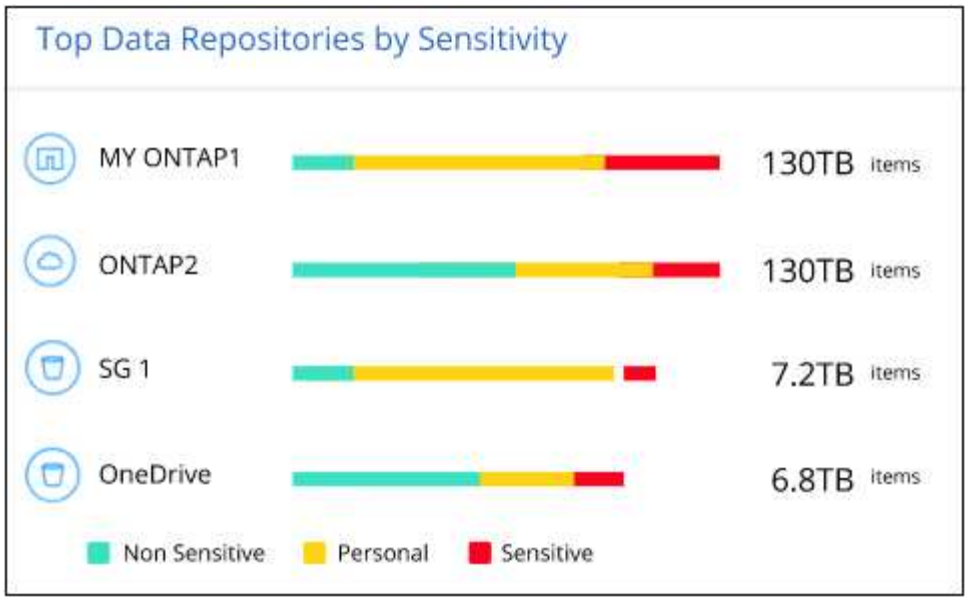
현재 추적된 알림 및 권장 해결 방법은 다음과 같습니다.

경고	설명	해결
높은 데이터 암호화 속도가 감지되었습니다	데이터 소스에서 암호화된 파일 또는 손상된 파일의 비율이 비정상적으로 증가했습니다. 즉, 지난 7일 동안 암호화된 파일의 비율이 20% 이상 증가했습니다. 예를 들어 파일의 50%가 암호화되면 이 숫자가 60%로 증가하게 됩니다.	링크를 클릭하여 을 시작합니다 "데이터 감지 조사 페이지". 여기서 Specific_Working Environment_and_Category(암호화 및 손상)_의 필터를 선택하여 모든 암호화 및 손상된 파일의 목록을 볼 수 있습니다.
광범위한 권한이 있는 중요한 데이터가 발견되었습니다	파일에서 중요한 데이터가 검색되고 데이터 소스에서 액세스 권한 수준이 너무 높습니다.	링크를 클릭하여 을 시작합니다 "데이터 감지 조사 페이지". 여기에서 특정_작업 환경_,민감도 수준(민감한 개인) 및 _열기 권한 _ 에 대한 필터를 선택하여 이 문제가 있는 파일 목록을 볼 수 있습니다.
Cloud Backup을 사용하여 하나 이상의 볼륨이 백업되지 않습니다	작업 환경의 일부 볼륨이 을(를) 사용하여 보호되고 있지 않습니다 "클라우드 백업".	링크를 클릭하여 Cloud Backup을 시작한 다음 작업 환경에서 백업하지 않는 볼륨을 식별하고 해당 볼륨에 대해 백업을 설정할 것인지 결정할 수 있습니다.
데이터 소스에 있는 하나 이상의 저장소(볼륨, 버킷 등)가 데이터 센스에 의해 스캔되지 않습니다	데이터 원본의 일부 데이터가 을(를) 사용하여 스캔되지 않습니다 "클라우드 데이터 감지" 규정 준수 및 개인 정보 보호 문제를 식별하고 최적화 기회를 찾습니다.	링크를 클릭하여 데이터 센스를 시작하고 스캔하지 않는 항목에 대한 스캐닝 및 매핑을 활성화합니다.
ONTAP 시스템은 견고하게 제작된 것이 아닙니다	ONTAP 시스템의 특정 설정은 의 권장 사항에 따라 설정되지 않습니다 "ONTAP 시스템에 대한 NetApp 보안 강화 가이드 를 참조하십시오".	링크를 클릭하면 로 리디렉션됩니다 ONTAP 환경 패널을 강화합니다 아래에서 경고를 유발하는 문제와 문제를 해결하는 방법을 확인할 수 있습니다.

데이터 민감도에 따른 상위 데이터 저장소

Sensitivity Level을 통한 상위 데이터 리포지토리 _ 패널에는 가장 중요한 항목이 포함된 상위 4개의 데이터 저장소(작업 환경 및 데이터 소스)가 나열됩니다. 각 작업 환경의 막대 차트는 다음과 같이 구분됩니다.

- 중요하지 않은 데이터입니다
- 개인 데이터
- 민감한 개인 데이터



각 섹션 위로 마우스를 가져가면 각 범주의 총 항목 수를 볼 수 있습니다.

각 영역을 클릭하면 데이터 감지 조사 페이지에서 필터링된 결과를 볼 수 있으므로 더 자세히 조사할 수 있습니다.

도메인 관리자 그룹 제어

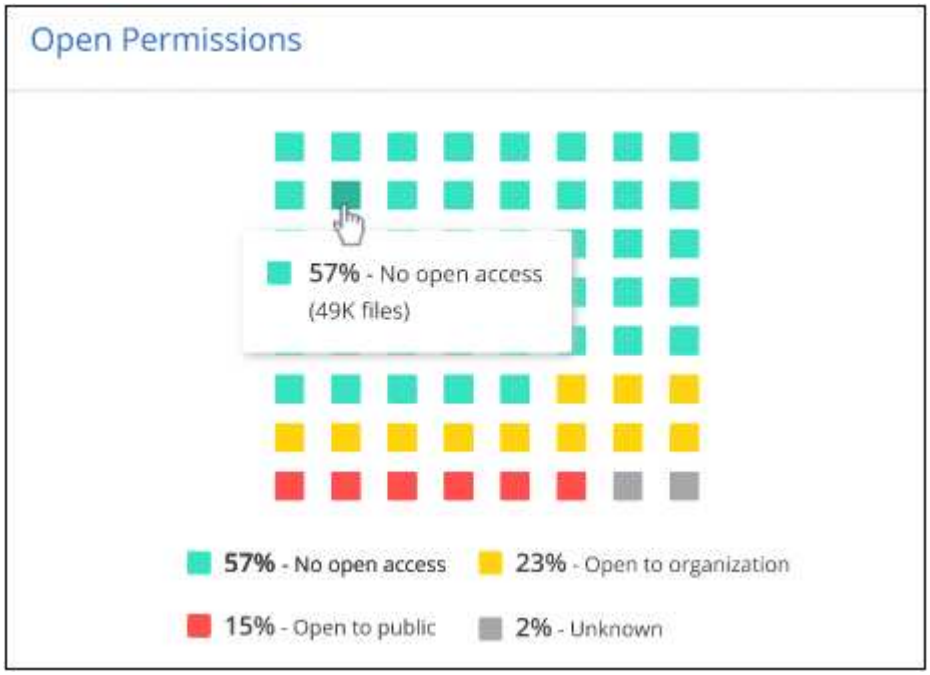
도메인 관리자 그룹 제어_패널에는 도메인 관리자 그룹에 추가된 최근 5명의 사용자가 표시되어 모든 사용자가 해당 그룹에서 허용되는지 확인할 수 있습니다. 이(가) 있어야 합니다 "글로벌 Active Directory 통합" 클라우드 데이터 센스로 들어가 이 패널이 활성화되도록 합니다.

기본 관리 그룹에는 "관리자", "도메인 관리자", "엔터프라이즈 관리자", "엔터프라이즈 키 관리자" 및 "키 관리자"가 포함됩니다.

열려 있는 권한 유형에 따라 데이터가 나열됩니다

Open Permissions_패널은 스캔되는 모든 파일에 대해 존재하는 각 권한 유형의 백분율을 표시합니다. 차트는 데이터 센스에서 제공되며 다음과 같은 유형의 권한을 보여 줍니다.

- 개방 액세스 없음
- 조직에 열기
- 공개
- 알 수 없는 액세스

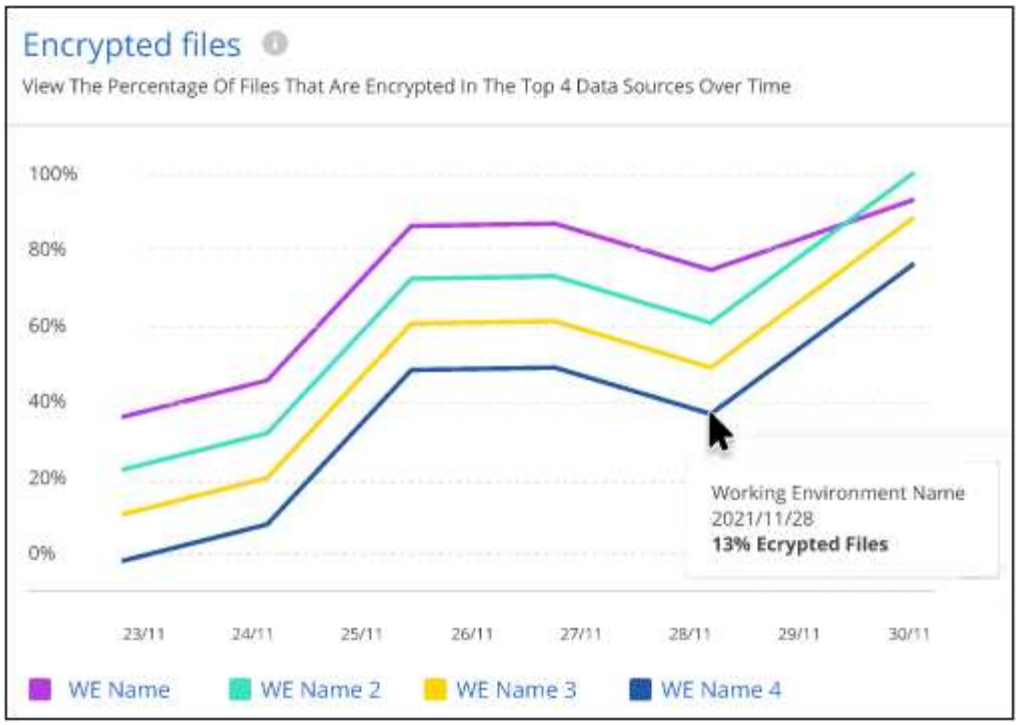


각 섹션 위로 마우스를 가져가면 각 범주의 파일 백분율 및 총 개수를 볼 수 있습니다.

각 영역을 클릭하면 데이터 감지 조사 페이지에서 필터링된 결과를 볼 수 있으므로 더 자세히 조사할 수 있습니다.

암호화된 파일에 의해 데이터가 나열됩니다

_Encrypted Files_패널은 시간이 지남에 따라 암호화되는 파일의 비율이 가장 높은 상위 4개의 데이터 소스를 표시합니다. 일반적으로 암호로 보호된 항목입니다. 이를 위해 지난 7일 동안의 암호화 속도를 비교하여 어떤 데이터 소스가 20% 이상 증가하는지 확인합니다. 이 용량이 증가하면 랜섬웨어가 이미 시스템을 공격하게 됩니다.

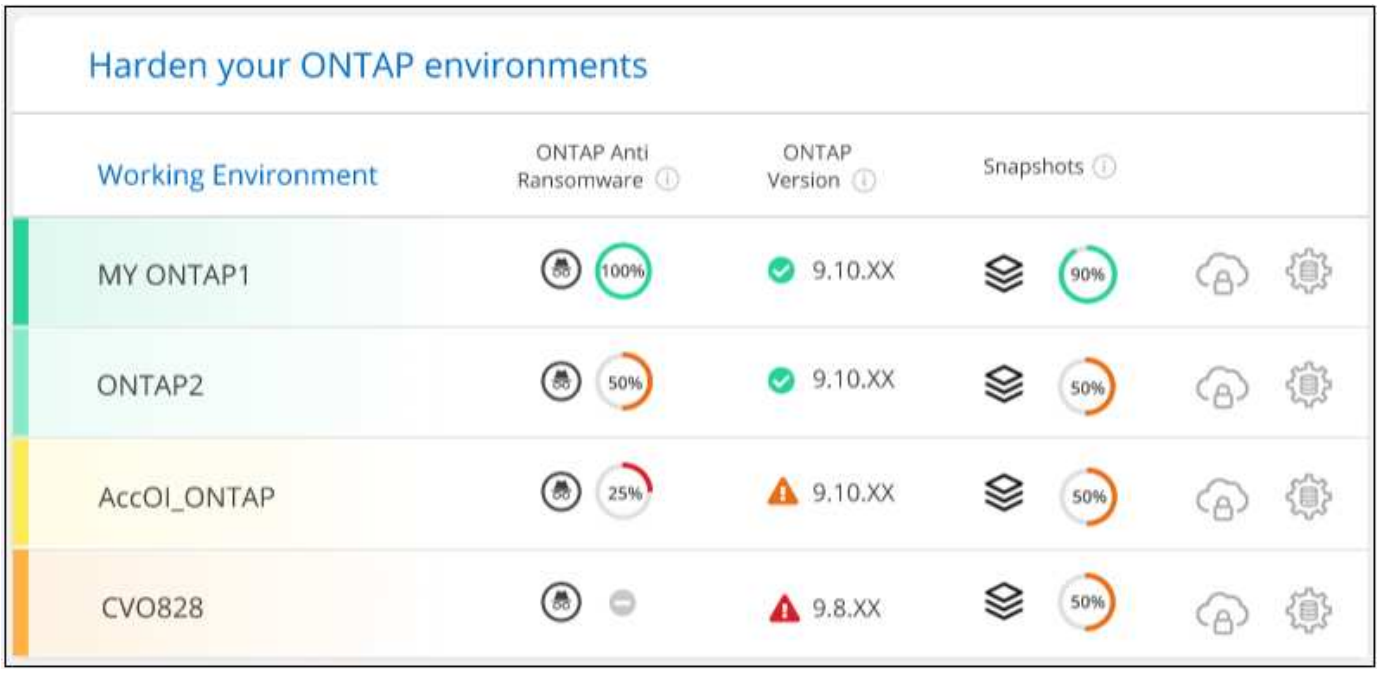


데이터 소스 중 하나에 대한 행을 클릭하여 데이터 감지 조사 페이지에서 필터링된 결과를 보고 더 자세히 조사할 수 있습니다.

ONTAP 시스템 강화 상태

ONTAP 환경 _ 패널 은(는) 에 따라 배포가 얼마나 안전한지 추적하는 ONTAP 시스템의 특정 설정 상태를 제공합니다 "ONTAP 시스템에 대한 NetApp 보안 강화 가이드 를 참조하십시오" 로 이동합니다 "ONTAP의 랜섬웨어 방지 기능" 비정상적인 활동을 사전에 감지하여 경고합니다.

권장사항을 검토한 후 잠재적 문제를 어떤 방식으로 해결할 것인지 결정할 수 있습니다. 다음 단계에 따라 클러스터의 설정을 변경하거나, 변경 사항을 다른 시간으로 연기하거나, 제안을 무시할 수 있습니다. 이 패널은 현재 사내 ONTAP 및 Cloud Volumes ONTAP 시스템을 지원합니다.



추적 중인 설정은 다음과 같습니다.

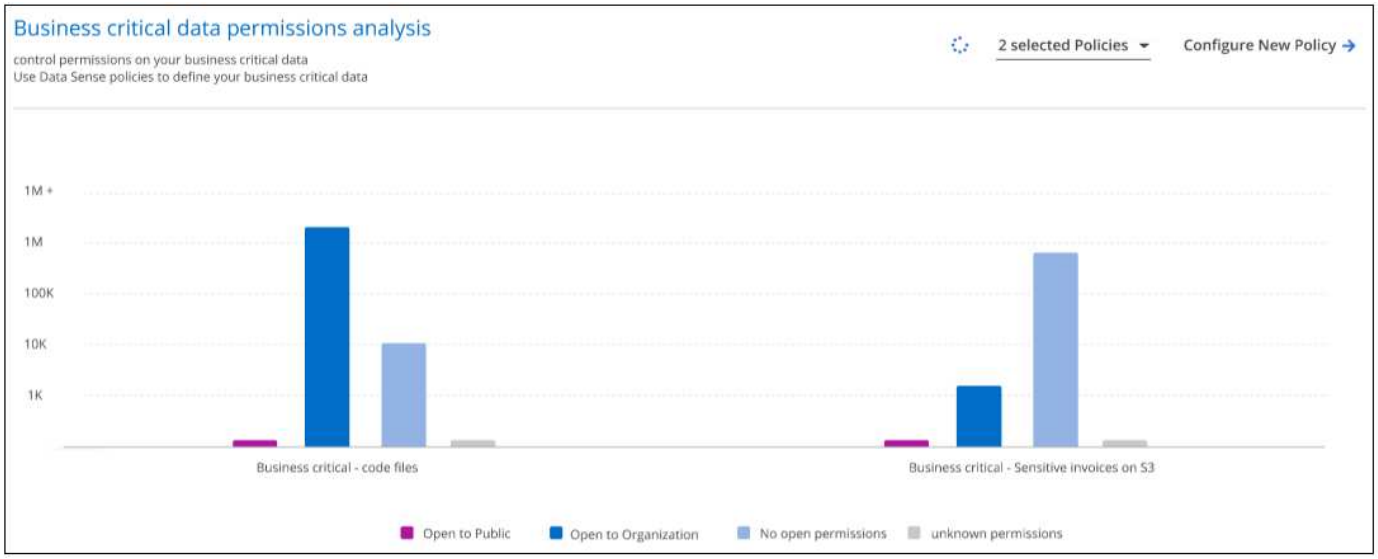
강화 목표	설명	해결
온박스 안티 랜섬웨어	온박스 안티 랜섬웨어가 활성화된 볼륨의 비율입니다. 사내 ONTAP 시스템에만 적용됩니다. 녹색 상태 아이콘은 볼륨의 85% 이상이 활성화되어 있음을 나타냅니다. 노란색은 40-85%가 활성화되었음을 나타냅니다. 빨간색은 40% 미만임을 나타냅니다.	"볼륨에서 안티 랜섬웨어를 활성화하는 방법을 확인하십시오" System Manager 사용:
ONTAP 버전	클러스터에 설치된 ONTAP 소프트웨어의 버전입니다. 녹색 상태 아이콘은 버전이 현재 버전임을 나타냅니다. 노란색 아이콘은 클러스터가 1개 또는 2개의 패치 버전이나 온프레미스 시스템의 경우 1개의 부 버전 뒤이거나 다른 시스템의 경우 1개의 주 버전 뒤임을 나타냅니다. 빨간색 아이콘은 클러스터가 3개의 패치 버전 또는 2개의 부 버전 또는 온프레미스 시스템의 경우 1개의 주 버전 또는 다른 버전의 경우 2개의 주 버전 뒤임을 나타냅니다.	"사내 클러스터를 업그레이드하는 가장 좋은 방법을 확인하십시오" 또는 "Cloud Volumes ONTAP 시스템".

강화 목표	설명	해결
스냅샷 수	데이터 볼륨에 대해 활성화된 스냅샷 기능과 스냅샷 복사본이 있는 볼륨의 비율은 얼마입니까? 녹색 상태 아이콘은 볼륨의 85% 이상이 스냅샷을 활성화했음을 나타냅니다. 노란색은 40-85%가 활성화되었음을 나타냅니다. 빨간색은 40% 미만임을 나타냅니다.	"온프레미스 클러스터에서 스냅샷을 활성화하는 방법을 알아보십시오" 또는 "Cloud Volumes ONTAP 시스템에".

Cloud Backup 버튼을 클릭하여 볼륨에 대한 백업을 활성화하거나 Data Sense 버튼을 클릭하여 클러스터의 볼륨을 검사하여 규정 준수 및 거버넌스 준수를 조사할 수 있습니다.

중요한 비즈니스 데이터에 대한 사용 권한의 상태입니다

비즈니스 크리티컬 데이터 권한 분석 패널은 비즈니스에 중요한 데이터의 사용 권한 상태를 표시합니다. 이를 통해 비즈니스 크리티컬 데이터를 얼마나 잘 보호하고 있는지 빠르게 평가할 수 있습니다.



가장 중요한 비즈니스 데이터를 보기 위해 만든 Data Sense_Policies_를 선택한 후에만 데이터가 채워지기 때문에 처음에는 이 패널에 데이터가 없습니다. 자세한 내용은 를 참조하십시오 "데이터 센스를 사용하여 정책을 만드십시오".

이 패널에 최대 2개의 정책을 추가한 후 그래프에는 정책의 기준을 충족하는 모든 데이터에 대한 사용 권한 분석이 표시됩니다. 다음과 같은 항목 수가 나열됩니다.

- 공개 권한으로 열기 – Data Sense에서 공개라고 여기는 항목입니다
- 조직 권한에 대한 공개 – Data Sense가 조직에 개방적이라고 여기는 항목입니다
- 열린 권한 없음 – Data Sense에서 열린 권한이 없는 것으로 간주하는 항목입니다
- 알 수 없는 권한 – Data Sense에서 알 수 없는 사용 권한으로 간주하는 항목입니다

차트의 각 막대 위로 마우스를 가져가면 각 범주의 결과 수를 볼 수 있습니다. 막대를 클릭하면 열려 있는 권한이 있는 항목과 파일 권한을 조정해야 하는지 여부를 자세히 조사할 수 있도록 데이터 감지 조사 페이지가 표시됩니다.

지식 및 지원

지원을 위해 등록하십시오

""

도움을 받으십시오

""

법적 고지

""

""

- "Cloud Manager 3.9에 대한 고지 사항"