워크로드 보호

BlueXP ransomware protection

NetApp
December 20, 2024

목차

워크로드 보호

랜섬웨어 전략으로 워크로드를 보호합니다

BlueXP 랜섬웨어 보호를 사용하여 다음 작업을 완료하여 랜섬웨어 공격으로부터 워크로드를 보호할 수 있습니다.

- SnapCenter 소프트웨어 또는 VMware vSphere용 SnapCenter 플러그인과 함께 워크로드 정합성이 보장되는 보호를 지원합니다.
- 스냅샷, 백업 및 랜섬웨어 보호(_ 감지 정책 _)에 대해 생성하는 정책이 포함된 랜섬웨어 보호 전략을 생성하거나 관리합니다.
- 전략을 가져와서 조정합니다.
- 파일 공유를 그룹화하여 워크로드를 개별적으로 보호하는 대신 더욱 쉽게 보호할 수 있습니다.
- 랜섬웨어 차단 전략을 삭제합니다.
- 어떤 서비스가 보호에 사용됩니까? * 다음 서비스를 사용하여 보호 정책을 관리할 수 있습니다. 이러한 서비스의 보호 정보가 BlueXP 랜섬웨어 보호에 나타납니다.
- 파일 공유, VM 파일 공유를 위한 BlueXP 백업 및 복구
- VM 데이터 저장소용 SnapCenter for VMware
- Oracle 및 MySQL용 SnapCenter

보호 정책

변경할 수 있는 보호 정책에 대한 정보와 보호 전략에 포함된 정책 유형을 검토하는 것이 도움이 될 수 있습니다.

- 어떤 보호 정책을 변경할 수 있습니까? *

다음과 같은 워크로드 보호에 따라 보호 정책을 변경할 수 있습니다.

- * NetApp 애플리케이션에 의해 보호되지 않는 워크로드 *: 이러한 워크로드는 SnapCenter, VMware vSphere용 SnapCenter 플러그인 또는 BlueXP 백업 및 복구에 의해 관리되지 않습니다. 이러한 워크로드에는 ONTAP 또는 다른 제품의 일부로 생성된 스냅샷이 있을 수 있습니다. ONTAP FPolicy 보호가 적용된 경우 ONTAP를 사용하여 FPolicy 보호를 변경할 수 있습니다.
- * NetApp 애플리케이션을 통한 기존 보호 워크로드 *: 이러한 워크로드에는 SnapCenter, VMware vSphere용 SnapCenter 또는 BlueXP 백업 및 복구에 의해 관리되는 백업 또는 스냅샷 정책이 있습니다.
  - 스냅샷 또는 백업 정책을 SnapCenter, SnapCenter for VMware 또는 BlueXP 백업 및 복구를 통해 관리하는 경우에도 이러한 애플리케이션에 의해 계속 관리됩니다. BlueXP 랜섬웨어 방어를 사용하면 이러한 워크로드에 랜섬웨어 감지 정책을 적용할 수도 있습니다.
  - ONTAP의 ARP(자율적 랜섬웨어 방어) 및 FPolicy에 의해 랜섬웨어 감지 정책을 관리하는 경우 해당 워크로드가 보호되고 ARP 및 FPolicy로 계속 관리됩니다.
- 랜섬웨어 방지 전략에 필요한 정책은 무엇입니까? *

랜섬웨어 보호 전략에는 다음 정책이 필요합니다.

- 랜섬웨어 감지 정책

- 스냅샷 정책

BlueXP 랜섬웨어 방지 전략에서 백업 정책이 필요하지 않습니다.

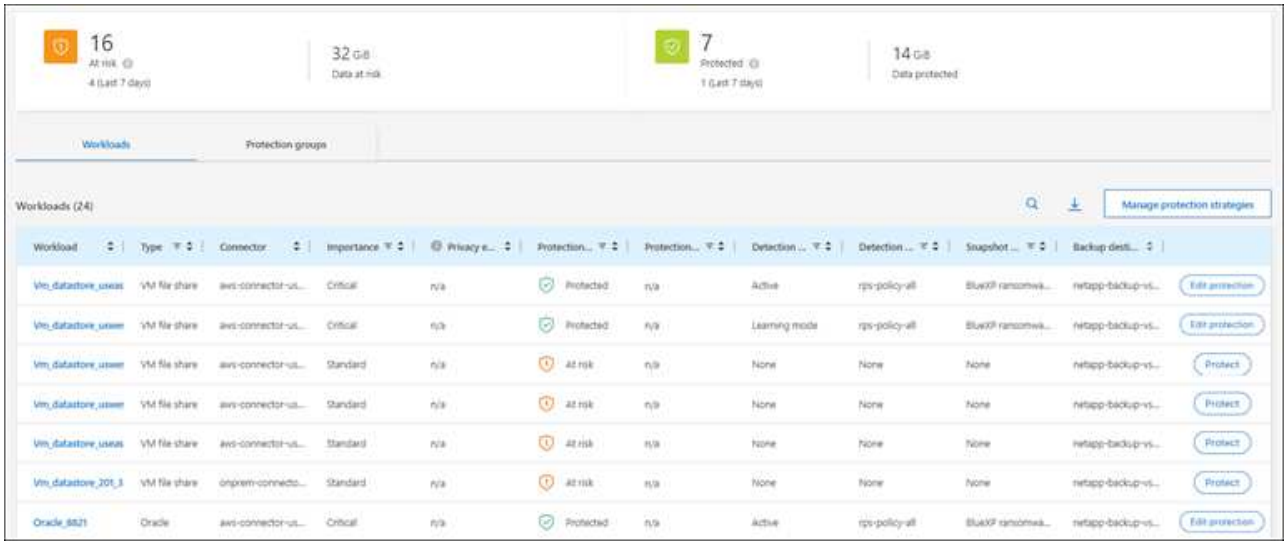
워크로드에 대한 랜섬웨어 방어 체계를 확인하십시오

워크로드를 보호하는 첫 번째 단계 중 하나는 현재 워크로드와 해당 워크로드의 보호 상태를 확인하는 것입니다. 다음과 같은 워크로드 유형을 볼 수 있습니다.

- 애플리케이션 워크로드
- VM 워크로드
- 파일 공유 워크로드

단계

1. BlueXP 왼쪽 탐색 창에서 * 보호 * > * 랜섬웨어 방어 * 를 선택하십시오.
2. 다음 중 하나를 수행합니다.
   - 대시보드의 데이터 보호 창에서 * 모두 보기 * 를 선택합니다.
   - 메뉴에서 * 보호 * 를 선택합니다.



3. 이 페이지에서 워크로드에 대한 보호 세부 정보를 보고 변경할 수 있습니다.

> SnapCenter 또는 BlueXP 백업 및 복구 서비스에 이미 보호 정책이 있는 워크로드의 경우 보호를 편집할 수 없습니다. 이러한 워크로드에 대해 BlueXP 랜섬웨어는 자율적 랜섬웨어 방어 및/또는 FPolicy 보호가 다른 서비스에서 이미 활성화되어 있는 경우 이를 지원합니다. 에 대한 자세한 내용은 "자율 랜섬웨어 보호" "BlueXP 백업 및 복구", 및 "ONTAP FPolicy를 사용해 보십시오"을 참조하십시오.

보호 페이지의 보호 세부 정보

보호 페이지에는 워크로드 보호에 대한 다음 정보가 표시됩니다.

- 보호 상태 *: 워크로드는 다음 보호 상태 중 하나를 표시하여 정책이 적용되었는지 여부를 나타낼 수 있습니다.

- * Protected *: 정책이 적용됩니다. ARP는 워크로드와 관련된 모든 볼륨에서 활성화됩니다.
- * 위험 *: 정책이 적용되지 않습니다. 워크로드에 기본 감지 정책이 설정되어 있지 않으면 스냅숏 및 백업 정책이 활성화되어 있더라도 "위험에 처합니다."
- * 진행 중 *: 정책이 적용되지만 아직 완료되지 않았습니다.
- * 실패 * : 정책이 적용되었지만 작동하지 않습니다.
- 감지 상태 *: 워크로드에는 다음 랜섬웨어 감지 상태 중 하나가 포함될 수 있습니다.
- * 학습 *: 랜섬웨어 감지 정책이 최근 워크로드에 할당되었으며 서비스가 워크로드를 스캔하고 있습니다.
- * 활성 *: 랜섬웨어 감지 보호 정책이 할당됩니다.
- * 설정되지 않음 *: 랜섬웨어 감지 보호 정책이 할당되지 않았습니다.
- * Error *: 랜섬웨어 감지 정책이 할당되었지만 서비스에 오류가 발생했습니다.

BlueXP 랜섬웨어 보호에서 보호가 활성화된 경우 랜섬웨어 감지 정책 상태가 학습 모드에서 활성 모드로 변경되면 경고 감지 및 보고가 시작됩니다.

- 감지 정책 *: 랜섬웨어 감지 정책이 할당된 경우 해당 정책의 이름이 나타납니다. 감지 정책이 할당되지 않은 경우 "해당 없음"이 나타납니다.
- 스냅샷 및 백업 정책 *: 이 열에는 워크로드에 적용된 스냅샷 및 백업 정책과 해당 정책을 관리하는 제품 또는 서비스가 표시됩니다.
- SnapCenter에서 관리합니다
- VMware vSphere용 SnapCenter 플러그인으로 관리됩니다
- BlueXP 백업 및 복구를 통해 관리됩니다
- 스냅샷 및 백업을 관리하는 랜섬웨어 보호 정책의 이름입니다
- 없음
- 워크로드 중요성 *

BlueXP 랜섬웨어 방어는 각 워크로드의 분석을 기반으로 검색 중에 각 워크로드에 중요하거나 우선순위를 할당합니다. 워크로드 중요도는 다음과 같은 스냅샷 빈도에 의해 결정됩니다.

- * 중요 *: 시간당 1개 이상의 스냅샷 복사본 생성(매우 공격적인 보호 일정)
- * 중요 *: 시간당 1개 미만이지만 매일 1개 이상의 스냅샷 복사본을 생성합니다
- * 표준 *: 매일 1개 이상의 스냅샷 복사본이 생성됩니다
- 사전 정의된 감지 정책 *

다음 BlueXP 랜섬웨어 방지 사전 정의된 정책 중 하나를 선택할 수 있으며, 이는 워크로드 중요도에 따라 다릅니다.

정책 레벨	스냅샷	주파수	보존(일)	스냅샷 복사본 수입니다	총 최대 스냅샷 복사본 수입니다
* 중요 워크로드 정책 *	매시간 분기	15분마다	3	288	309
	매일	1일마다	14	14	309
	매주	1주마다	35	5	309
	매월	30일마다	60	2	309
* 중요 워크로드 정책 *	매시간 분기	30분마다	3	144	165
	매일	1일마다	14	14	165
	매주	1주마다	35	5	165
	매월	30일마다	60	2	165
* 표준 워크로드 정책 *	매시간 분기	30분마다	3	72	93
	매일	1일마다	14	14	93
	매주	1주마다	35	5	93
	매월	30일마다	60	2	93

SnapCenter를 통해 애플리케이션 또는 VM 일관성 있는 보호를 지원합니다

애플리케이션 또는 VM 일관성 있는 보호 기능을 활성화하면 애플리케이션 또는 VM 워크로드를 일관된 방식으로 보호할 수 있으며, 복구가 필요한 경우 지연 및 일관된 상태를 유지하여 잠재적인 데이터 손실을 방지할 수 있습니다.

이 프로세스에서 BlueXP 백업 및 복구를 사용하여 애플리케이션용 SnapCenter 소프트웨어 서버 또는 VMware vSphere용 SnapCenter 플러그인의 등록을 시작합니다.

워크로드 정합성이 보장된 보호를 설정하면 BlueXP 랜섬웨어 방어 에서 보호 전략을 관리할 수 있습니다. 이 보호 전략에는 BlueXP 랜섬웨어 보호에서 관리되는 랜섬웨어 감지 정책과 함께 다른 곳에서 관리되는 스냅샷 및 백업 정책이 포함됩니다.

BlueXP 백업 및 복구를 사용하여 VMware vSphere용 SnapCenter 또는 SnapCenter 플러그인을 등록하는 방법에 대해 자세히 알아보려면 다음 정보를 참조하십시오.

- "SnapCenter 서버 소프트웨어를 등록합니다"
- "VMware vSphere용 SnapCenter 플러그인을 등록합니다"

단계

1. BlueXP 랜섬웨어 방어 메뉴에서 * 대시보드 * 를 선택합니다.
2. 권장 사항 창에서 다음 권장 사항 중 하나를 찾아 * 검토 및 수정 * 을 선택합니다.
   - 사용 가능한 SnapCenter 서버를 BlueXP에 등록하십시오
   - BlueXP에 사용 가능한 SCV(VMware vSphere)용 SnapCenter 플러그인을 등록하십시오
3. 정보에 따라 BlueXP 백업 및 복구를 사용하는 VMware vSphere 호스트용 SnapCenter 또는 SnapCenter 플러그인을 등록합니다.
4. BlueXP 랜섬웨어 방어로 되돌아갑니다.
5. BlueXP 랜섬웨어 방어에서 대시보드로 이동하여 검색 프로세스를 다시 시작합니다.
6. BlueXP 랜섬웨어 보호에서 * Protection * 을 선택하여 보호 페이지를 확인하십시오.
7. 보호 페이지의 스냅샷 및 백업 정책 열에서 세부 정보를 검토하여 정책이 다른 곳에서 관리되는지 확인합니다.

랜섬웨어 차단 전략을 추가하십시오

워크로드에 랜섬웨어 보호 전략을 추가할 수 있습니다. 이렇게 하는 방법은 스냅샷과 백업 정책이 이미 있는지 여부에 따라 달라집니다.

- * 스냅샷 또는 백업 정책이 없는 경우 랜섬웨어 방지 전략을 수립하십시오 *. 워크로드에 스냅샷 또는 백업 정책이 없을 경우 BlueXP 랜섬웨어 방어 전략을 생성할 수 있습니다. 랜섬웨어 방지 전략에는 NetApp 랜섬웨어 방어 에서 생성하는 다음과 같은 정책이 포함됩니다.
  - 스냅샷 정책
  - 백업 정책
  - 랜섬웨어 감지 정책
- * 다른 NetApp 제품 또는 서비스에서 관리되는 스냅샷 및 백업 정책이 이미 있는 워크로드에 대한 감지 정책을 생성합니다. * 감지 정책은 다른 제품에서 관리되는 정책을 변경하지 않습니다.

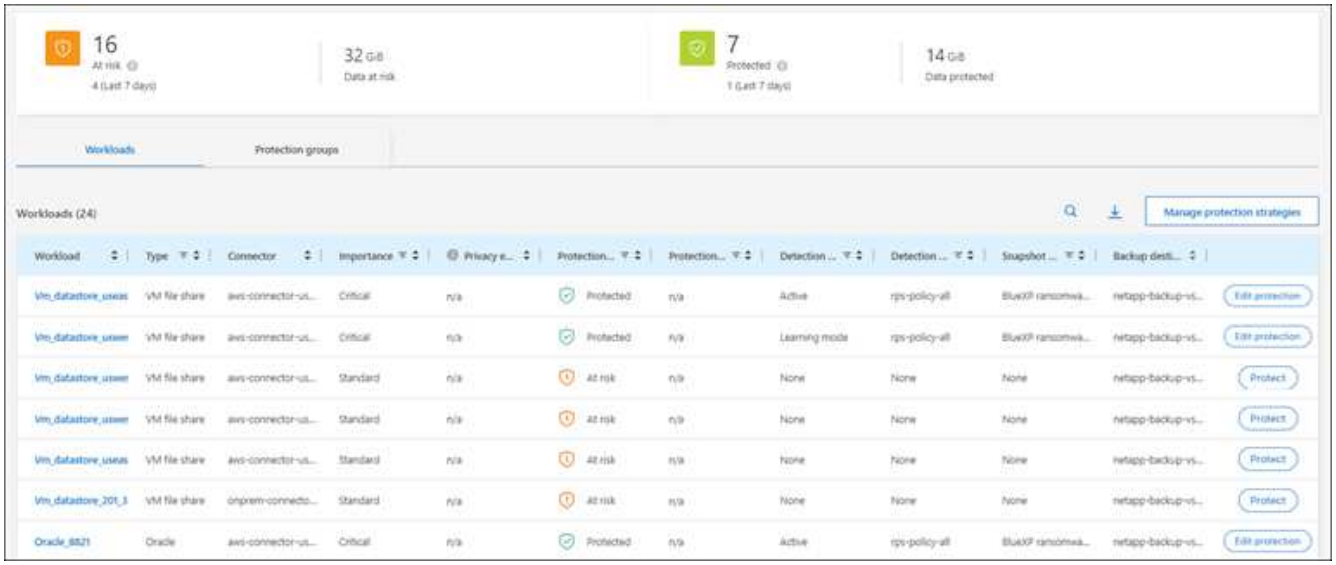
랜섬웨어 보호 전략 생성**(**스냅샷 또는 백업 정책이 없는 경우**)**

워크로드에 스냅샷 또는 백업 정책이 없을 경우 BlueXP 랜섬웨어 방어 전략을 생성할 수 있습니다. 랜섬웨어 방지 전략에는 NetApp 랜섬웨어 방어 에서 생성하는 다음과 같은 정책이 포함됩니다.

- 스냅샷 정책
- 백업 정책
- 랜섬웨어 감지 정책

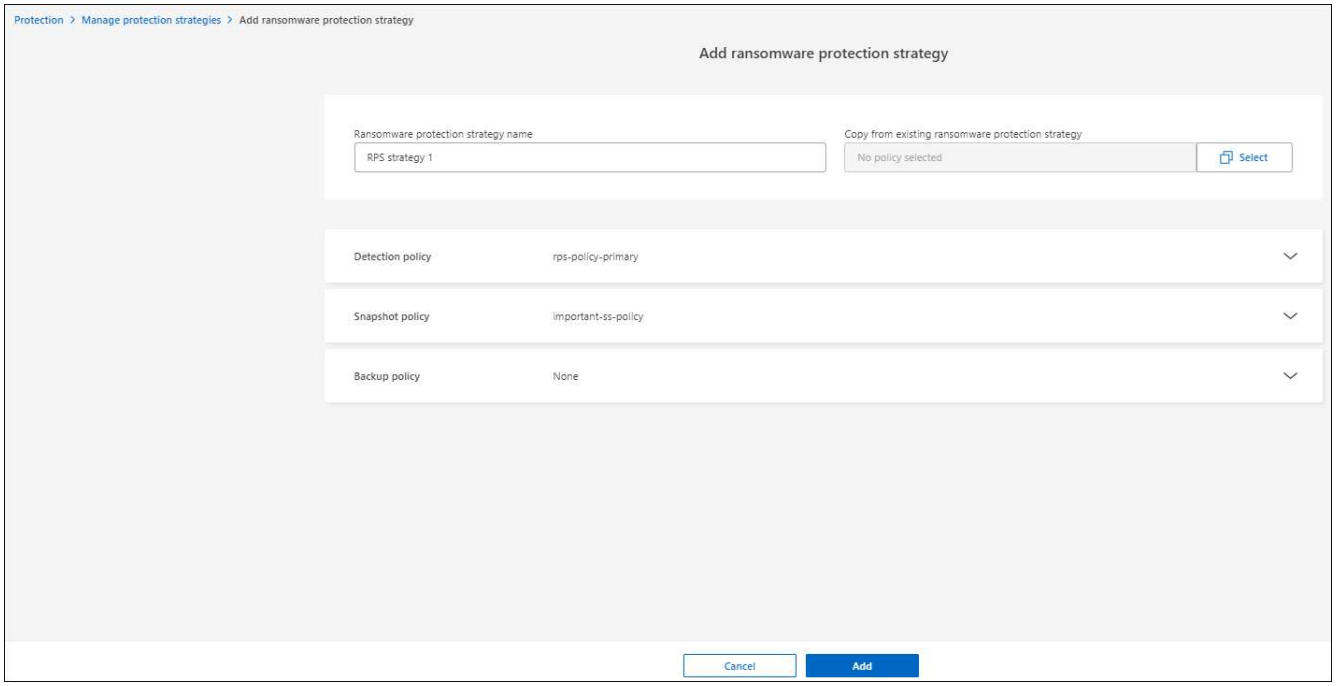
랜섬웨어 차단 전략을 수립하기 위한 단계

1. BlueXP 랜섬웨어 방어 메뉴에서 * 보호 * 를 선택합니다.



2. 보호 페이지에서 * 보호 전략 관리 * 를 선택합니다.

3. 랜섬웨어 방지 전략 페이지에서 * 추가 * 를 선택합니다.



4. 새 전략 이름을 입력하거나 기존 이름을 입력하여 복사합니다. 기존 이름을 입력할 경우 복사할 이름을 선택하고 *

복사 * 를 선택합니다.

기존 전략을 복사하고 수정하도록 선택하면 원래 이름에 "_copy"가 추가됩니다. 이름과 하나 이상의 설정을 변경하여 고유하게 만들어야 합니다.

5. 각 항목에 대해 * 아래쪽 화살표 * 를 선택합니다.

◦ * 감지 정책 *:

▪ * 정책 *: 미리 설계된 감지 정책 중 하나를 선택합니다.

▪ * 기본 감지 *: 랜섬웨어 탐지를 통해 서비스에서 잠재적 랜섬웨어 공격을 감지하도록 지원합니다.

▪ * 파일 확장자 차단 * : 서비스에서 알려진 의심스러운 파일 확장자를 차단하려면 이 기능을 활성화하십시오. 이 서비스는 기본 감지가 활성화될 때 자동화된 스냅샷 복사본을 생성합니다.

차단된 파일 확장명을 변경하려면 System Manager에서 편집합니다.

◦ * 스냅샷 정책 *:

▪ * Snapshot policy base ame *: 정책을 선택하거나 * Create * 를 선택하고 스냅샷 정책의 이름을 입력합니다.

▪ * Snapshot locking *: 랜섬웨어 공격이 백업 스토리지 대상 경로를 관리하더라도 일정 기간 동안 수정하거나 삭제할 수 없도록 기본 스토리지의 스냅샷 복사본을 잠급니다. 이를 _immutable storage_라고도 합니다. 따라서 복구 시간이 단축됩니다.

스냅샷이 잠겨 있으면 볼륨 만료 시간이 스냅샷 복사본의 만료 시간으로 설정됩니다.

스냅샷 복사본 잠금은 ONTAP 9.12.1 이상에서 사용할 수 있습니다. SnapLock에 대한 자세한 내용은 을 참조하십시오 "ONTAP의 SnapLock".

▪ * Snapshot schedules *: 스케줄 옵션, 보관할 스냅샷 복사본 수를 선택하고 스케줄을 사용하도록 선택합니다.

◦ * 백업 정책 *:

▪ * 백업 정책 기본 이름 *: 새 이름을 입력하거나 기존 이름을 선택하십시오.

▪ * 백업 스케줄 * : 보조 스토리지에 대한 스케줄 옵션을 선택하고 스케줄을 활성화합니다.

보조 저장소에 대한 백업 잠금을 활성화하려면 * 설정 * 옵션을 사용하여 백업 대상을 구성하십시오. 자세한 내용은 을 참조하십시오 "설정을 구성합니다".

6. 추가 * 를 선택합니다.

이미 스냅샷 및 백업 정책이 있는 워크로드에 감지 정책을 추가합니다

BlueXP 랜섬웨어 보호를 사용하면 다른 NetApp 제품 또는 서비스에서 관리되는 스냅샷 및 백업 정책이 이미 있는 워크로드에 랜섬웨어 감지 정책을 할당할 수 있습니다. 감지 정책은 다른 제품에서 관리되는 정책을 변경하지 않습니다.

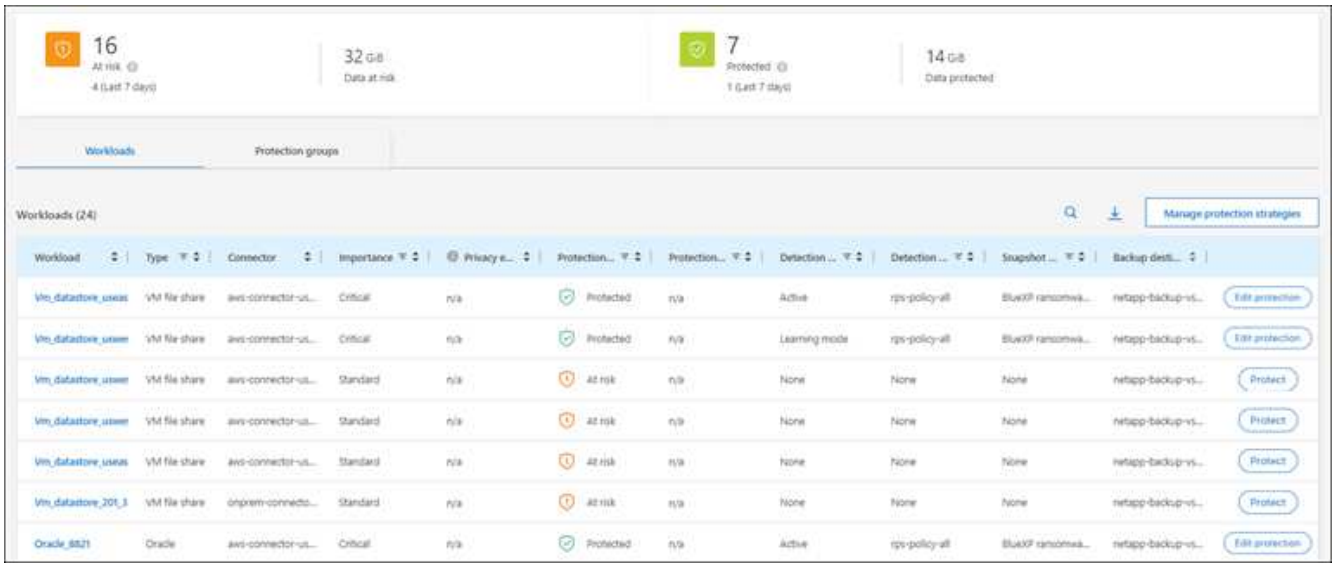
BlueXP 백업, 복구, SnapCenter와 같은 기타 서비스에서는 다음 유형의 정책을 사용하여 워크로드를 제어합니다.

- 스냅샷을 관리하는 정책
- 보조 스토리지에 대한 복제를 관리하는 정책

- 정책: 오브젝트 스토리지에 대한 백업을 관리합니다

단계

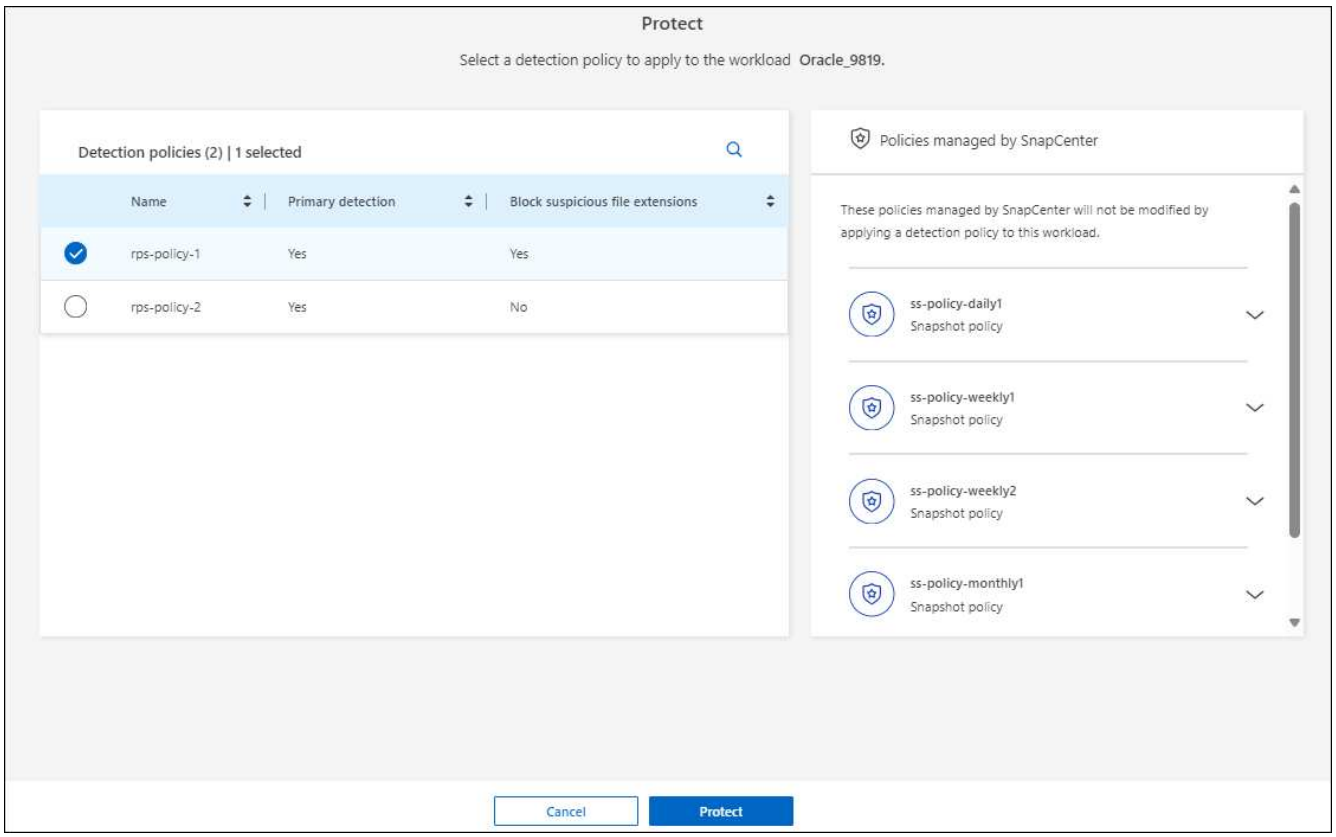
1. BlueXP 랜섬웨어 방어 메뉴에서 * 보호 * 를 선택합니다.



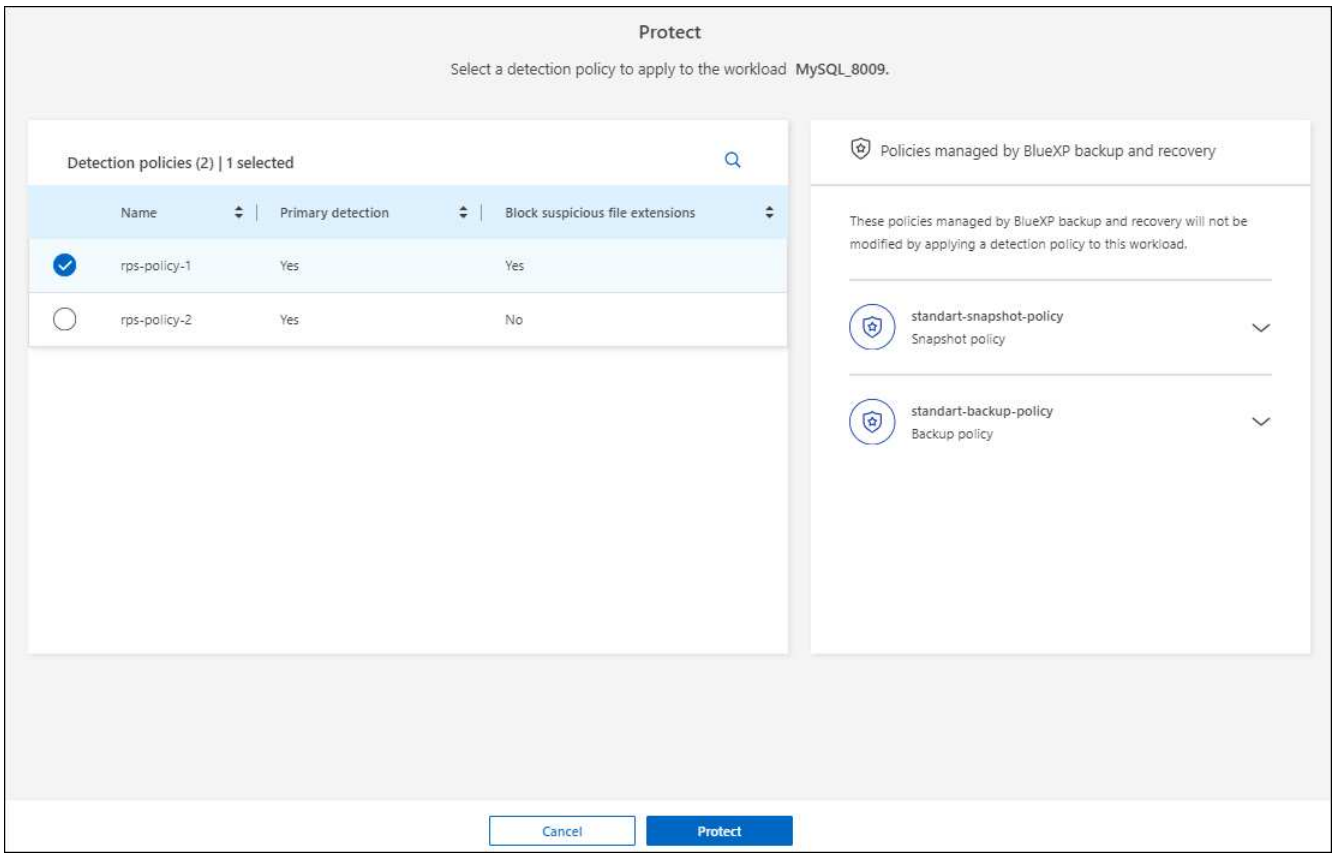
2. 보호 페이지에서 워크로드를 선택하고 * 보호 * 를 선택합니다.

   보호 페이지에는 SnapCenter Software, VMware vSphere용 SnapCenter, BlueXP 백업 및 복구에서 관리하는 정책이 표시됩니다.

   다음 예에서는 SnapCenter에서 관리하는 정책을 보여 줍니다.



다음 예에서는 BlueXP 백업 및 복구를 통해 관리되는 정책을 보여줍니다.



3. 다른 곳에서 관리되는 정책에 대한 자세한 내용을 보려면 * 아래쪽 화살표 * 를 클릭하십시오.
4. 다른 곳에서 관리되는 스냅샷 및 백업 정책 외에 검색 정책을 적용하려면 감지 정책을 선택합니다.
5. protect * 를 선택합니다.
6. 보호 페이지에서 감지 정책 열을 검토하여 할당된 감지 정책을 확인합니다. 또한 스냅샷 및 백업 정책 열에는 정책을 관리하는 제품 또는 서비스의 이름이 표시됩니다.

다른 정책을 할당합니다

현재 보호 정책을 대체하는 다른 보호 정책을 할당할 수 있습니다.

단계

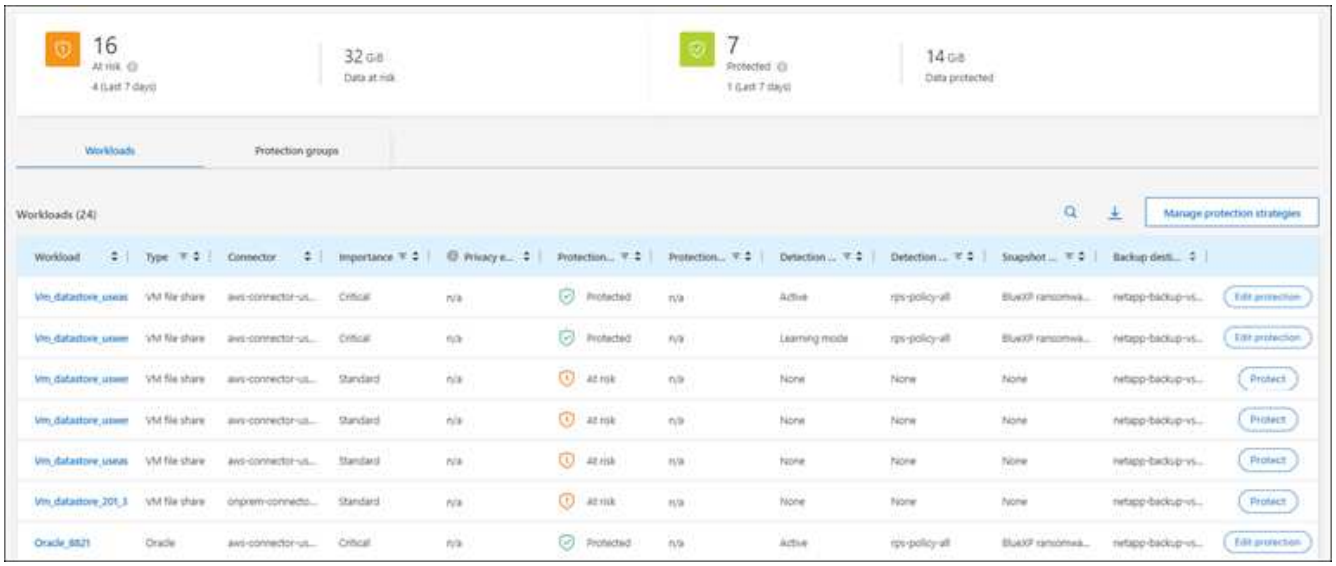
1. BlueXP 랜섬웨어 방어 메뉴에서 * 보호 * 를 선택합니다.
2. 보호 페이지의 워크로드 행에서 * 보호 편집 * 을 선택합니다.
3. 정책 페이지에서 세부 정보를 검토할 정책에 대한 아래쪽 화살표를 클릭합니다.
4. 할당할 정책을 선택합니다.
5. 변경을 완료하려면 * Protect * 를 선택합니다.

파일 공유를 그룹화하여 보다 쉽게 보호할 수 있습니다

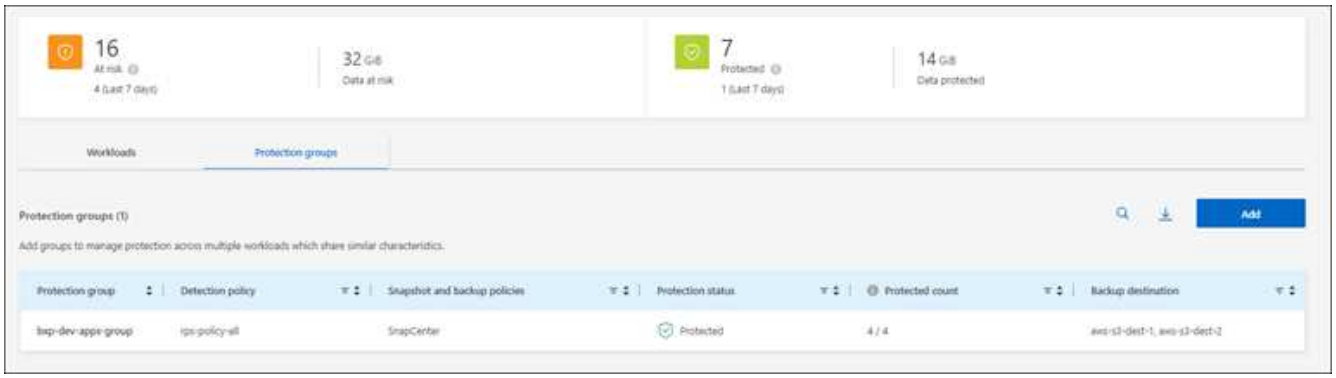
파일 공유를 그룹화하면 데이터 자산을 보다 쉽게 보호할 수 있습니다. 이 서비스는 각 볼륨을 개별적으로 보호하는 대신 그룹의 모든 볼륨을 동시에 보호할 수 있습니다.

단계

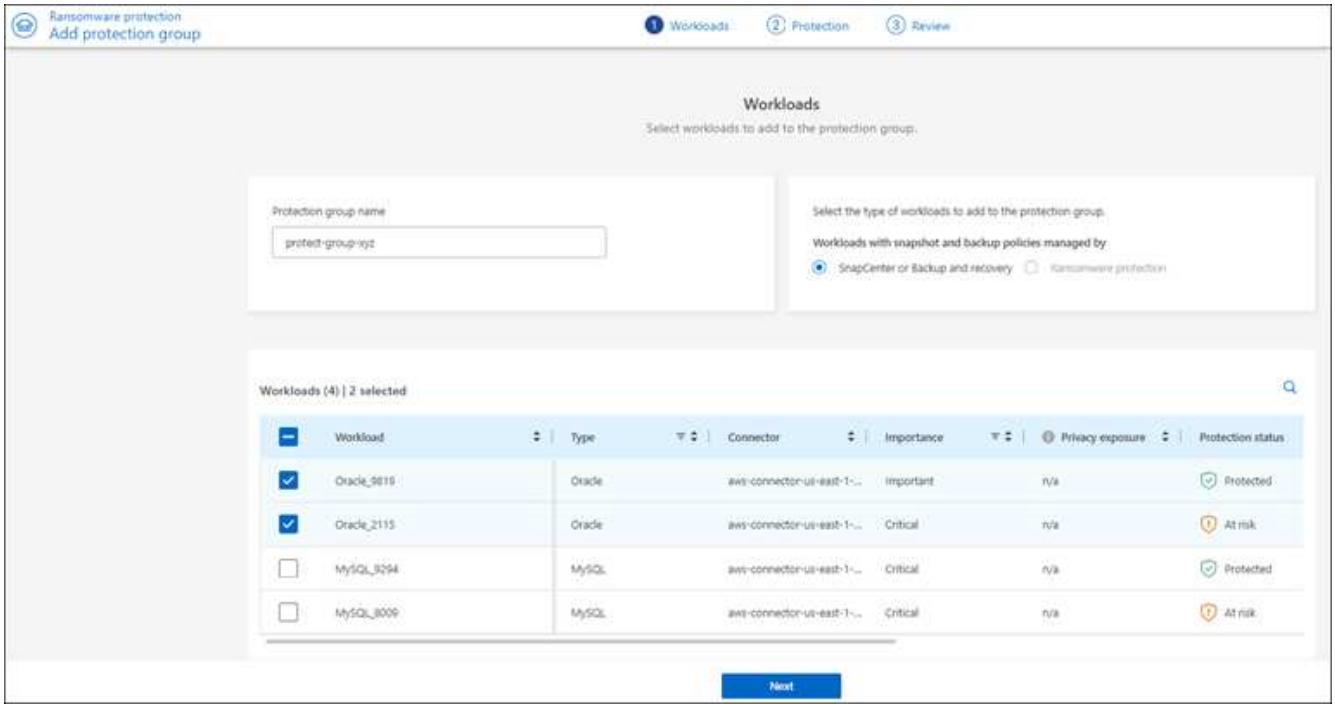
1. BlueXP 랜섬웨어 방어 메뉴에서 * 보호 * 를 선택합니다.



2. 보호 페이지에서 * 보호 그룹 * 탭을 선택합니다.



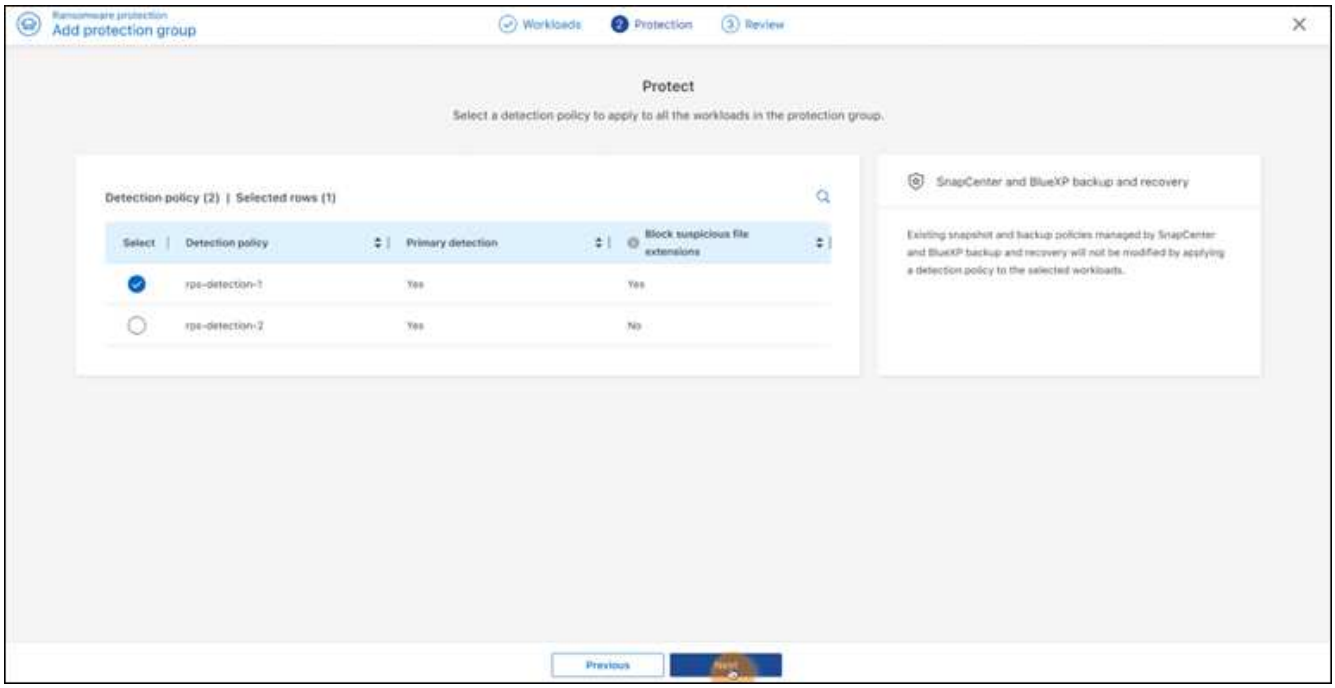
3. 추가 * 를 선택합니다.



4. 보호 그룹의 이름을 입력합니다.
5. 다음 단계 중 하나를 수행합니다.
   a. 보호 정책이 이미 마련되어 있는 경우 다음 중 하나를 통해 관리되는지 여부를 기준으로 워크로드를 그룹화할지 여부를 선택합니다.
      - BlueXP 랜섬웨어 보호
      - SnapCenter 또는 BlueXP 백업 및 복구
   b. 보호 정책이 이미 마련되어 있지 않은 경우 페이지에 사전 구성된 랜섬웨어 보호 전략이 표시됩니다.
      i. 그룹을 보호할 그룹을 선택하고 * 다음 * 을 선택합니다.
      ii. 선택한 워크로드에 여러 작업 환경에 볼륨이 있는 경우, 클라우드에 백업할 수 있도록 여러 작업 환경의 백업 대상을 선택합니다.
6. 그룹에 추가할 워크로드를 선택합니다.

   작업 부하에 대한 자세한 내용을 보려면 오른쪽으로 스크롤합니다.

7. 다음 * 을 선택합니다.



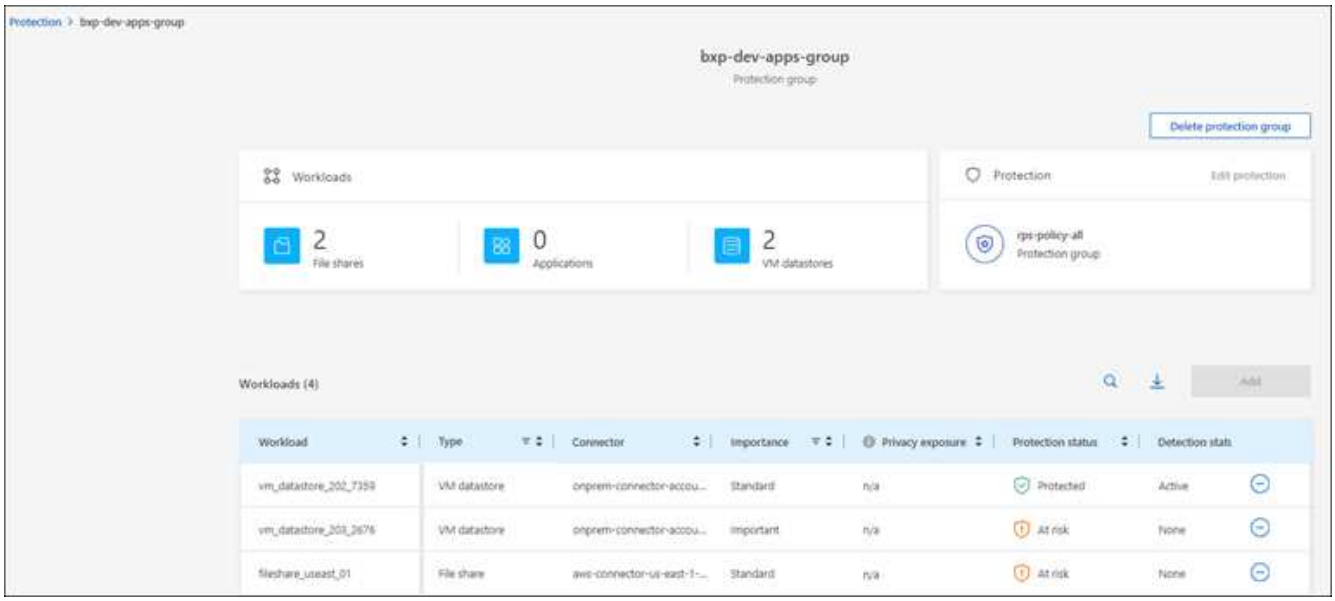
8. 이 그룹의 보호를 제어할 정책을 선택합니다.
9. 다음 * 을 선택합니다.
10. 보호 그룹에 대한 선택 항목을 검토합니다.
11. 추가 * 를 선택합니다.

그룹에서 워크로드를 제거합니다

나중에 기존 그룹에서 워크로드를 제거해야 할 수도 있습니다.

단계

1. BlueXP 랜섬웨어 방어 메뉴에서 * 보호 * 를 선택합니다.
2. 보호 페이지에서 * 보호 그룹 * 탭을 선택합니다.
3. 하나 이상의 워크로드를 제거할 그룹을 선택합니다.



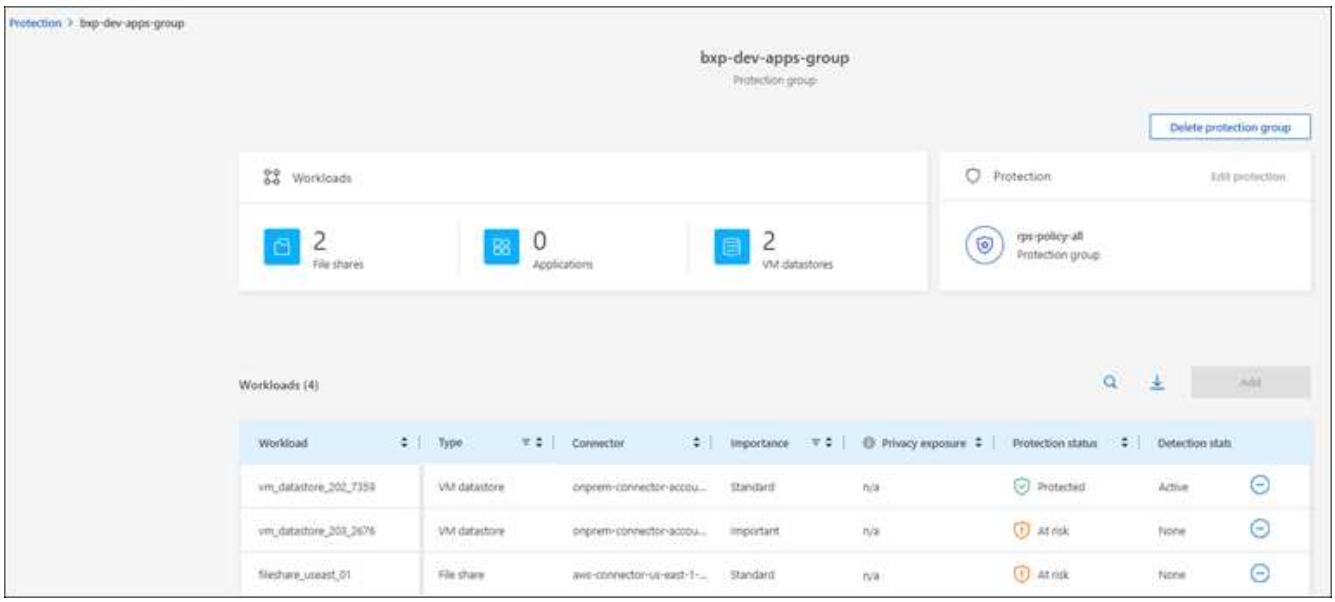
4. 선택한 보호 그룹 페이지에서 그룹에서 제거할 워크로드를 선택하고 * 작업 * 옵션을 선택합니다.•••
5. 작업 메뉴에서 * 작업 부하 제거 * 를 선택합니다.
6. 작업 부하를 제거할지 확인하고 * 제거 * 를 선택합니다.

보호 그룹을 삭제합니다

보호 그룹을 삭제하면 그룹 및 해당 보호가 제거되지만 개별 워크로드가 제거되지는 않습니다.

단계

1. BlueXP 랜섬웨어 방어 메뉴에서 * 보호 * 를 선택합니다.
2. 보호 페이지에서 * 보호 그룹 * 탭을 선택합니다.
3. 하나 이상의 워크로드를 제거할 그룹을 선택합니다.



4. 선택한 보호 그룹 페이지의 오른쪽 위에서 * Delete protection group * 을 선택합니다.

5. 그룹을 삭제할 것인지 확인하고 * Delete * 를 선택합니다.

랜섬웨어 방지 전략 관리

랜섬웨어 전략은 삭제할 수 있습니다.

랜섬웨어 차단 전략으로 보호되는 워크로드를 확인하십시오

랜섬웨어 보호 전략을 삭제하기 전에 해당 전략으로 보호되는 워크로드를 확인할 수 있습니다.

전략 목록에서 또는 특정 전략을 편집할 때 워크로드를 볼 수 있습니다.

전략 목록을 볼 때의 단계

1. BlueXP 랜섬웨어 방어 메뉴에서 * 보호 * 를 선택합니다.
2. 보호 페이지에서 * 보호 전략 관리 * 를 선택합니다.

   랜섬웨어 방지 전략 페이지에는 전략 목록이 표시됩니다.

3. 랜섬웨어 보호 전략 페이지의 보호된 워크로드 열에서 행 끝에 있는 아래쪽 화살표를 클릭합니다.

랜섬웨어 차단 전략을 삭제합니다

현재 워크로드와 연결되어 있지 않은 보호 전략을 삭제할 수 있습니다.

단계

1. BlueXP 랜섬웨어 방어 메뉴에서 * 보호 * 를 선택합니다.
2. 보호 페이지에서 * 보호 전략 관리 * 를 선택합니다.
3. 전략 관리 페이지에서 삭제할 전략에 대한 * 작업 * 옵션을 선택합니다 ••• .
4. 작업 메뉴에서 * 정책 삭제 * 를 선택합니다.

BlueXP 분류를 사용하여 개인 식별 정보를 검색합니다

BlueXP 랜섬웨어 차단 서비스 내에서 BlueXP 제품군의 핵심 구성요소인 BlueXP 분류를 사용하여 파일 공유 워크로드에서 데이터를 스캔하고 분류할 수 있습니다. 데이터를 분류하면 데이터에 PII(개인 식별 정보)가 포함되어 있는지 여부를 식별하는 데 도움이 되므로 보안 위험이

증가할 수 있습니다.

이 프로세스는 작업 부하의 중요도에 영향을 주어 적절한 보호 기능을 갖추도록 할 수 있습니다.

BlueXP 분류를 활성화합니다

BlueXP 랜섬웨어 보호 서비스 내에서 BlueXP 분류를 사용하려면 먼저 BlueXP 분류를 활성화하여 데이터를 스캔해야 합니다.

관리자는 BlueXP 분류 UI를 대체 방법으로 사용하여 BlueXP 랜섬웨어 보호에서 BlueXP 분류를 활성화할 수 있습니다.

서비스를 사용하기 전에 다음과 같은 BlueXP 분류 리소스를 검토하는 것이 도움이 될 수 있습니다.

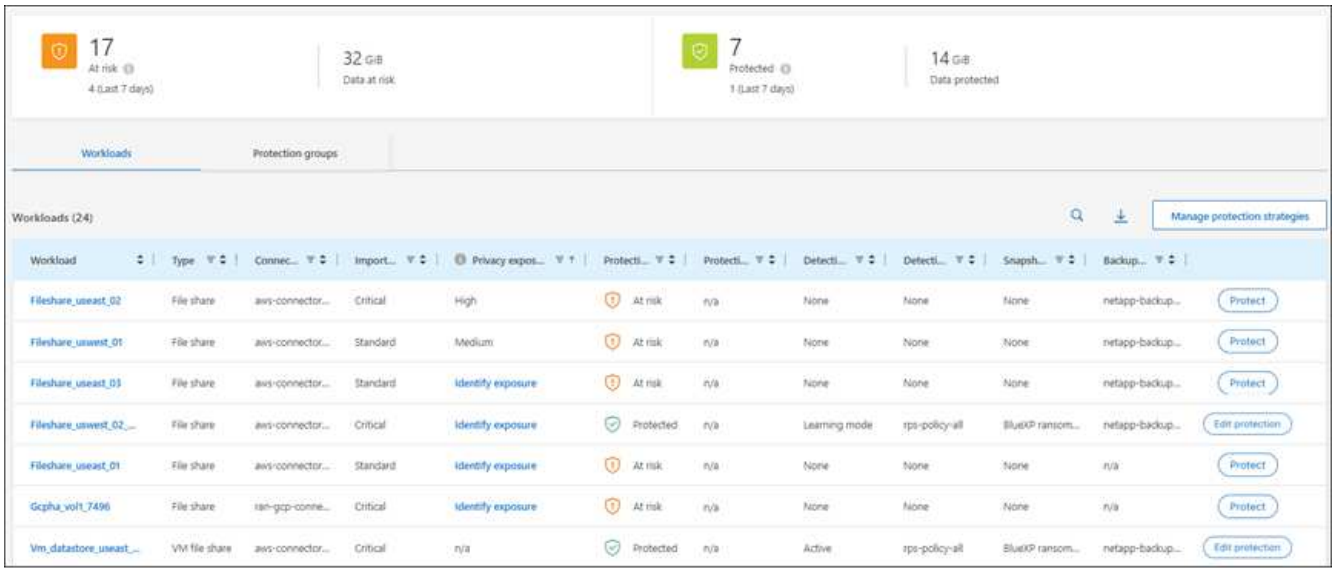
- "BlueXP 분류에 대해 알아보십시오"
- "개인 데이터의 범주입니다"
- "조직에 저장된 데이터를 조사합니다"

시작하기 전에

BlueXP 랜섬웨어 차단에서 PII 데이터를 스캔하는 것은 BlueXP 분류를 구축한 고객에게 제공됩니다. BlueXP 분류는 BlueXP 플랫폼의 일부로 추가 비용 없이 사용할 수 있으며 사내 또는 고객 클라우드에 구축할 수 있습니다.

단계

1. BlueXP 랜섬웨어 방어 메뉴에서 * 보호 * 를 선택합니다.
2. 보호 페이지의 워크로드 열에서 파일 공유 워크로드를 찾습니다.



3. BlueXP 분류를 사용하여 개인 식별 데이터를 스캔하려면 * 개인 정보 노출 * 열에서 * 노출 식별 * 을 선택합니다.

결과

데이터 양에 따라 검색하는 데 몇 분이 걸릴 수 있습니다. 보호 페이지는 BlueXP 분류가 파일을 식별하고 스캔 중인 파일의 수를 표시합니다.

스캔이 완료되면 프라이버시 노출 열에 노출 수준이 낮음, 중간 또는 높음으로 표시됩니다.

개인 정보 노출을 검토합니다

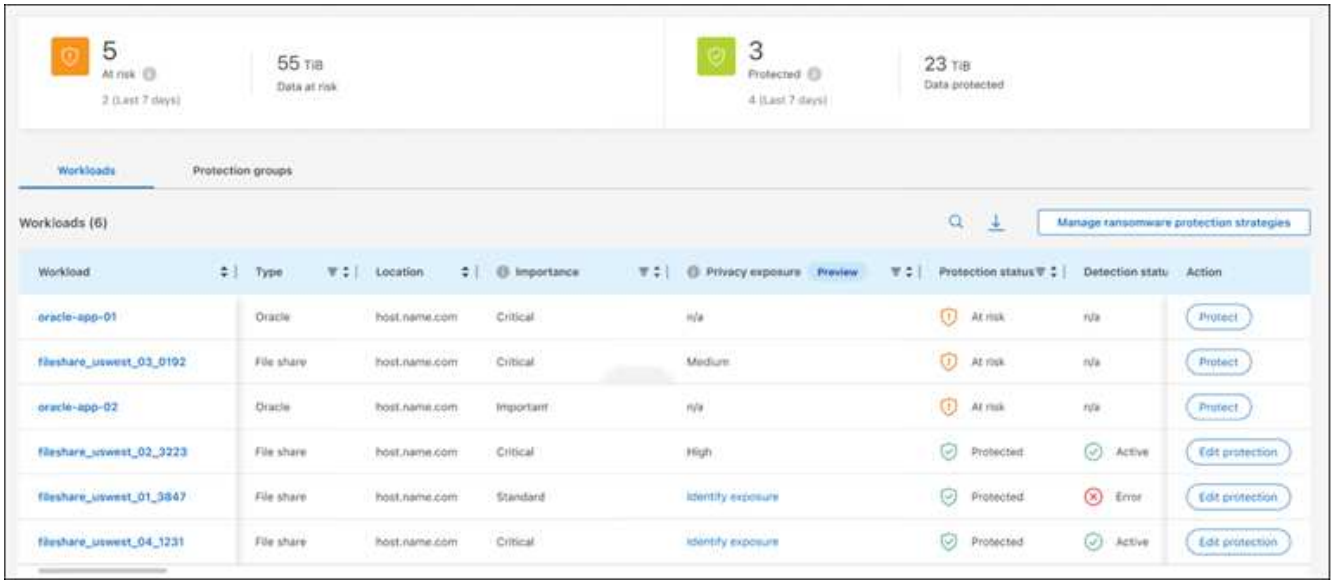
BlueXP 분류에서 PII(개인 식별 정보)를 검색한 후 PII 데이터 위험을 확인할 수 있습니다.

PII 데이터는 다음과 같은 개인정보 노출 위험 상태 중 하나를 가질 수 있습니다.

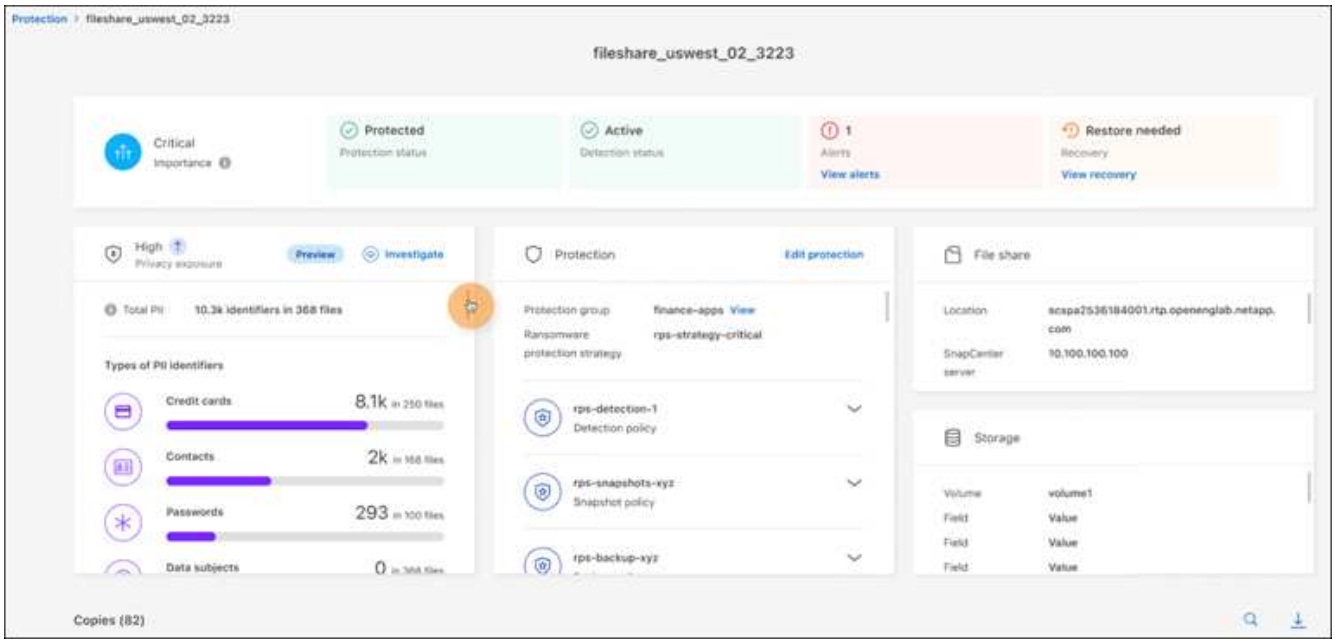
- * 높음 *: 파일의 70% 이상이 PII를 가지고 있습니다
- * 중간 *: 30% 이상, 70% 미만의 파일에 PII가 있습니다
- * 낮음 *: 0보다 크고 30% 미만의 파일에 PII가 있습니다

단계

1. BlueXP 랜섬웨어 방어 메뉴에서 * 보호 * 를 선택합니다.
2. 보호 페이지의 워크로드 열에서 개인 정보 노출 열에 상태가 표시된 파일 공유 워크로드를 찾습니다.



3. 워크로드 세부 정보를 보려면 워크로드 열에서 워크로드 링크를 선택합니다.



4. 워크로드 세부 정보 페이지에서 개인 정보 노출 타일의 정보를 검토합니다.

개인 정보 노출이 워크로드 중요도에 미치는 영향

개인 정보 노출 변경은 작업 부하의 중요성에 영향을 줄 수 있습니다.

프라이버시 노출 시:	이 개인 정보 노출에서:	개인 정보 노출:	워크로드의 중요성은 다음과 같습니다.
* 감소 *	높음, 중간 또는 낮음	중간, 낮음 또는 없음	그대로 유지됩니다
* 증가 *	없음	낮음	표준 상태로 유지됩니다
	낮음	중간	표준에서 중요로 변경
	낮음 또는 중간	높음	표준 또는 중요에서 긴급으로 변경

를 참조하십시오

BlueXP 분류에 대한 자세한 내용은 다음 BlueXP 분류 항목을 참조하십시오.

- "BlueXP 분류에 대해 알아보십시오"
- "개인 데이터의 범주입니다"
- "조직에 저장된 데이터를 조사합니다"