NetApp Ransomware Resilience 설명서

NetApp Ransomware Resilience

NetApp
October 31, 2025

목차

NetApp Ransomware Resilience 설명서

릴리스 노트

NetApp Ransomware Resilience 의 새로운 기능

NetApp Ransomware Resilience 의 새로운 기능을 알아보세요.

2025년 10월 6일

BlueXP ransomware protection 이제 **NetApp Ransomware Resilience** 습니다**.**

BlueXP ransomware protection 서비스의 이름이 NetApp Ransomware Resilience 로 변경되었습니다.

BlueXP 는 이제 **NetApp Console** 입니다**.**

NetApp Console 엔터프라이즈급 온프레미스 및 클라우드 환경 전반의 스토리지 및 데이터 서비스를 중앙에서 관리하여 실시간 통찰력, 더 빠른 워크플로, 간소화된 관리를 제공합니다.

변경된 사항에 대한 자세한 내용은 다음을 참조하세요. "NetApp Console 릴리스 노트" .

데이터 침해 감지

랜섬웨어 복원력에는 몇 단계만으로 활성화할 수 있는 새로운 감지 메커니즘이 포함되어 있어 데이터 침해의 조기 지표로 비정상적인 사용자 읽기를 감지합니다. 랜섬웨어 복원력은 과거 데이터에서 예상되는 정상적인 동작 프로필인 과거 기준선을 생성하여 사용자 읽기 이벤트를 수집하고 분석합니다. 새로운 사용자 활동이 이러한 기존 기준에서 크게 벗어나는 경우(예상치 못한 읽기 급증과 의심스러운 읽기 패턴이 결합된 경우) 알림이 생성됩니다. 랜섬웨어 복원력에는 의심스러운 읽기 패턴을 감지하는 AI 모델이 포함되어 있습니다.

저장 계층에서 ARP를 통한 암호화 감지와 달리, Ransomware Resilience SaaS 서비스에서는 FPolicy 이벤트를 수집하여 사용자 동작 이상을 감지합니다.

> 새로운 것을 사용해야 합니다"랜섬웨어 복원력 사용자 동작 관리자 및 랜섬웨어 복원력 사용자 동작 뷰어" 의심스러운 사용자 행동 감지 설정에 액세스하는 역할입니다.

자세한 내용은 다음을 참조하세요."의심스러운 사용자 활동 감지 활성화" 그리고"비정상적인 사용자 동작 보기" .

추가적으로 의심스러운 사용자 활동 감지

Ransomware Resilience는 데이터 침해 감지 외에도 관찰된 의심스러운 사용자 활동을 기반으로 다음과 같은 알림 유형을 감지합니다.

- 데이터 파괴 - 잠재적 공격 - 파일 삭제 수가 기존 기준을 초과하면 잠재적 공격의 심각도를 알려주는 알림이 생성됩니다.
- 의심스러운 사용자 동작 - 잠재적 공격 - 랜섬웨어 공격과 유사한 순서로 읽기, 이름 바꾸기 및 삭제 작업이 관찰되면 잠재적 공격의 심각도를 알려주는 경고가 생성됩니다.
- 의심스러운 사용자 동작 - 경고 - 파일 활동(읽기, 삭제, 이름 바꾸기 등)의 총 수가 이전 기준을 초과하면 경고 심각도의 알림이 생성됩니다.

데이터 침해 감지를 위한 새로운 사용자 역할

의심스러운 사용자 활동 알림을 관리하기 위해 Ransomware Resilience는 콘솔 조직 관리자가 의심스러운 사용자 활동 감지에 대한 액세스 권한을 부여할 수 있는 두 가지 새로운 역할, 즉 Ransomware Resilience 사용자 동작 관리자와 Ransomware Resilience 사용자 동작 뷰어를 도입했습니다.

의심스러운 사용자 동작 설정을 구성하려면 사용자 동작 관리자여야 합니다. 랜섬웨어 복원력 관리자 역할은 의심스러운 사용자 동작 설정을 구성하는 데 지원되지 않습니다.

자세한 내용은 다음을 참조하세요. "NetApp Ransomware Resilience 역할 기반 액세스" .

2025년 8월 12일

이 릴리스에는 일반적인 개선 사항 및 개선 사항이 포함되어 있습니다.

2025년 7월 15일

SAN 워크로드 지원

이 릴리스에는 BlueXP ransomware protection 의 SAN 워크로드에 대한 지원이 포함되어 있습니다. 이제 NFS 및 CIFS 워크로드뿐만 아니라 SAN 워크로드도 보호할 수 있습니다.

자세한 내용은 다음을 참조하세요. "BlueXP ransomware protection 전제 조건" .

향상된 작업 부하 보호

이 릴리스에서는 SnapCenter 나 BlueXP backup and recovery 와 같은 다른 NetApp 도구의 스냅샷 및 백업 정책을 사용하는 워크로드에 대한 구성 프로세스가 개선되었습니다. 이전 릴리스에서는 BlueXP ransomware protection 다른 도구의 정책을 발견하여 사용자가 감지 정책을 변경할 수만 있었습니다. 이 릴리스를 사용하면 스냅샷 및 백업 정책을 BlueXP ransomware protection 정책으로 바꾸거나 다른 도구의 정책을 계속 사용할 수 있습니다.

자세한 내용은 다음을 참조하세요."작업 부하 보호" .

이메일 알림

BlueXP ransomware protection 잠재적인 공격을 감지하면 BlueXP 알림에 알림이 나타나고, 사용자가 구성한 이메일 주소로 이메일이 전송됩니다.

이메일에는 심각도, 영향을 받는 작업 부하, BlueXP ransomware protection 알림 탭의 알림에 대한 링크에 대한 정보가 포함되어 있습니다.

BlueXP ransomware protection 에서 SIEM(보안 및 이벤트 관리) 시스템을 구성한 경우 해당 서비스는 SIEM 시스템으로 경고 세부 정보를 전송합니다.

자세한 내용은 다음을 참조하세요."감지된 랜섬웨어 알림 처리" .

2025년 6월 9일

랜딩 페이지 업데이트

이번 릴리스에는 BlueXP ransomware protection 의 랜딩 페이지가 업데이트되어 무료 평가판 시작과 검색이 더욱 쉬워졌습니다.

준비 훈련 업데이트

이전에는 새로운 샘플 워크로드에 대한 공격을 시뮬레이션하여 랜섬웨어 대비 훈련을 실행할 수 있었습니다. 이 기능을 사용하면 시뮬레이션된 공격을 조사하고 작업 부하를 복구할 수 있습니다. 이 기능을 사용하여 경고 알림, 대응 및 복구를 테스트하세요. 필요한 만큼 자주 이 훈련을 실행하고 일정을 잡으세요.

이번 릴리스에서는 BlueXP ransomware protection 대시보드의 새 버튼을 사용하여 테스트 워크로드에 대한 랜섬웨어 준비 훈련을 실행할 수 있습니다. 이를 통해 제어된 환경 내에서 랜섬웨어 공격을 시뮬레이션하고, 그 영향을 조사하고, 워크로드를 효율적으로 복구하기가 더 쉬워졌습니다.

이제 NFS 워크로드뿐만 아니라 CIFS(SMB) 워크로드에 대한 준비 훈련을 실행할 수 있습니다.

자세한 내용은 다음을 참조하세요. "랜섬웨어 공격 대비 훈련을 실시하세요" .

BlueXP classification 업데이트 활성화

BlueXP ransomware protection 서비스 내에서 BlueXP classification 사용하기 전에 BlueXP classification 활성화하여 데이터를 검사해야 합니다. 데이터를 분류하면 개인 식별 정보(PII)를 찾는 데 도움이 되며, 이는 보안 위험을 증가시킬 수 있습니다.

BlueXP ransomware protection 내에서 파일 공유 워크로드에 BlueXP classification 배포할 수 있습니다. 개인정보 노출 열에서 노출 식별 옵션을 선택합니다. 분류 서비스를 활성화한 경우 이 작업을 통해 노출을 식별할 수 있습니다. 그렇지 않은 경우, 이 릴리스에서는 대화 상자에 BlueXP classification 배포할 수 있는 옵션이 표시됩니다. *배포*를 선택하면 BlueXP classification 서비스 랜딩 페이지로 이동하여 해당 서비스를 배포할 수 있습니다. 여

자세한 내용은 다음을 참조하세요. "클라우드에 BlueXP classification 배포" BlueXP ransomware protection 서비스를 사용하려면 다음을 참조하세요. "BlueXP classification 사용하여 개인 식별 정보를 스캔하세요" .

2025년 5월 13일

BlueXP ransomware protection 에서 지원되지 않는 작업 환경 보고

검색 워크플로 중에 지원되는 워크로드 또는 지원되지 않는 워크로드 위에 마우스를 올리면 BlueXP ransomware protection 더 자세한 정보를 보고합니다. 이를 통해 일부 워크로드가 BlueXP ransomware protection 서비스에서 발견되지 않는 이유를 이해하는 데 도움이 됩니다.

서비스가 작업 환경을 지원하지 않는 데에는 여러 가지 이유가 있습니다. 예를 들어, 작업 환경의 ONTAP 버전이 필요한 버전보다 낮을 수 있습니다. 지원되지 않는 작업 환경 위에 마우스를 올리면 툴팁에 그 이유가 표시됩니다.

초기 검색 중에 지원되지 않는 작업 환경을 볼 수 있으며, 결과를 다운로드할 수도 있습니다. 설정 페이지의 워크로드 검색 옵션에서 검색 결과를 볼 수도 있습니다.

자세한 내용은 다음을 참조하세요. "BlueXP ransomware protection 에서 워크로드를 발견하세요" .

2025년 4월 29일

Amazon FSx for NetApp ONTAP 지원

이 릴리스는 Amazon FSx for NetApp ONTAP 지원합니다. 이 기능은 BlueXP ransomware protection 기능으로 FSx for ONTAP 워크로드를 보호하는 데 도움이 됩니다.

FSx for ONTAP 클라우드에서 NetApp ONTAP 스토리지의 성능을 제공하는 완전 관리형 서비스입니다.

온프레미스에서 사용하는 것과 동일한 기능, 성능 및 관리 기능을 제공하며, 기본 AWS 서비스의 민첩성과 확장성을 갖추고 있습니다.

BlueXP ransomware protection 워크플로에 다음과 같은 변경 사항이 적용되었습니다.

- Discovery에는 FSx for ONTAP 9.15 작업 환경의 워크로드가 포함됩니다.
- 보호 탭에는 FSx for ONTAP 환경의 워크로드가 표시됩니다. 이 환경에서는 FSx for ONTAP 백업 서비스를 사용하여 백업 작업을 수행해야 합니다. BlueXP ransomware protection 스냅샷을 사용하여 이러한 작업 부하를 복원할 수 있습니다.

FSx for ONTAP 에서 실행되는 워크로드에 대한 백업 정책은 BlueXP 에서 설정할 수 없습니다. Amazon FSx for NetApp ONTAP 에 설정된 기존 백업 정책은 변경되지 않습니다.

- 경고 사건은 새로운 FSx for ONTAP 작업 환경을 보여줍니다.

자세한 내용은 다음을 참조하세요. "BlueXP ransomware protection 및 작업 환경에 대해 알아보세요" .

지원되는 옵션에 대한 정보는 다음을 참조하세요. "BlueXP ransomware protection 제한 사항" .

BlueXP 액세스 역할이 필요합니다

이제 BlueXP ransomware protection 보고, 검색하고, 관리하려면 다음 액세스 역할 중 하나가 필요합니다. 조직 관리자, 폴더 또는 프로젝트 관리자, 랜섬웨어 보호 관리자 또는 랜섬웨어 보호 뷰어.

"모든 서비스에 대한 BlueXP 액세스 역할에 대해 알아보세요" .

2025년 4월 14일

준비 훈련 보고서

이번 릴리스에서는 랜섬웨어 공격 대비 훈련 보고서를 검토할 수 있습니다. 준비 훈련을 통해 새로 생성된 샘플 워크로드에 대한 랜섬웨어 공격을 시뮬레이션할 수 있습니다. 그런 다음 시뮬레이션된 공격을 조사하고 샘플 작업 부하를 복구합니다. 이 기능은 경고 알림, 대응 및 복구 프로세스를 테스트하여 실제 랜섬웨어 공격이 발생할 경우 대비가 되어 있는지 확인하는 데 도움이 됩니다.

자세한 내용은 다음을 참조하세요. "랜섬웨어 공격 대비 훈련을 실시하세요" .

새로운 역할 기반 액세스 제어 역할 및 권한

이전에는 사용자의 책임에 따라 역할과 권한을 할당하여 BlueXP ransomware protection 에 대한 사용자 액세스를 관리하는 데 도움이 되었습니다. 이번 릴리스에서는 업데이트된 권한을 갖춘 BlueXP ransomware protection 에 특화된 두 가지 새로운 역할이 추가되었습니다. 새로운 역할은 다음과 같습니다.

- 랜섬웨어 보호 관리자
- 랜섬웨어 보호 뷰어

권한에 대한 자세한 내용은 다음을 참조하세요. "BlueXP ransomware protection 역할 기반 기능 액세스" .

결제 개선

이번 릴리스에는 결제 프로세스에 대한 여러 가지 개선 사항이 포함되어 있습니다.

자세한 내용은 다음을 참조하세요. "라이센싱 및 지불 옵션 설정" .

2025년 3월 10일

공격을 시뮬레이션하고 대응하세요

이 릴리스에서는 랜섬웨어 경고에 대한 대응을 테스트하기 위해 랜섬웨어 공격을 시뮬레이션합니다. 이 기능은 경고 알림, 대응 및 복구 프로세스를 테스트하여 실제 랜섬웨어 공격이 발생할 경우 대비가 되어 있는지 확인하는 데 도움이 됩니다.

자세한 내용은 다음을 참조하세요. "랜섬웨어 공격 대비 훈련을 실시하세요" .

발견 프로세스 개선

이 릴리스에는 선택적 검색 및 재발견 프로세스에 대한 개선 사항이 포함되어 있습니다.

- 이 릴리스에서는 이전에 선택한 작업 환경에 추가된 새로 생성된 워크로드를 검색할 수 있습니다.
- 이번 릴리스에서는 새로운 작업 환경을 선택할 수도 있습니다. 이 기능은 환경에 추가된 새로운 워크로드를 보호하는 데 도움이 됩니다.
- 이러한 검색 프로세스는 초기 검색 프로세스 중에 또는 설정 옵션 내에서 수행할 수 있습니다.

자세한 내용은 다음을 참조하세요. "이전에 선택한 작업 환경에 대해 새로 생성된 작업 부하를 검색합니다." 그리고 "설정 옵션을 사용하여 기능 구성" .

높은 암호화가 감지되면 경고가 발생합니다.

이 릴리스를 사용하면 높은 수준의 파일 확장자를 변경하지 않아도 워크로드에서 높은 수준의 암호화가 감지되면 알림을 볼 수 있습니다. ONTAP Autonomous Ransomware Protection(ARP) AI를 사용하는 이 기능은 랜섬웨어 공격 위험이 있는 워크로드를 식별하는 데 도움이 됩니다. 이 기능을 사용하면 확장자가 변경되었는지 여부와 관계없이 영향을 받은 파일의 전체 목록을 다운로드할 수 있습니다.

자세한 내용은 다음을 참조하세요. "감지된 랜섬웨어 경고에 대응하세요" .

2024년 12월 16일

Data Infrastructure Insights Storage Workload Security를 사용하여 비정상적인 사용자 동작을 감지합니다.

이 릴리스에서는 Data Infrastructure Insights Storage Workload Security를 사용하여 스토리지 워크로드에서 비정상적인 사용자 동작을 감지할 수 있습니다. 이 기능은 잠재적인 보안 위협을 식별하고 잠재적으로 악의적인 사용자를 차단하여 데이터를 보호하는 데 도움이 됩니다.

자세한 내용은 다음을 참조하세요. "감지된 랜섬웨어 경고에 대응하세요" .

Data Infrastructure Insights Storage Workload Security를 사용하여 비정상적인 사용자 동작을 감지하기 전에 BlueXP ransomware protection 설정 옵션을 사용하여 옵션을 구성해야 합니다.

참조하다 "BlueXP ransomware protection 설정 구성" .

검색하고 보호할 작업 부하 선택

이 릴리스를 사용하면 이제 다음 작업을 수행할 수 있습니다.

- 각 커넥터 내에서 워크로드를 검색할 작업 환경을 선택합니다. 환경 내 특정 작업 부하만 보호하고 다른 작업 부하에는 영향을 미치지 않으려는 경우 이 기능이 유용할 수 있습니다.
- 워크로드 검색 중에 커넥터별로 워크로드를 자동으로 검색하도록 설정할 수 있습니다. 이 기능을 사용하면 보호하려는 작업 부하를 선택할 수 있습니다.
- 이전에 선택한 작업 환경에 대해 새로 생성된 작업 부하를 찾아보세요.

참조하다 "워크로드 검색" .

2024년 11월 7일

데이터 분류를 활성화하고 개인 식별 정보(PII)를 스캔합니다.

이 릴리스를 사용하면 BlueXP classification 제품군의 핵심 구성 요소인 BlueXP 분류를 사용하여 파일 공유 워크로드의 데이터를 스캔하고 분류할 수 있습니다. 데이터를 분류하면 데이터에 개인 정보나 비공개 정보가 포함되어 있는지 식별하는 데 도움이 되며, 이는 보안 위험을 증가시킬 수 있습니다. 이 프로세스는 워크로드 중요도에도 영향을 미치며 적절한 수준의 보호로 워크로드를 보호하고 있는지 확인하는 데 도움이 됩니다.

BlueXP ransomware protection 에서 PII 데이터 스캔은 일반적으로 BlueXP classification 배포한 고객에게 제공됩니다. BlueXP classification 추가 비용 없이 BlueXP 플랫폼의 일부로 제공되며 온프레미스 또는 고객 클라우드에 배포할 수 있습니다.

참조하다 "BlueXP ransomware protection 설정 구성" .

스캐닝을 시작하려면 보호 페이지에서 개인 정보 노출 열의 *노출 식별*을 클릭하세요.

"BlueXP classification 사용하여 개인 식별이 가능한 민감한 데이터를 스캔합니다." .

Microsoft Sentinel과 **SIEM** 통합

이제 Microsoft Sentinel을 사용하여 위협 분석 및 감지를 위해 보안 및 이벤트 관리 시스템(SIEM)으로 데이터를 전송할 수 있습니다. 이전에는 SIEM으로 AWS Security Hub 또는 Splunk Cloud를 선택할 수 있었습니다.

"BlueXP ransomware protection 설정 구성에 대해 자세히 알아보세요." .

지금 **30**일 무료 체험하세요

이번 릴리스를 통해 BlueXP ransomware protection 새로 배포한 경우 30일 동안 무료로 체험할 수 있습니다. 이전에는 BlueXP ransomware protection 90일 무료 체험판으로 제공되었습니다. 이미 90일 무료 체험판을 이용 중이라면 해당 혜택은 90일 동안 계속 적용됩니다.

Podman의 파일 수준에서 애플리케이션 작업 부하를 복원합니다.

파일 수준에서 애플리케이션 워크로드를 복원하기 전에 이제 공격으로 인해 영향을 받았을 수 있는 파일 목록을 보고 복원하려는 파일을 식별할 수 있습니다. 이전에는 조직(이전에는 계정)의 BlueXP 커넥터가 Podman을 사용하는 경우 이 기능이 비활성화되었습니다. 이제 Podman에서 사용할 수 있습니다. BlueXP ransomware protection 사용하여 복원할 파일을 선택하거나, 알림으로 영향을 받은 모든 파일을 나열한 CSV 파일을 업로드하거나, 복원할 파일을 수동으로 지정할 수 있습니다.

"랜섬웨어 공격으로부터 복구하는 방법에 대해 자세히 알아보세요" .

2024년 9월 30일

파일 공유 작업 부하의 사용자 정의 그룹화

이번 릴리스에서는 파일 공유를 그룹으로 묶어 데이터 자산을 더 쉽게 보호할 수 있습니다. 이 서비스는 그룹의 모든 볼륨을 동시에 보호할 수 있습니다. 이전에는 각 볼륨을 별도로 보호해야 했습니다.

"랜섬웨어 보호 전략에서 파일 공유 작업 부하를 그룹화하는 방법에 대해 자세히 알아보세요." .

2024년 9월 2일

Digital Advisor 의 보안 위험 평가

BlueXP ransomware protection 이제 NetApp Digital Advisor 에서 클러스터와 관련된 높고 심각한 보안 위험에 대한 정보를 수집합니다. 위험이 발견되면 BlueXP ransomware protection 대시보드의 권장 작업 창에 "클러스터 <이름>에서 알려진 보안 취약점을 수정하세요."라는 권장 사항을 제공합니다. 대시보드의 권장 사항에서 *검토 및 수정*을 클릭하면 Digital Advisor 와 CVE(일반적인 취약성 및 노출) 문서를 검토하여 보안 위험을 해결할 것을 제안합니다. 여러 보안 위험이 있는 경우 Digital Advisor 에서 정보를 검토하세요.

참조하다 "Digital Advisor 문서" .

Google Cloud Platform으로 백업

이 릴리스에서는 백업 대상을 Google Cloud Platform 버킷으로 설정할 수 있습니다. 이전에는 NetApp StorageGRID, Amazon Web Services 및 Microsoft Azure에만 백업 대상을 추가할 수 있었습니다.

"BlueXP ransomware protection 설정 구성에 대해 자세히 알아보세요." .

Google Cloud Platform 지원

이 서비스는 이제 스토리지 보호를 위해 Google Cloud Platform용 Cloud Volumes ONTAP 지원합니다. 이전에는 이 서비스가 온프레미스 NAS와 함께 Amazon Web Services 및 Microsoft Azure용 Cloud Volumes ONTAP 만 지원했습니다.

"BlueXP ransomware protection 및 지원되는 데이터 소스, 백업 대상 및 작업 환경에 대해 알아보세요." .

역할 기반 액세스 제어

이제 역할 기반 액세스 제어(RBAC)를 사용하여 특정 활동에 대한 액세스를 제한할 수 있습니다. BlueXP ransomware protection BlueXP 의 두 가지 역할, 즉 BlueXP 계정 관리자와 비계정 관리자(뷰어)를 사용합니다.

각 역할이 수행할 수 있는 작업에 대한 자세한 내용은 다음을 참조하세요. "역할 기반 액세스 제어 권한" .

2024년 8월 5일

Splunk Cloud를 통한 위협 탐지

위협 분석 및 감지를 위해 보안 및 이벤트 관리 시스템(SIEM)에 자동으로 데이터를 전송할 수 있습니다. 이전 릴리스에서는 SIEM으로 AWS Security Hub만 선택할 수 있었습니다. 이 릴리스에서는 SIEM으로 AWS Security Hub

또는 Splunk Cloud를 선택할 수 있습니다.

"BlueXP ransomware protection 설정 구성에 대해 자세히 알아보세요." .

2024년 7월 1일

BYOL(Bring Your Own License)

이 릴리스에서는 NetApp 영업 담당자로부터 받는 NetApp 라이선스 파일(NLF)인 BYOL 라이선스를 사용할 수 있습니다.

"라이선싱 설정에 대해 자세히 알아보세요" .

파일 수준에서 애플리케이션 작업 부하 복원

파일 수준에서 애플리케이션 워크로드를 복원하기 전에 이제 공격으로 인해 영향을 받았을 수 있는 파일 목록을 보고 복원하려는 파일을 식별할 수 있습니다. BlueXP ransomware protection 사용하여 복원할 파일을 선택하거나, 알림으로 영향을 받은 모든 파일을 나열한 CSV 파일을 업로드하거나, 복원할 파일을 수동으로 지정할 수 있습니다.

이 릴리스에서는 계정의 모든 BlueXP 커넥터가 Podman을 사용하지 않는 경우 단일 파일 복원 기능이 활성화됩니다. 그렇지 않으면 해당 계정에서는 비활성화됩니다.

"랜섬웨어 공격으로부터 복구하는 방법에 대해 자세히 알아보세요" .

영향을 받은 파일 목록 다운로드

파일 수준에서 애플리케이션 워크로드를 복원하기 전에 이제 알림 페이지에 액세스하여 영향을 받은 파일 목록을 CSV 파일로 다운로드한 다음 복구 페이지를 사용하여 CSV 파일을 업로드할 수 있습니다.

"애플리케이션을 복원하기 전에 영향을 받은 파일을 다운로드하는 방법에 대해 자세히 알아보세요." .

보호 계획 삭제

이 릴리스를 통해 랜섬웨어 보호 전략을 삭제할 수 있습니다.

"작업 부하 보호 및 랜섬웨어 보호 전략 관리에 대해 자세히 알아보세요." .

2024년 6월 10일

기본 스토리지의 스냅샷 복사 잠금

이 옵션을 활성화하면 랜섬웨어 공격이 백업 저장소 대상까지 침투하더라도 일정 기간 동안 스냅샷 복사본을 수정하거나 삭제할 수 없도록 기본 저장소에 잠급니다.

"랜섬웨어 보호 전략에서 워크로드 보호 및 백업 잠금 활성화에 대해 자세히 알아보세요." .

Microsoft Azure용 Cloud Volumes ONTAP 지원

이 릴리스에서는 AWS용 Cloud Volumes Cloud Volumes ONTAP 과 온프레미스 ONTAP NAS 외에도 Microsoft Azure용 Cloud Volumes Cloud Volumes ONTAP 시스템으로 지원합니다.

"Azure에서 Cloud Volumes ONTAP 대한 빠른 시작"

"BlueXP ransomware protection 에 대해 알아보세요" .

Microsoft Azure가 백업 대상으로 추가되었습니다**.**

이제 AWS 및 NetApp StorageGRID 와 함께 Microsoft Azure를 백업 대상으로 추가할 수 있습니다.

"보호 설정을 구성하는 방법에 대해 자세히 알아보세요." .

2024년 5월 14일

라이센스 업데이트

90일 무료 체험판에 가입해보세요. 곧 Amazon Web Services Marketplace에서 사용량에 따라 요금을 지불하는 구독을 구매하거나 자체 NetApp 라이선스를 가져올 수 있게 됩니다.

"라이선싱 설정에 대해 자세히 알아보세요" .

CIFS 프로토콜

이 서비스는 이제 NFS와 CIFS 프로토콜을 모두 사용하는 AWS 시스템에서 온프레미스 ONTAP 및 Cloud Volumes ONTAP 지원합니다. 이전 릴리스에서는 NFS 프로토콜만 지원했습니다.

작업량 세부 정보

이번 릴리스에서는 보호 및 기타 페이지에서 워크로드 정보에 대한 자세한 내용을 제공하여 워크로드 보호 평가를 개선했습니다. 작업 부하 세부 정보에서 현재 할당된 정책을 검토하고 구성된 백업 대상을 검토할 수 있습니다.

"보호 페이지에서 작업 세부 정보 보기에 대해 자세히 알아보세요." .

애플리케이션 일관성 및 **VM** 일관성 보호 및 복구

이제 NetApp SnapCenter 소프트웨어를 사용하여 애플리케이션 일관성 보호를 수행하고 SnapCenter Plug-in for VMware vSphere 사용하여 VM 일관성 보호를 수행하여 나중에 복구가 필요할 경우 잠재적인 데이터 손실을 방지하기 위해 조용하고 일관된 상태를 달성할 수 있습니다. 복구가 필요한 경우 애플리케이션이나 VM을 이전에 사용 가능한 상태로 복원할 수 있습니다.

"워크로드 보호에 대해 자세히 알아보세요" .

랜섬웨어 보호 전략

워크로드에 스냅샷이나 백업 정책이 없는 경우 랜섬웨어 보호 전략을 만들 수 있습니다. 여기에는 이 서비스에서 만드는 다음 정책이 포함될 수 있습니다.

- 스냅샷 정책
- 백업 정책
- 탐지 정책

"워크로드 보호에 대해 자세히 알아보세요" .

위협 탐지

이제 타사 보안 및 이벤트 관리(SIEM) 시스템을 사용하여 위협 감지 기능을 사용할 수 있습니다. 대시보드에는 이제 설정 페이지에서 구성할 수 있는 "위협 감지 활성화"에 대한 새로운 권장 사항이 표시됩니다.

"설정 옵션 구성에 대해 자세히 알아보세요" .

거짓 양성 경고 해제

이제 알림 탭에서 거짓 양성 결과를 무시하거나 데이터를 즉시 복구할지 결정할 수 있습니다.

"랜섬웨어 경고에 대응하는 방법에 대해 자세히 알아보세요" .

감지 상태

보호 페이지에 새로운 감지 상태가 나타나 작업 부하에 적용된 랜섬웨어 감지 상태를 보여줍니다.

"작업 부하 보호 및 보호 상태 보기에 대해 자세히 알아보세요." .

CSV 파일 다운로드

보호, 알림 및 복구 페이지에서 CSV 파일*을 다운로드할 수 있습니다.

"대시보드 및 기타 페이지에서 CSV 파일을 다운로드하는 방법에 대해 자세히 알아보세요." .

문서 링크

이제 문서 보기 링크가 UI에 포함되었습니다. 대시보드 세로 *작업*에서 이 문서에 액세스할 수 있습니다.  옵션. 릴리스 노트에서 세부 정보를 보려면 *새로운 기능*을 선택하고, BlueXP ransomware protection 설명서 홈페이지를 보려면 *설명서*를 선택하세요.

BlueXP backup and recovery

이제 BlueXP backup and recovery 서비스를 시스템에서 미리 활성화할 필요가 없습니다. 보다 "전제 조건" . BlueXP ransomware protection 서비스는 설정 옵션을 통해 백업 대상을 구성하는 데 도움이 됩니다. 보다 "설정 구성" .

설정 옵션

이제 BlueXP ransomware protection 설정에서 백업 대상을 설정할 수 있습니다.

"설정 옵션 구성에 대해 자세히 알아보세요" .

2024년 3월 5일

보호 정책 관리

미리 정의된 정책을 사용하는 것 외에도 이제 정책을 만들 수 있습니다. "정책 관리에 대해 자세히 알아보세요" .

보조 저장소(**DataLock**)의 불변성

이제 개체 저장소에서 NetApp DataLock 기술을 사용하여 보조 저장소에서 백업을 변경할 수 없게 만들 수 있습니다. "보호 정책 생성에 대해 자세히 알아보세요" .

NetApp StorageGRID 에 자동 백업

AWS를 사용하는 것 외에도 이제 StorageGRID 백업 대상으로 선택할 수 있습니다. "백업 대상 구성에 대해 자세히 알아보세요" .

잠재적 공격을 조사하기 위한 추가 기능

이제 탐지된 잠재적 공격을 조사하기 위해 더욱 자세한 법의학적 세부 정보를 볼 수 있습니다. "감지된 랜섬웨어 경고에 대응하는 방법에 대해 자세히 알아보세요." .

복구 프로세스

복구 프로세스가 향상되었습니다. 이제 워크로드에 대해 볼륨별로 또는 모든 볼륨을 복구할 수 있습니다. "랜섬웨어 공격으로부터 복구하는 방법에 대해 자세히 알아보세요(사고가 해결된 후)" .

"BlueXP ransomware protection 에 대해 알아보세요" .

2023년 10월 6일

BlueXP ransomware protection 서비스는 데이터를 보호하고, 잠재적인 공격을 탐지하고, 랜섬웨어 공격으로부터 데이터를 복구하는 SaaS 솔루션입니다.

미리보기 버전의 경우, 이 서비스는 BlueXP 조직 전체에서 온프레미스 NAS 스토리지의 Oracle, MySQL, VM 데이터 저장소 및 파일 공유의 애플리케이션 기반 워크로드와 AWS의 Cloud Volumes ONTAP (NFS 프로토콜 사용)을 개별적으로 보호하고 Amazon Web Services 클라우드 스토리지에 데이터를 백업합니다.

BlueXP ransomware protection 서비스는 여러 NetApp 기술을 최대한 활용하여 데이터 보안 관리자나 보안 운영 엔지니어가 다음과 같은 목표를 달성할 수 있도록 지원합니다.

- 모든 작업 부하에 대한 랜섬웨어 보호 기능을 한눈에 확인하세요.
- 랜섬웨어 보호 권장 사항에 대한 통찰력을 얻으세요
- BlueXP ransomware protection 권장 사항을 기반으로 보호 태세를 개선합니다.
- 랜섬웨어 공격으로부터 주요 워크로드와 고위험 데이터를 보호하기 위해 랜섬웨어 보호 정책을 할당하세요.
- 랜섬웨어 공격에 대비하여 워크로드 상태를 모니터링하여 데이터 이상을 발견합니다.
- 랜섬웨어 사고가 업무에 미치는 영향을 신속하게 평가하세요.
- 저장된 데이터에서 재감염이 발생하지 않도록 데이터를 복원하고 랜섬웨어 사고로부터 지능적으로 복구하세요.

"BlueXP ransomware protection 에 대해 알아보세요" .

NetApp Ransomware Resilience 의 알려진 제한 사항

알려진 제한 사항은 이 제품 릴리스에서 지원하지 않거나 올바르게 상호 운용되지 않는 플랫폼, 장치 또는 기능을 나타냅니다. 이러한 제한 사항을 주의 깊게 검토하세요.

준비 훈련 재설정 옵션 문제

랜섬웨어 공격 대비 훈련을 위해 ONTAP 9.11.1 볼륨을 선택하면 랜섬웨어 복원력에서 경고를 보냅니다. "볼륨 복제" 옵션을 사용하여 데이터를 복구하고 드릴을 재설정하면 재설정 작업이 실패합니다.

Amazon FSx for NetApp ONTAP 제한 사항

Amazon FSx for NetApp ONTAP 시스템은 랜섬웨어 복원력에서 지원됩니다. 이 시스템에는 다음과 같은 제한 사항이 적용됩니다.

- Fsx for ONTAP 에서는 백업 정책이 지원되지 않습니다. 이 환경에서는 백업을 위해 Amazon FSx 사용하여 백업 작업을 수행해야 합니다. 랜섬웨어 복원력을 사용하면 이러한 작업 부하를 복원할 수 있습니다.
- 복원 작업은 스냅샷에서만 수행됩니다.

시작하기

NetApp Ransomware Resilience 에 대해 알아보세요

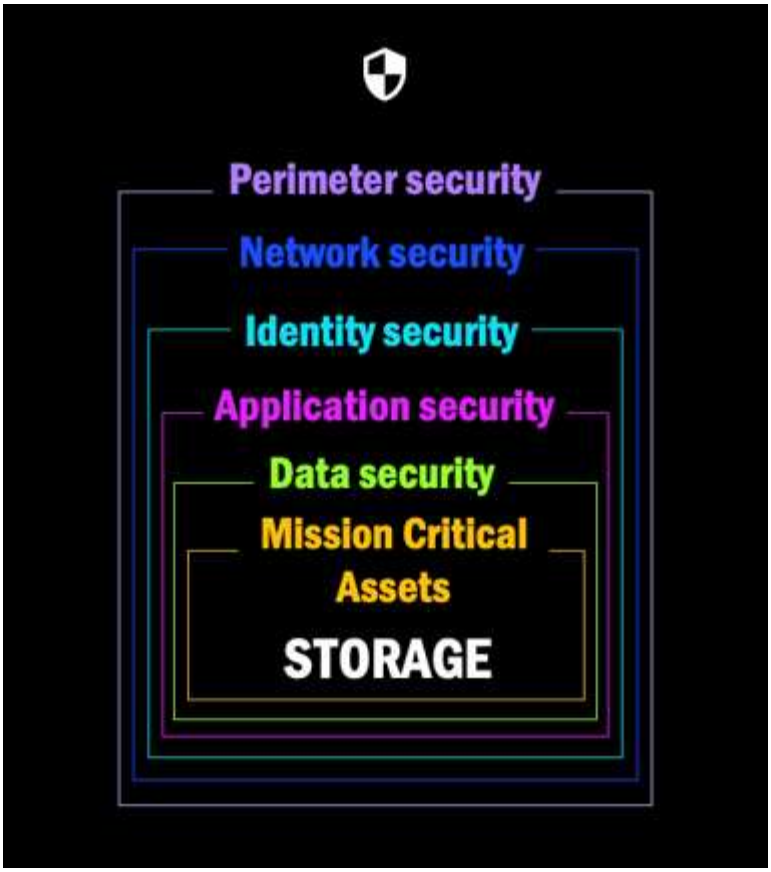
랜섬웨어 공격은 사용자의 데이터에 대한 접근을 차단할 수 있으며, 공격자는 데이터 공개나 암호 해독을 조건으로 몸값을 요구할 수 있습니다. IDC에 따르면, 랜섬웨어 피해자가 여러 차례 랜섬웨어 공격을 경험하는 것은 드문 일이 아닙니다. 이러한 공격으로 인해 귀하의 데이터 접근이 하루에서 몇 주까지 중단될 수 있습니다.

NetApp Ransomware Resilience 랜섬웨어 공격으로부터 데이터를 보호합니다. 랜섬웨어 복원력에서는 온프레미스 NAS 스토리지(NFS 및 CIFS 프로토콜 사용)와 SAN 스토리지(FC, iSCSI 및 NVMe)의 Oracle, MySQL, VM 데이터 저장소 및 파일 공유의 애플리케이션 기반 워크로드에 대한 보호가 제공되며, NetApp Console 에서 Amazon Web Services용 Cloud Volumes ONTAP , Google Cloud용 Cloud Volumes ONTAP , Microsoft Azure용 Cloud Volumes ONTAP 및 Amazon FSx for NetApp ONTAP 도 보호됩니다. Amazon Web Services, Google Cloud, Microsoft Azure 클라우드 스토리지, NetApp StorageGRID 에 데이터를 백업할 수 있습니다.

데이터 계층의 랜섬웨어 복원력

귀사의 보안 태세는 일반적으로 다양한 사이버 위협으로부터 보호하기 위해 여러 계층의 방어 체계를 포함합니다.

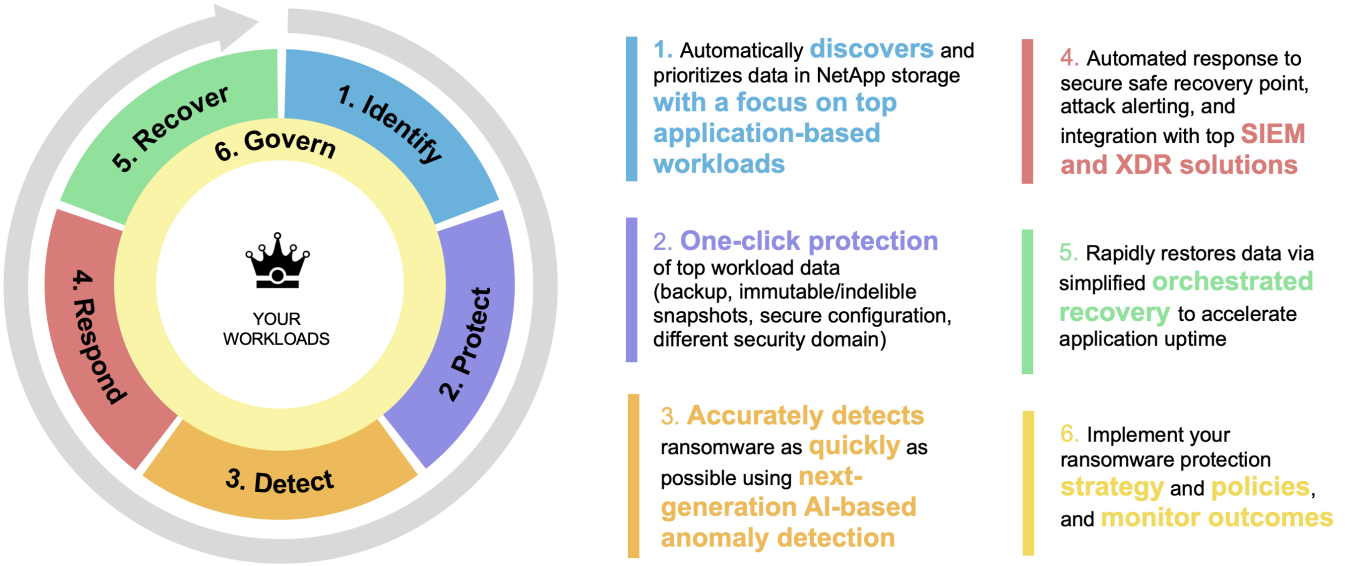
- 가장 바깥쪽 계층: 방화벽, 침입 탐지 시스템, 가상 사설망을 사용하여 네트워크 경계를 보호하는 첫 번째 방어선입니다.
- 네트워크 보안: 이 계층은 네트워크 분할, 트래픽 모니터링, 암호화를 기반으로 구축됩니다.
- **ID** 보안: 인증 방법, 액세스 제어 및 ID 관리를 사용하여 권한이 있는 사용자만 중요한 리소스에 액세스할 수 있도록 보장합니다.
- 애플리케이션 보안: 안전한 코딩 관행, 보안 테스트, 런타임 애플리케이션 자체 보호를 사용하여 소프트웨어 애플리케이션을 보호합니다.
- 데이터 보안: 데이터 보호, 백업, 복구 전략을 통해 데이터를 안전하게 보호합니다. 랜섬웨어 복원력은 이 계층에서 작동합니다.



랜섬웨어 복원력으로 할 수 있는 일

랜섬웨어 복원력은 여러 NetApp 기술을 최대한 활용하여 스토리지 관리자, 데이터 보안 관리자 또는 보안 운영 엔지니어가 다음과 같은 목표를 달성할 수 있도록 지원합니다.

- NetApp Console , 프로젝트 및 콘솔 에이전트 전반의 NetApp 온프레미스 NAS(NFS 또는 CIFS) 및 SAN(FC, iSCSI 및 NVMe) 시스템에서 모든 애플리케이션 기반, 파일 공유 또는 VMware 관리 워크로드를 *식별*합니다. 랜섬웨어 복원력은 데이터 우선순위를 분류하고 랜섬웨어 복원력 개선을 위한 권장 사항을 제공합니다.
- 데이터에 대한 백업, 스냅샷 복사 및 랜섬웨어 보호 전략을 활성화하여 워크로드를 *보호*하세요.
- 랜섬웨어 공격일 수 있는 이상 징후를 *감지*합니다.각주:[공격이 감지되지 않을 수도 있지만, 저희 조사에 따르면 NetApp 기술은 특정 파일 암호화 기반 랜섬웨어 공격에 대해 높은 수준의 감지율을 보였습니다.]
- 실수로 또는 악의적으로 복사본을 삭제할 수 없도록 잠긴 변조 방지 NetApp ONTAP 스냅샷을 자동으로 시작하여 잠재적인 랜섬웨어 공격에 *대응*합니다. 백업 데이터는 변경 불가능하게 유지되며 소스와 대상지에서 랜섬웨어 공격으로부터 종단 간 보호됩니다.
- 여러 NetApp 기술을 조율하여 워크로드 가동 시간을 가속화하는 데 도움이 되는 워크로드를 *복구*하세요. 특정 볼륨만 복구하도록 선택할 수 있습니다. 랜섬웨어 복원력은 최상의 옵션에 대한 권장 사항을 제공합니다.
- 관리: 랜섬웨어 보호 전략을 구현하고 결과를 모니터링합니다.



랜섬웨어 복원력 사용의 이점

랜섬웨어 복원력은 다음과 같은 이점을 제공합니다.

- 워크로드와 기존 스냅샷 및 백업 일정을 검색하고 상대적 중요도를 순위를 매깁니다.
- 랜섬웨어 보호 태세를 평가하고 이해하기 쉬운 대시보드에 표시합니다.
- 발견 및 보호 태세 분석을 기반으로 다음 단계에 대한 권장 사항을 제공합니다.
- 한 번의 클릭으로 AI/ML 기반 데이터 보호 권장 사항을 적용합니다.
- MySQL, Oracle, VMware 데이터 저장소 및 파일 공유와 같은 주요 애플리케이션 기반 워크로드의 데이터를 보호합니다.
- AI 기술을 사용하여 기본 스토리지의 데이터에 대한 랜섬웨어 공격을 실시간으로 감지합니다.
- 감지된 잠재적 공격에 대응하여 스냅샷 복사본을 생성하고 비정상적인 활동에 대한 알림을 시작함으로써 자동화된 작업을 시작합니다.
- RPO 정책을 충족하기 위해 큐레이션된 복구를 적용합니다. 랜섬웨어 복원력은 NetApp Backup and Recovery (이전의 Cloud Backup) 및 SnapCenter 포함한 여러 NetApp 복구 서비스를 사용하여 랜섬웨어 사고로부터 복구를 조율합니다.
- 역할 기반 액세스 제어(RBAC)를 사용하여 기능 및 작업에 대한 액세스를 관리합니다.

비용

NetApp Ransomware Resilience 평가판 사용에 대해 요금을 청구하지 않습니다.

> 2024년 10월 출시부터 Ransomware Resilience의 새로운 배포는 30일 무료 평가판을 제공합니다. 이전에 Ransomware Resilience는 90일 무료 체험판을 제공했습니다. 이미 90일 무료 체험판에 등록한 경우, 해당 체험판은 90일 동안 유효합니다.

백업 및 복구와 랜섬웨어 복원력을 모두 사용하는 경우, 두 제품으로 보호되는 공통 데이터는 랜섬웨어 복원력에 의해서만 청구됩니다.

라이선스 또는 PayGo 구독을 구매한 후, 랜섬웨어 탐지 정책(자율 랜섬웨어 보호)이 활성화된(랜섬웨어 복원력에서

발견 또는 설정) 모든 워크로드와 하나 이상의 스냅샷 또는 백업 정책이 있는 경우, 랜섬웨어 복원력은 해당 워크로드를 "보호됨"으로 분류하고 구매한 용량 또는 PayGo 구독에 차감합니다. 백업이나 스냅샷 정책이 있더라도 탐지 정책 없이 워크로드가 발견되면 "위험"으로 분류되며 구매한 용량에 포함되지 않습니다.

보호된 작업 부하량은 90일 체험 기간이 종료된 후 구매한 용량이나 구독에 차감됩니다. 랜섬웨어 복원력은 효율성 이전에 보호된 작업과 관련된 데이터에 대해 GB 기준으로 요금이 청구됩니다.

라이센스

랜섬웨어 복원력을 사용하면 무료 체험판, 사용량에 따른 요금 지불 구독 또는 자체 라이선스 사용 등 다양한 라이선스 플랜을 사용할 수 있습니다.

랜섬웨어 복원력에는 NetApp ONTAP One 라이선스가 필요합니다.

랜섬웨어 복원력 라이선스에는 추가 NetApp 제품이 포함되지 않습니다. 랜섬웨어 복원력은 라이선스가 없어도 백업 및 복구를 사용할 수 있습니다.

비정상적인 사용자 행동을 감지하기 위해 Ransomware Resilience는 ONTAP 내의 머신 러닝(ML) 모델인 NetApp Autonomous Ransomware Protection을 사용하여 악성 파일 활동을 감지합니다. 이 모델은 랜섬웨어 복원력 라이선스에 포함되어 있습니다.

자세한 내용은 다음을 참조하십시오. "라이센스 설정" .

NetApp Console

랜섬웨어 복원력은 NetApp Console 통해 이용할 수 있습니다.

NetApp Console 엔터프라이즈급 온프레미스 및 클라우드 환경 전반에서 NetApp 스토리지 및 데이터 서비스를 중앙에서 관리할 수 있는 기능을 제공합니다. NetApp 데이터 서비스에 액세스하고 사용하려면 콘솔이 필요합니다. 관리 인터페이스로서, 하나의 인터페이스에서 여러 스토리지 리소스를 관리할 수 있습니다. 콘솔 관리자는 기업 내 모든 시스템의 저장소와 서비스에 대한 액세스를 제어할 수 있습니다.

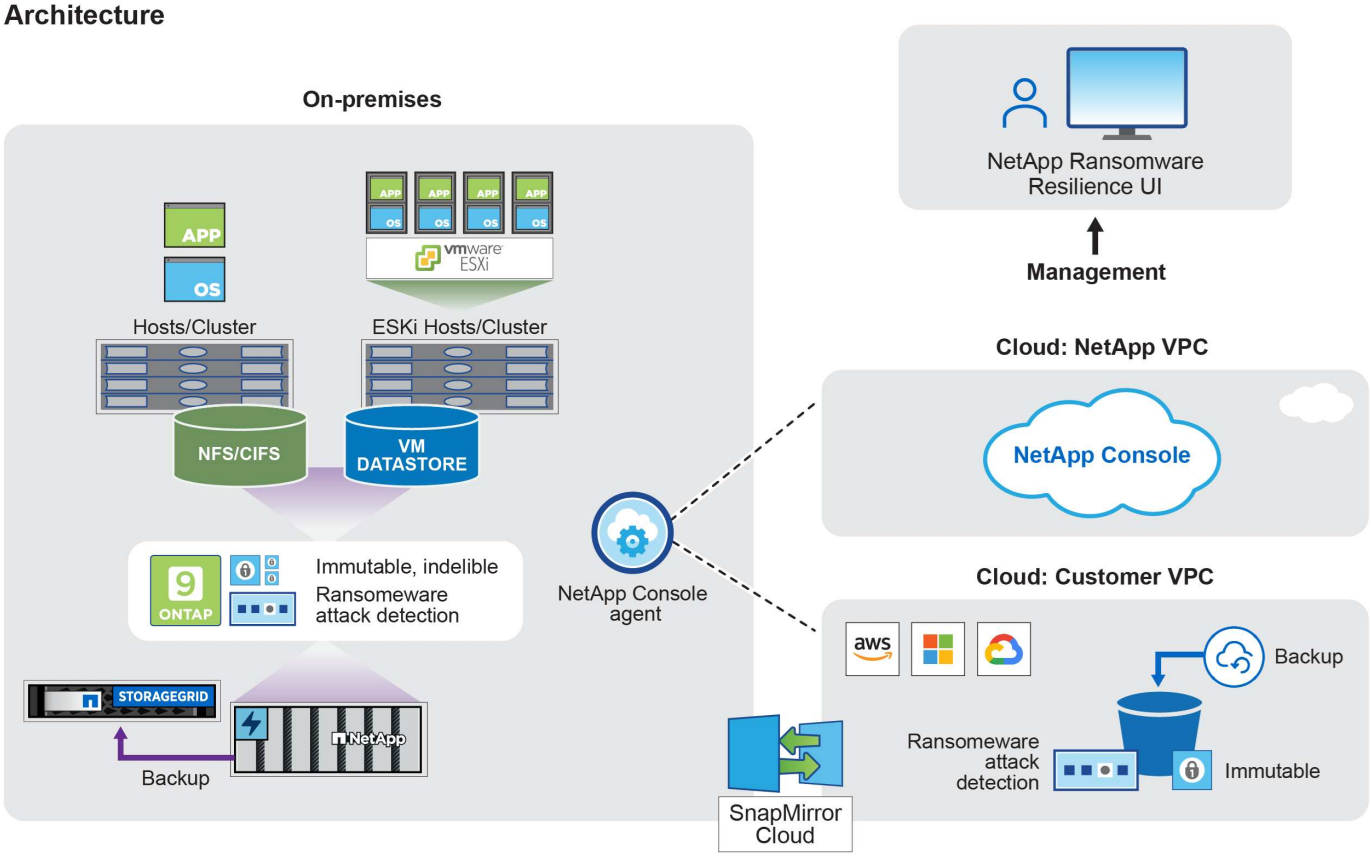
NetApp Console 사용하려면 라이선스나 구독이 필요하지 않으며, 스토리지 시스템이나 NetApp 데이터 서비스에 대한 연결을 보장하기 위해 클라우드에 Console 에이전트를 배포해야 할 때만 요금이 부과됩니다. 그러나 콘솔에서 액세스할 수 있는 일부 NetApp 데이터 서비스는 라이선스 기반이거나 구독 기반입니다.

자세히 알아보세요"NetApp Console" .

랜섬웨어 복원력의 작동 방식

랜섬웨어 복원력은 NetApp Backup and Recovery 사용하여 파일 공유 워크로드에 대한 스냅샷 및 백업 정책을 검색하고 설정하고, SnapCenter 또는 SnapCenter for VMware를 사용하여 애플리케이션 및 VM 워크로드에 대한 스냅샷 및 백업 정책을 검색하고 설정합니다. 또한 Ransomware Resilience는 백업 및 복구와 SnapCenter / SnapCenter for VMware를 사용하여 파일 및 워크로드에 일관된 복구를 수행합니다.

Architecture



특징	설명
식별하다	• 콘솔에 연결된 모든 고객 온프레미스 NAS(NFS 및 CIFS 프로토콜), SAN(FC, iSCSI 및 NVMe) 및 Cloud Volumes ONTAP 데이터를 찾습니다. • ONTAP 및 SnapCenter 서비스 API에서 고객 데이터를 식별하고 이를 워크로드와 연결합니다. 자세히 알아보세요 "ONTAP" 그리고 "SnapCenter 소프트웨어" . • NetApp 스냅샷 복사본과 백업 정책의 각 볼륨의 현재 보호 수준과 온박스 감지 기능을 검색합니다. 랜섬웨어 복원력은 백업 및 복구, ONTAP 서비스, 자율 랜섬웨어 보호(ONTAP 버전에 따라 ARP 또는 ARP/AI), 정책, 백업 정책, 스냅샷 정책과 같은 NetApp 기술을 사용하여 이러한 보호 태세를 워크로드와 연결합니다. 자세히 알아보세요 "자율형 랜섬웨어 보호" , "NetApp Backup and Recovery" , 그리고 "ONTAP 정책" . • 자동으로 검색된 보호 수준을 기반으로 각 워크로드에 비즈니스 우선순위를 할당하고, 비즈니스 우선순위에 따라 워크로드에 대한 보호 정책을 권장합니다. 워크로드 우선순위는 워크로드와 연관된 각 볼륨에 이미 적용된 스냅샷 빈도를 기준으로 합니다.
보호하다	• 식별된 각 워크로드에 정책을 적용하여 워크로드를 적극적으로 모니터링하고 백업 및 복구, SnapCenter, ONTAP API 사용을 조율합니다.

특징	설명
감지하다	• 잠재적으로 비정상적인 암호화 및 활동을 감지하는 통합 머신 러닝(ML) 모델을 통해 잠재적인 공격을 감지합니다. • 기본 스토리지에서 잠재적인 랜섬웨어 공격을 탐지하고 비정상적인 활동에 대응하여 가장 가까운 데이터 복원 지점을 생성하기 위해 추가 자동 스냅샷 복사본을 생성하는 이중 계층 탐지 기능을 제공합니다. 랜섬웨어 복원력은 주요 작업 부하의 성능에 영향을 주지 않고 더욱 정밀하게 잠재적 공격을 식별할 수 있는 기능을 제공합니다. • ONTAP, 자율 랜섬웨어 보호(ONTAP 버전에 따라 ARP 또는 ARP/AI) 및 FPolicy 기술을 사용하여 관련 워크로드에 공격하는 특정 의심 파일을 파악하고 매핑합니다.
대답하다	• 공격에 대한 법의학적 검토를 완료하는 데 도움이 되는 파일 활동, 사용자 활동, 엔트로피와 같은 관련 데이터를 표시합니다. • ONTAP, 자율 랜섬웨어 보호(ONTAP 버전에 따라 ARP 또는 ARP/AI), FPolicy 등의 NetApp 기술과 제품을 사용하여 빠른 스냅샷 복사를 시작합니다.
다시 덮다	• 백업 및 복구, ONTAP, 자율 랜섬웨어 보호(ONTAP 버전에 따라 ARP 또는 ARP/AI), FPolicy 기술과 서비스를 사용하여 최적의 스냅샷 또는 백업을 결정하고 최적의 복구 지점 실제(RPA)를 권장합니다. • 애플리케이션 일관성을 유지하면서 VM, 파일 공유, 블록 스토리지, 데이터베이스 등의 워크로드 복구를 조율합니다.
통치	• 랜섬웨어 보호 전략을 할당합니다. • 결과를 모니터링하는 데 도움이 됩니다.

지원되는 백업 대상, 시스템 및 워크로드 데이터 소스

랜섬웨어 복원력은 다음과 같은 백업 대상, 시스템 및 데이터 소스를 지원합니다.

지원되는 백업 대상

- 아마존 웹 서비스(AWS) S3
- 구글 클라우드 플랫폼
- 마이크로소프트 애저 블롭
- NetApp StorageGRID

지원 시스템

- ONTAP 버전 9.11.1 이상을 사용하는 온프레미스 ONTAP NAS(NFS 및 CIFS 프로토콜 사용)
- ONTAP 버전 9.17.1 이상을 사용하는 온프레미스 ONTAP SAN(FC, iSCSI 및 NVMe 프로토콜 사용)
- AWS용 Cloud Volumes ONTAP 9.11.1 이상(NFS 및 CIFS 프로토콜 사용)
- Google Cloud Platform용 Cloud Volumes ONTAP 9.11.1 이상(NFS 및 CIFS 프로토콜 사용)
- Microsoft Azure용 Cloud Volumes ONTAP 9.12.1 이상(NFS 및 CIFS 프로토콜 사용)

- AWS, Google Cloud Platform 및 Microsoft Azure(FC, iSCSI 및 NVMe 프로토콜 사용)용 Cloud Volumes ONTAP 9.17.1 이상
- ARP(Autonomous Ransomware Protection)를 사용하는 Amazon FSx for NetApp ONTAP(ARP/AI 아님)

  ARP/AI에는 ONTAP 9.16 이상이 필요합니다.

다음은 지원되지 않습니다: FlexGroup 볼륨, 9.11.1보다 이전 버전의 ONTAP , 마운트 지점 볼륨, 마운트 경로 볼륨, 오프라인 볼륨 및 DP(데이터 보호) 볼륨.

지원되는 워크로드 데이터 소스

랜섬웨어 복원력은 기본 데이터 볼륨에서 다음과 같은 애플리케이션 기반 워크로드를 보호합니다.

- NetApp 파일 공유
- 블록 스토리지
- VMware 데이터스토어
- 데이터베이스(MySQL 및 Oracle)
- 곧 더 많은 것이 나올 예정입니다

또한 SnapCenter 또는 SnapCenter for VMware를 사용하는 경우 해당 제품에서 지원하는 모든 워크로드도 랜섬웨어 복원력에 명시되어 있습니다. 랜섬웨어 복원력은 작업 부하에 맞춰 일관된 방식으로 이러한 항목을 보호하고 복구할 수 있습니다.

랜섬웨어 보호에 도움이 될 수 있는 용어

랜섬웨어 보호와 관련된 용어를 이해하는 것이 도움이 될 수 있습니다.

- 보호: 랜섬웨어 복원력의 보호는 보호 정책을 사용하여 정기적으로 스냅샷과 변경 불가능한 백업이 다른 보안 도메인에 발생하도록 보장하는 것을 의미합니다.
- 작업 부하: 랜섬웨어 복원력의 작업 부하에는 MySQL이나 Oracle 데이터베이스, VMware 데이터 저장소 또는 파일 공유가 포함될 수 있습니다.

NetApp Ransomware Resilience 전제 조건

운영 환경, 로그인, 네트워크 액세스 및 웹 브라우저의 준비 상태를 확인하여 NetApp Ransomware Resilience 을 시작하세요.

랜섬웨어 복원력을 사용하려면 다음 전제 조건을 충족해야 합니다.

NetApp Console 에서

- 리소스를 검색하기 위한 조직 관리자 권한이 있는 NetApp Console 사용자 계정입니다.
- 온-프레미스 ONTAP 클러스터나 AWS 또는 Azure의 Cloud Volumes ONTAP 에 연결하는 활성 콘솔 에이전트가 하나 이상 있는 콘솔 조직입니다.
- 콘솔 에이전트에는 다음이 있어야 합니다. `cloudmanager-ransomware-protection` 활성 상태의 컨테이너.

- AWS 또는 Azure의 NetApp 온프레미스 ONTAP 클러스터 또는 Cloud Volumes ONTAP 있는 콘솔 시스템이 하나 이상 있어야 합니다. Ransomware Resilience는 NAS(NFS 및 SMB)와 SAN(iSCSI, FC 및 NVMe) 프로토콜을 모두 지원합니다.
  - 랜섬웨어 복원력은 ONTAP 버전 9.11.1 이상을 사용하는 ONTAP 또는 Cloud Volumes ONTAP 클러스터에서 지원됩니다.

    SAN 워크로드에서 랜섬웨어 복원력을 사용하려면 ONTAP 9.17.1 이상을 실행해야 합니다.

  - AWS 또는 Azure 클라우드의 온프레미스 ONTAP 클러스터나 Cloud Volumes ONTAP 아직 콘솔에 온보딩되지 않은 경우 콘솔 에이전트가 필요합니다.

    참조하다 "콘솔 에이전트를 구성하는 방법을 알아보세요" 그리고 "표준 콘솔 요구 사항" .

    단일 콘솔 조직에 여러 콘솔 에이전트가 있는 경우 Ransomware Resilience는 콘솔 UI에서 현재 선택된 에이전트를 제외한 모든 콘솔 에이전트에서 ONTAP 리소스를 스캔합니다.

ONTAP 9.11.1 이상

- 온프레미스 ONTAP 인스턴스에서 ONTAP One 라이선스가 활성화됩니다.
- Ransomware Resilience에서 사용되는 NetApp Autonomous Ransomware Protection 라이선스는 사용 중인 ONTAP 버전에 따라 온프레미스 ONTAP 인스턴스에서 활성화됩니다. 참조하다 "자율형 랜섬웨어 보호 개요" .

  Ransomware Resilience의 일반 릴리스에는 Preview 릴리스와 달리 NetApp Autonomous Ransomware Protection 기술에 대한 라이선스가 포함되어 있습니다. 참조하다 "자율형 랜섬웨어 보호 개요" 자세한 내용은.

  자세한 라이센스 세부 사항은 다음을 참조하세요."랜섬웨어 복원력에 대해 알아보세요" .

- 보호 구성(자율 랜섬웨어 보호 및 기타 기능 활성화 등)을 적용하려면 랜섬웨어 복원력에 ONTAP 클러스터에 대한 관리자 권한이 필요합니다. ONTAP 클러스터는 ONTAP 클러스터 관리자 사용자 자격 증명을 사용하여만 온보딩되어야 합니다.
- ONTAP 클러스터가 이미 관리자가 아닌 사용자 자격 증명을 사용하여 콘솔에 온보딩된 경우, 이 페이지에 설명된 대로 ONTAP 클러스터에 로그인하여 관리자가 아닌 사용자 권한을 필요한 권한으로 업데이트해야 합니다.

데이터 백업

- 백업 대상과 액세스 권한 집합을 위한 NetApp StorageGRID, AWS S3, Azure Blob 또는 Google Cloud Platform의 계정입니다.

  를 참조하세요 "AWS, Azure 또는 S3 권한 목록" 자세한 내용은.

- 시스템에서 NetApp Backup and Recovery 활성화할 필요가 없습니다.

  랜섬웨어 복원력은 설정 옵션을 통해 백업 대상을 구성하는 데 도움이 됩니다. 보다 "설정 구성" .

의심스러운 사용자 행동

랜섬웨어 복원력이 의심스러운 사용자 동작에 대한 알림을 제공하려면 사용자 활동 에이전트를 구성해야 합니다. 자세한 내용은 다음을 참조하세요. "NetApp Ransomware Resilience 에서 의심스러운 사용자 활동 감지 구성".

ONTAP 시스템에서 관리자가 아닌 사용자 권한 업데이트

특정 시스템에 대한 관리자가 아닌 사용자 권한을 업데이트해야 하는 경우 다음 단계를 완료하세요.

1. 콘솔에 로그인하여 ONTAP 사용자 권한을 업데이트해야 하는 시스템을 찾으세요.
2. 자세한 내용을 보려면 시스템을 선택하세요.
3. 사용자 이름을 표시하려면 *추가 정보 보기*를 선택하세요.
4. 관리자 사용자를 사용하여 ONTAP 클러스터 CLI에 로그인합니다.
5. 해당 사용자의 기존 역할을 표시합니다. 입력하다:

```
security login show -user-or-group-name <username>
```

6. 사용자의 역할을 변경합니다. 입력하다:

```
security login modify -user-or-group-name <username> -application
console|http|ontapi|ssh|telnet -authentication-method password -role
admin
```

7. 랜섬웨어 복원력 UI로 돌아가서 사용하세요.

NetApp Ransomware Resilience 대한 빠른 시작

랜섬웨어 복원력을 설정하고 작업 부하를 보호하는 데 필요한 상위 수준의 단계를 알아보세요.

자세한 내용은 각 단계의 링크를 참조하세요.

1 필수 조건 검토

이러한 작업에는 콘솔 관리자 역할이 필요합니다.

- "콘솔 에이전트를 설치했는지 확인하세요."
- "시스템이 요구 사항을 충족하는지 확인하세요."
- "랜섬웨어 복원력 사용자 역할을 검토하고 랜섬웨어 복원력에 액세스하는 사용자에게 권한을 할당합니다."
- "라이센스 설정"

2 랜섬웨어 복원력 시작하기

이러한 작업에는 랜섬웨어 복원력 관리자 역할이 필요합니다.

- "콘솔에서 워크로드 검색"
- "대시보드에서 워크로드 보호 상태 보기"
- "선택적으로 랜섬웨어 공격 대비 훈련을 실시합니다."

3 랜섬웨어 복원력에서 보호 및 탐지 구성

이러한 작업에는 랜섬웨어 복원력 관리자 역할이 필요합니다. 의심스러운 사용자 동작 활동을 구성하려면 추가적인 랜섬웨어 복원력 사용자 동작 관리자 역할이 필요합니다.

- "작업 부하 보호"
  - 선택적으로,"의심스러운 사용자 활동 감지를 구성하여 보호 강화"
- 선택적으로 백업 대상을 구성합니다.
  - "NetApp StorageGRID, Amazon Web Services, Google Cloud Platform 또는 Microsoft Azure를 백업 대상으로 준비합니다." .
  - "백업 대상 구성"
- "잠재적인 랜섬웨어 공격 감지에 대응"
- "공격으로부터 복구(사고가 무력화된 후)"

4 다음은 무엇인가요?

랜섬웨어 복원력에서 보호 기능을 구성한 후, 다음으로 할 수 있는 일은 다음과 같습니다.

- "데이터 분류를 활성화하여 거버넌스 및 보안 위험을 식별합니다."
- "SIEM에 알림 보내기"
- "경고, 보호, 준비 훈련, 복구 또는 요약 보고서 다운로드"

NetApp Ransomware Resilience 설정

NetApp Ransomware Resilience 쉽게 배포할 수 있습니다. 시작하기 전에 검토하세요"전제 조건" 귀하의 환경이 준비되었는지 확인하세요.

백업 대상을 준비하세요

다음 백업 대상 중 하나를 준비하세요.

- NetApp StorageGRID
- 아마존 웹 서비스
- 구글 클라우드 플랫폼
- 마이크로소프트 애저

백업 대상지 자체에서 옵션을 구성한 후 나중에 Ransomware Resilience에서 백업 대상으로 구성하게 됩니다.

Ransomware Resilience에서 백업 대상을 구성하는 방법에 대한 자세한 내용은 다음을 참조하세요."백업 대상 구성" .

StorageGRID 백업 대상으로 준비

StorageGRID 백업 대상으로 사용하려면 다음을 참조하세요. "StorageGRID 문서" StorageGRID 에 대한 자세한 내용은 다음을 참조하세요.

AWS를 백업 대상으로 준비

- AWS에 계정을 설정합니다.
- 구성 "AWS 권한" AWS에서.

콘솔에서 AWS 스토리지를 관리하는 방법에 대한 자세한 내용은 다음을 참조하세요. "Amazon S3 버킷 관리" .

Azure를 백업 대상으로 준비

- Azure에 계정을 설정합니다.
- 구성 "Azure 권한" Azure에서.

콘솔에서 Azure 저장소를 관리하는 방법에 대한 자세한 내용은 다음을 참조하세요. "Azure 저장소 계정 관리" .

NetApp Console 설정

다음 단계는 콘솔과 랜섬웨어 복원력을 설정하는 것입니다.

검토 "표준 모드에 대한 콘솔 요구 사항" .

콘솔 에이전트 만들기

이 서비스를 체험하거나 사용하려면 NetApp 영업 담당자에게 문의하세요. 그런 다음 콘솔 에이전트를 사용하면 랜섬웨어 복원력에 적합한 기능이 포함됩니다.

Ransomware Resilience를 사용하여 콘솔 에이전트를 생성하려면 콘솔 에이전트를 생성할 권한이 있는 콘솔 조직 관리자에게 문의하고 해당 내용을 설명하는 설명서를 참조하십시오. "콘솔 에이전트를 만드는 방법" .

콘솔 에이전트가 여러 개 있는 경우 랜섬웨어 복원력 검사 데이터는 현재 콘솔에 표시되는 에이전트를 제외한 모든 콘솔 에이전트에서 수집됩니다. 이 서비스는 이 조직과 관련된 모든 프로젝트와 모든 콘솔 에이전트를 검색합니다.

NetApp Ransomware Resilience 에 액세스하세요

NetApp Console 통해 NetApp Ransomware Resilience 에 로그인합니다.

콘솔에 로그인하려면 NetApp 지원 사이트 자격 증명을 사용하거나 이메일과 비밀번호를 사용하여 NetApp 클라우드 로그인에 가입할 수 있습니다. "로그인에 대해 자세히 알아보세요" .

필수 콘솔 역할 이 작업을 수행하려면 조직 관리자, 폴더 또는 프로젝트 관리자, 랜섬웨어 복원력 관리자 또는 랜섬웨어 복원력 뷰어 역할이 필요합니다. "NetApp Console 의 랜섬웨어 복원력 역할에 대해 알아보세요" .

단계

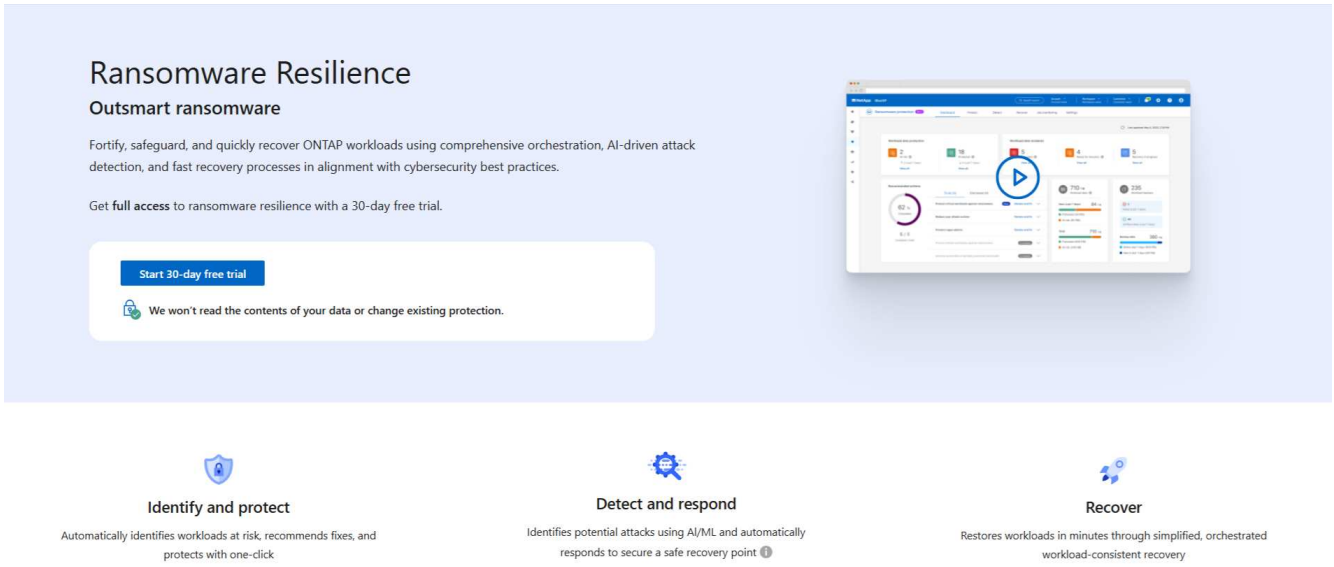
1. 웹 브라우저를 열고 이동하세요"콘솔" .

   콘솔 로그인 페이지가 나타납니다.

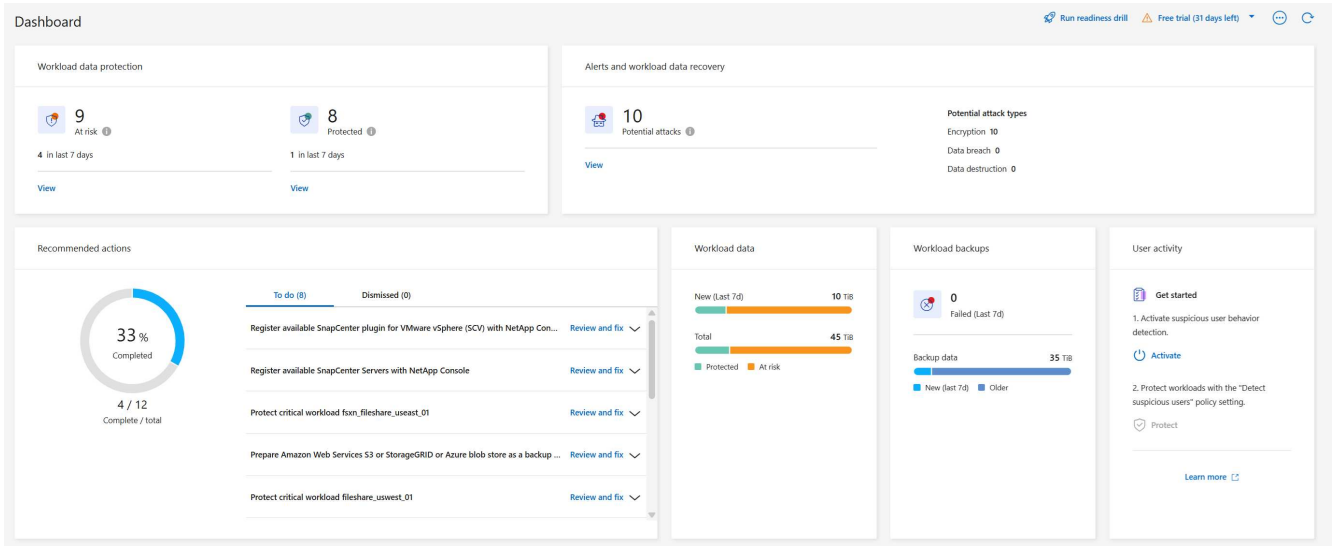
2. 콘솔에 로그인합니다.
3. 콘솔 왼쪽 탐색에서 보호 > *랜섬웨어 복원력*을 선택합니다.

   이 서비스에 처음 로그인하는 경우 랜딩 페이지가 나타납니다.

   콘솔 에이전트가 없거나 이 서비스에 적합한 에이전트가 아닌 경우, 콘솔 에이전트를 배포해야 합니다. "콘솔 에이전트를 설정하는 방법을 알아보세요" .



그렇지 않으면 랜섬웨어 복원력 대시보드가 나타납니다.



4. 아직 선택하지 않았다면 워크로드 검색 옵션을 선택하세요.

"워크로드 검색" .

NetApp Ransomware Resilience 에 대한 라이선싱 설정

NetApp Ransomware Resilience 사용하면 다양한 라이선스 플랜을 사용할 수 있습니다.

이 작업을 수행하려면 조직 관리자, 폴더 또는 프로젝트 관리자 역할이 필요합니다. "콘솔 액세스 역할에 대해 알아보세요" .

라이선스 유형 랜섬웨어 복원력은 다음 라이선스 유형으로 제공됩니다.

- 30일 무료 체험
- Amazon Web Services(AWS) Marketplace, Google Cloud Marketplace 또는 Azure Marketplace에서 PAYGO(Pay-as-you-go) 구독을 구매하세요.
- BYOL(Bring Your Own License): NetApp 영업 담당자로부터 받는 NetApp 라이선스 파일(NLF)입니다. 콘솔에서 라이선스 일련 번호를 사용하여 BYOL을 활성화할 수 있습니다.

BYOL을 설정하거나 PAYGO 구독을 구매한 후 콘솔의 Licenses and subscriptions 섹션에서 라이선스를 확인할 수 있습니다.

무료 평가판이 종료되거나 라이선스 또는 구독이 만료된 후에도 다음을 수행할 수 있습니다.

- 워크로드 및 워크로드 상태 보기
- 정책 등의 리소스 삭제
- 평가 기간 동안 또는 라이선스에 따라 생성된 모든 예약된 작업을 실행합니다.

기타 라이센스

랜섬웨어 복원력 라이선스에는 추가 NetApp 제품이 포함되지 않습니다. 하지만 Ransomware Resilience는 NetApp Backup and Recovery 와 통합될 수 있습니다.

백업 및 복구와 랜섬웨어 복원력을 모두 사용하는 경우, 두 제품으로 보호되는 공통 데이터는 랜섬웨어 복원력으로만 청구됩니다.

30일 무료 체험판으로 랜섬웨어 복원력을 시험해보세요

30일 무료 체험판을 통해 Ransomware Resilience를 사용해 보세요. 무료 평가판을 시작하려면 콘솔 조직 관리자여야 합니다.

체험 기간 동안에는 저장 용량 제한이 적용되지 않습니다.

언제든지 라이선스를 구매하거나 구독할 수 있으며, 30일 평가판이 종료될 때까지 요금이 청구되지 않습니다. 30일 체험 기간이 끝난 후 계속 사용하려면 BYOL 라이선스나 PAYGO 구독을 구매해야 합니다.

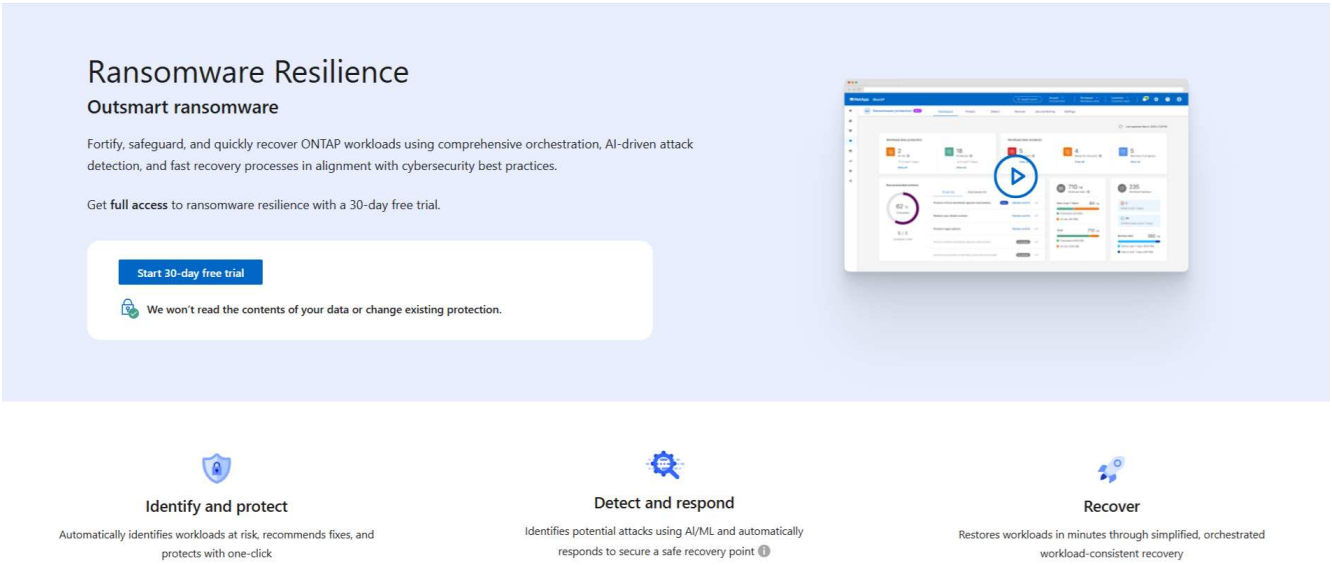
체험판 기간 동안에는 모든 기능을 사용할 수 있습니다.

단계

1. 접속하세요 "콘솔" .

2. 콘솔에 로그인합니다.
3. NetApp Console 에서 보호 > *랜섬웨어 복원력*을 선택합니다.

   이 서비스에 처음 로그인하는 경우 랜딩 페이지가 나타납니다.



4. 다른 서비스에 대한 콘솔 에이전트를 아직 추가하지 않은 경우"하나 추가하다" .
5. 랜섬웨어 복원력 랜딩 페이지에서 *워크로드 검색으로 시작*을 선택하여 워크로드를 검색합니다.

   이 옵션은 콘솔 에이전트를 성공적으로 설치한 경우에만 사용할 수 있습니다.

6. 무료 체험판 정보를 검토하려면 오른쪽 상단의 드롭다운 옵션을 선택하세요.

체험 종료 후 구독 또는 라이선스 구매

무료 체험 기간이 종료된 후에는 마켓플레이스 중 하나를 통해 구독하거나 NetApp 에서 라이선스를 구매할 수 있습니다.

이미 PAYGO 구독을 신청한 경우, 무료 체험 기간이 종료되면 라이센스가 자동으로 구독으로 전환됩니다.

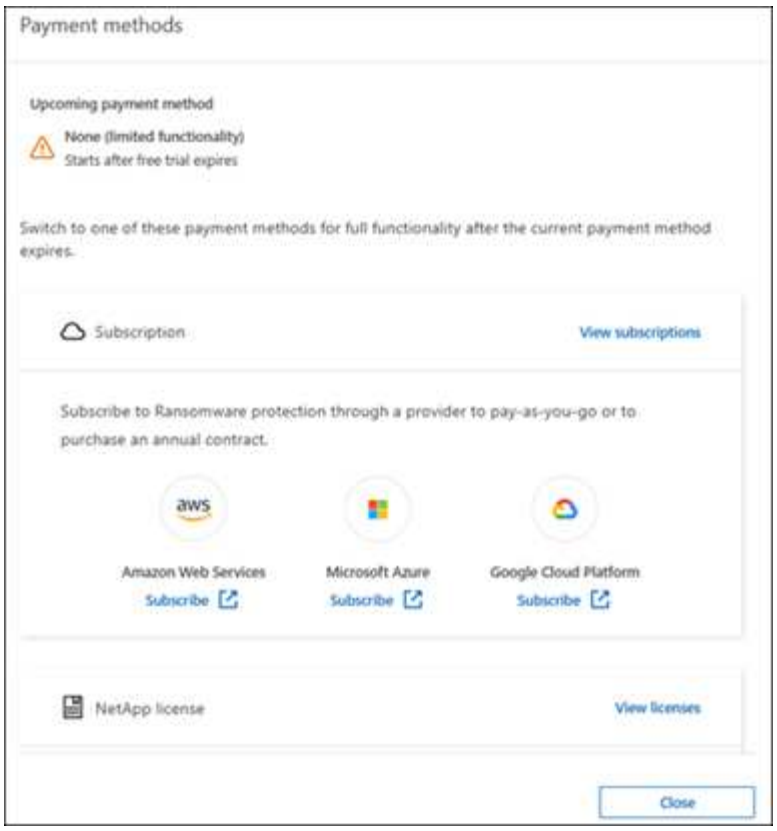
AWS Marketplace를 통해 구독하세요 Microsoft Azure Marketplace를 통해 구독하세요 Google Cloud Platform Marketplace를 통해 구독하세요 BYOL(Bring Your Own License)

AWS Marketplace를 통해 구독하세요

이 절차에서는 AWS Marketplace에서 직접 구독하는 방법에 대한 개요를 제공합니다.

단계

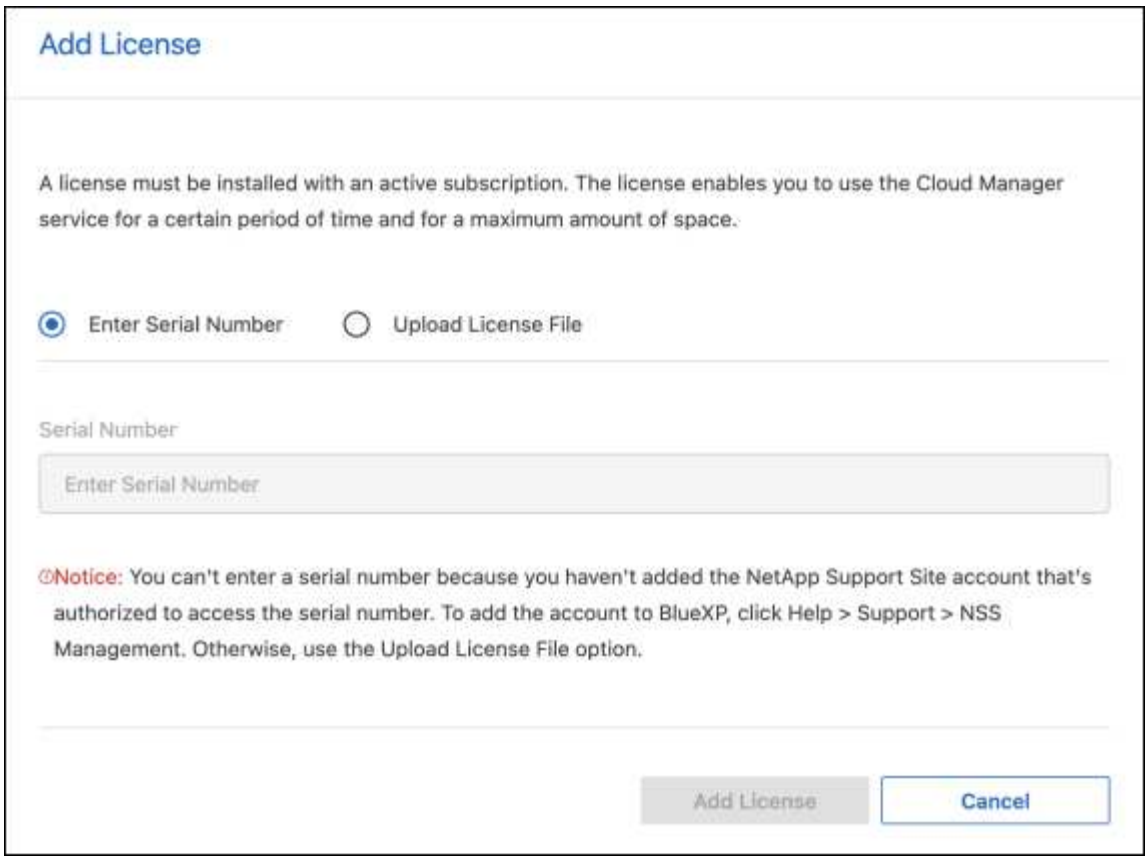
1. 랜섬웨어 복원력에서 다음 중 하나를 수행하세요.
   - 무료 체험 기간이 만료된다는 메시지가 표시되면 *결제 방법 보기*를 선택하세요.
   - 체험판을 시작하지 않은 경우 오른쪽 상단의 무료 체험판 알림을 선택한 다음 *결제 방법 보기*를 선택하세요.



2. 결제 방법 페이지에서 *Amazon Web Services*에 대한 *구독*을 선택합니다.
3. AWS Marketplace에서 *구매 옵션 보기*를 선택합니다.
4. AWS Marketplace를 사용하여 * NetApp Intelligent Services* 및 *Ransomware Resilience*를 구독하세요.
5. 랜섬웨어 복원력 페이지로 돌아오면 구독이 완료되었다는 메시지가 표시됩니다.

> Ransomware Resilience 일련 번호가 포함된 이메일이 전송되며, Ransomware Resilience가 AWS Marketplace에 구독되어 있음을 나타냅니다.

6. 랜섬웨어 복구 지불 방법 페이지로 돌아가세요.
7. *라이선스 추가*를 선택하여 콘솔에 라이센스를 추가합니다.



8. 라이선스 추가 페이지에서 *일련 번호 입력*을 선택하고, 귀하에게 전송된 이메일에 포함된 일련 번호를 입력한 다음, *라이선스 추가*를 선택합니다.
9. 라이선스 세부 정보를 보려면 콘솔 왼쪽 탐색에서 관리 > * Licenses and subscriptions*을 선택하세요.
   - 구독 정보를 보려면 *구독*을 선택하세요.
   - BYOL 라이선스를 보려면 *데이터 서비스 라이선스*를 선택하세요.
10. 랜섬웨어 회복력으로 돌아가기. 콘솔 왼쪽 탐색에서 보호 > *랜섬웨어 복원력*을 선택합니다.

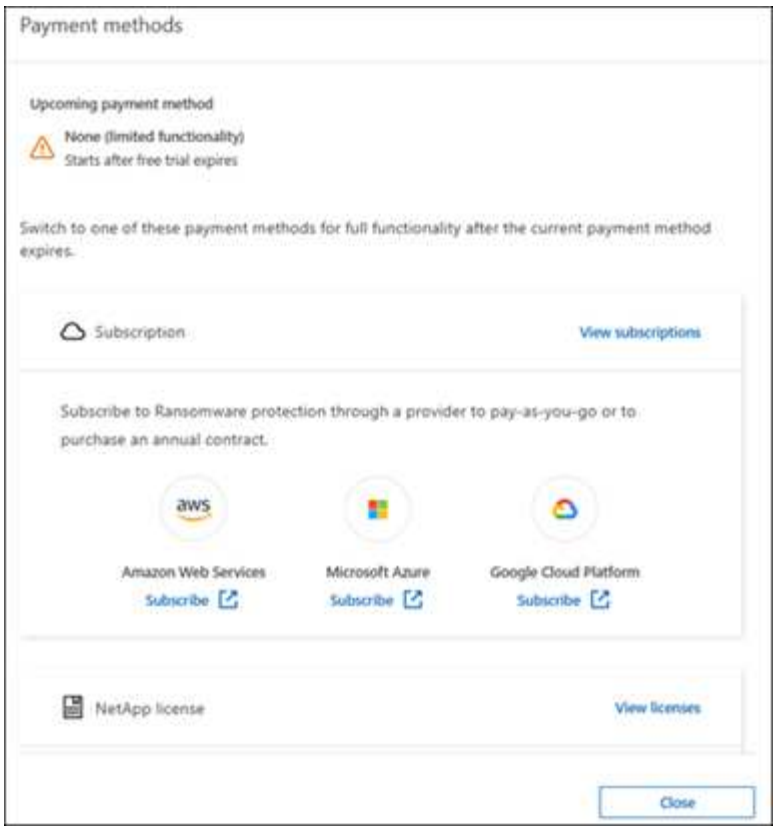
    라이센스가 추가되었음을 확인하는 메시지가 나타납니다.

Microsoft Azure Marketplace를 통해 구독하세요

이 절차에서는 Azure Marketplace에서 직접 구독하는 방법에 대한 간략한 개요를 제공합니다.

단계

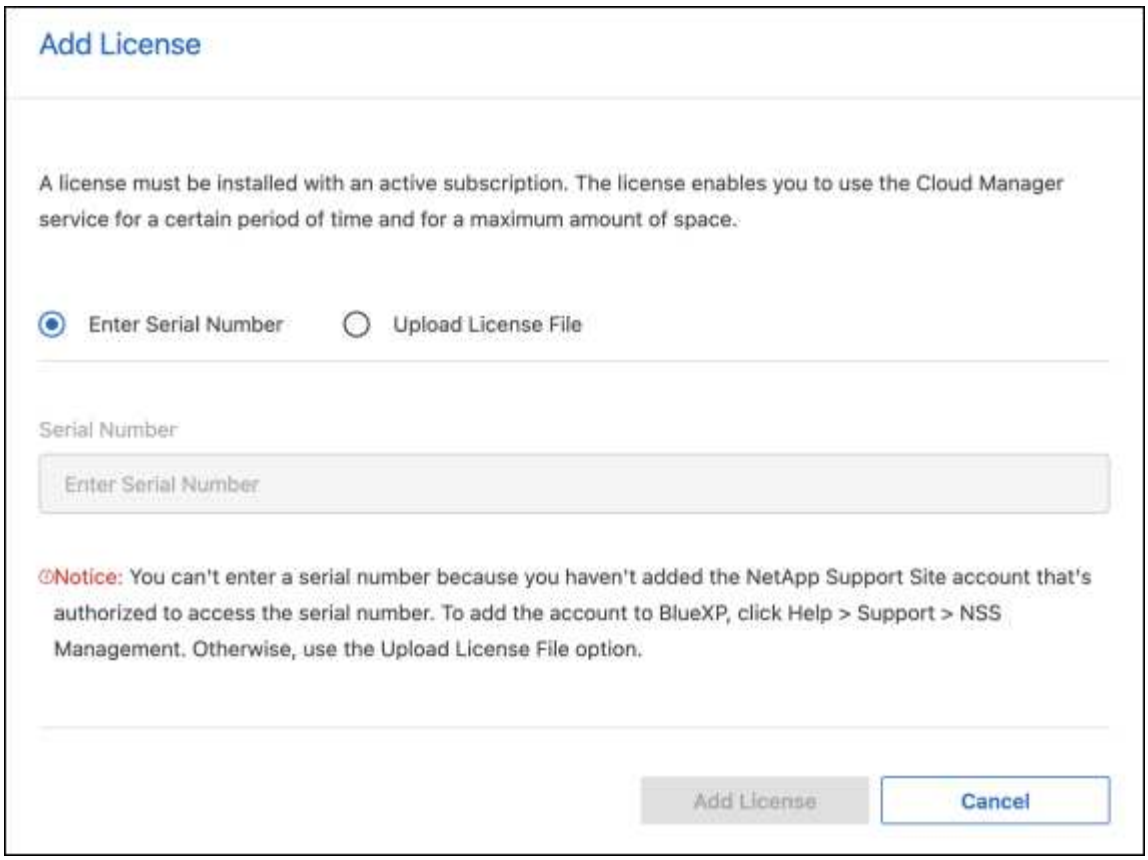
1. 랜섬웨어 복원력에서 다음 중 하나를 수행하세요.
   - 무료 체험 기간이 만료된다는 메시지가 표시되면 *결제 방법 보기*를 선택하세요.
   - 체험판을 시작하지 않은 경우 오른쪽 상단의 무료 체험판 알림을 선택한 다음 *결제 방법 보기*를 선택하세요.



2. 결제 방법 페이지에서 *Microsoft Azure Marketplace*에 대한 *구독*을 선택합니다.
3. Azure Marketplace에서 *구매 옵션 보기*를 선택합니다.
4. Azure Marketplace를 사용하여 * NetApp Intelligent Services* 및 *Ransomware Resilience*를 구독하세요.
5. 랜섬웨어 복원력 페이지로 돌아오면 구독이 완료되었다는 메시지가 표시됩니다.

> Ransomware Resilience 일련 번호가 포함된 이메일이 전송되며, Ransomware Resilience가 Azure Marketplace에 구독되어 있음을 나타냅니다.

6. 랜섬웨어 복구 지불 방법 페이지로 돌아가세요.
7. 라이선스를 추가하려면 *라이선스 추가*를 선택하세요.



8. 라이선스 추가 페이지에서 *일련 번호 입력*을 선택한 다음, 이메일로 전송된 일련 번호를 입력하세요. *라이선스 추가*를 선택하세요.
9. Licenses and subscriptions 에서 라이선스 세부 정보를 보려면 콘솔 왼쪽 탐색에서 거버넌스 > * Licenses and subscriptions*을 선택하세요.
   - 구독 정보를 보려면 *구독*을 선택하세요.
   - BYOL 라이선스를 보려면 *데이터 서비스 라이선스*를 선택하세요.
10. 랜섬웨어 회복력으로 돌아가기. 콘솔 왼쪽 탐색에서 보호 > *랜섬웨어 복원력*을 선택합니다.

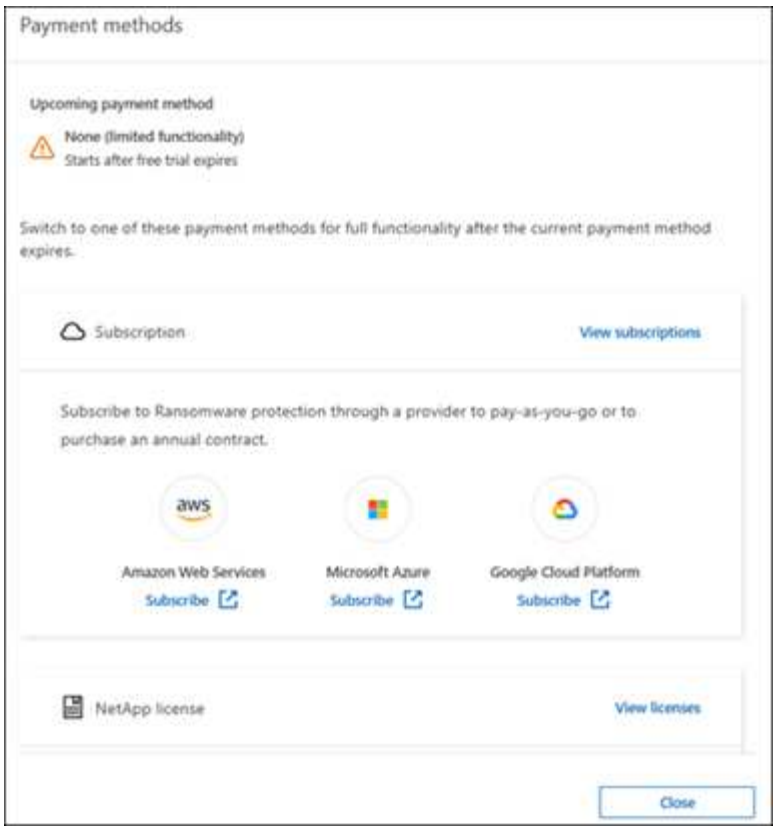
    라이센스가 추가되었다는 메시지가 나타납니다.

Google Cloud Platform Marketplace를 통해 구독하세요

이 절차에서는 Google Cloud Platform Marketplace에서 직접 구독하는 방법에 대한 개요를 제공합니다.

단계

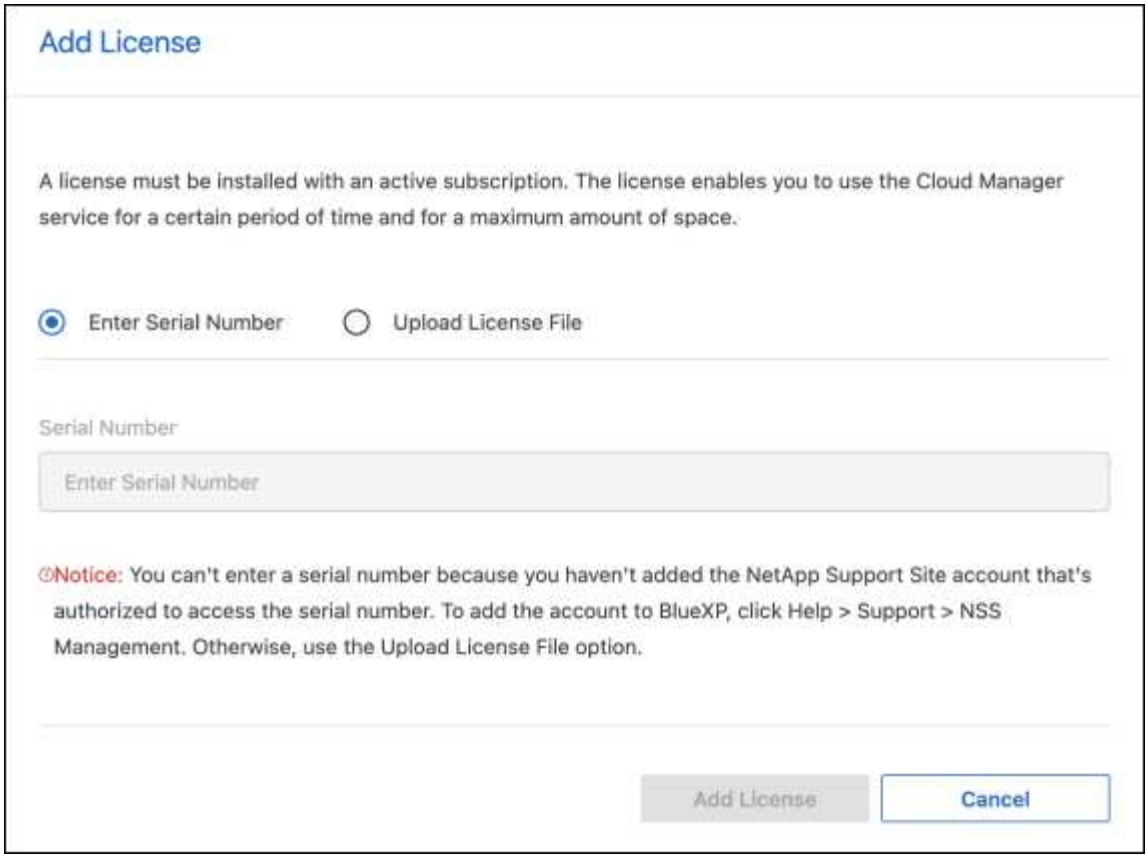
1. 랜섬웨어 복원력에서 다음 중 하나를 수행하세요.
   - 무료 체험 기간이 만료된다는 메시지가 표시되면 *결제 방법 보기*를 선택하세요.
   - 체험판을 시작하지 않은 경우 오른쪽 상단의 무료 체험판 알림을 선택한 다음 *결제 방법 보기*를 선택하세요.



2. 결제 방법 페이지에서 Google Cloud Platform Marketplace*에 대한 *구독*을 선택합니다.
3. Google Cloud Platform Marketplace에서 *구독*을 선택합니다.
4. Google Cloud Platform Marketplace를 사용하여 * NetApp Intelligent Services* 및 *Ransomware Resilience*를 구독하세요.
5. 랜섬웨어 복원력 페이지로 돌아오면 구독이 완료되었다는 메시지가 표시됩니다.

Ransomware Resilience 일련 번호가 포함된 이메일이 전송되며 Ransomware Resilience가 Google Cloud Platform Marketplace에 구독되어 있음을 나타냅니다.

6. 랜섬웨어 복구 지불 방법 페이지로 돌아가세요.
7. 콘솔에 라이선스를 추가하려면 *라이선스 추가*를 선택하세요.



8. 라이선스 추가 페이지에서 *일련 번호 입력*을 선택하세요. 귀하에게 전송된 이메일의 일련번호를 입력하세요. *라이선스 추가*를 선택하세요.
9. 라이선스 세부 정보를 보려면 콘솔 왼쪽 탐색에서 거버넌스 > * Licenses and subscriptions*을 선택하세요.
   - 구독 정보를 보려면 *구독*을 선택하세요.
   - BYOL 라이선스를 보려면 *데이터 서비스 라이선스*를 선택하세요.
10. 랜섬웨어 회복력으로 돌아가기. 콘솔 왼쪽 탐색에서 보호 > *랜섬웨어 복원력*을 선택합니다.

    라이센스가 추가되었다는 메시지가 나타납니다.

BYOL(Bring Your Own License)

자체 라이선스(BYOL)를 사용하려면 라이선스를 구매하고 NetApp 라이선스 파일(NLF)을 받은 다음 콘솔에 라이선스를 추가해야 합니다.

콘솔에 라이센스 파일을 추가합니다

NetApp 영업 담당자로부터 랜섬웨어 복원력 라이선스를 구매한 후 랜섬웨어 복원력 일련 번호와 NetApp 지원 사이트(NSS) 계정 정보를 입력하여 라이선스를 활성화합니다.

시작하기 전에

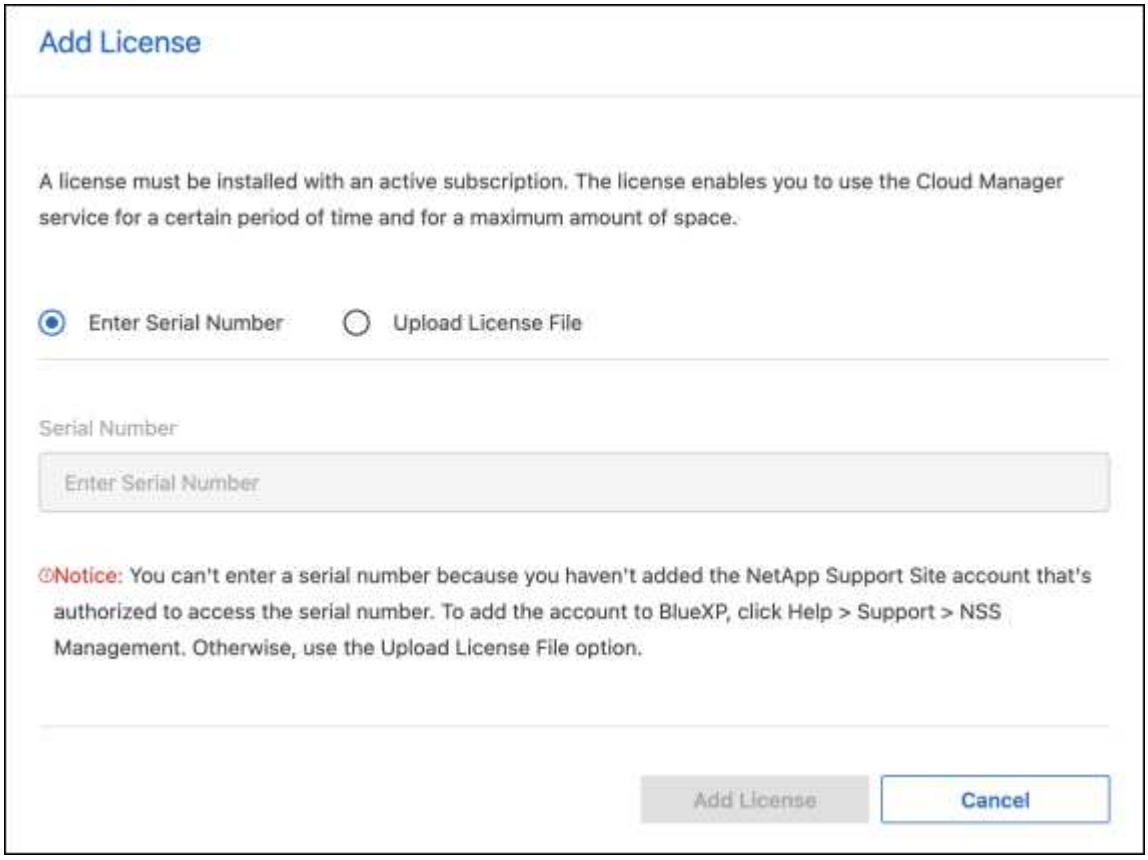
랜섬웨어 복원력 일련번호가 필요합니다. 판매 주문서에서 이 번호를 찾거나, 계정 팀에 문의하여 정보를 얻으세요.

단계

1. 라이센스를 취득한 후 Ransomware Resilience로 돌아가세요. 오른쪽 상단의 결제 방법 보기 옵션을 선택하세요.

또는 무료 평가판이 만료된다는 메시지가 표시되면 *구독 또는 라이선스 구매*를 선택하세요.

2. *라이선스 추가*를 선택하여 콘솔 라이선스 및 구독 페이지로 이동합니다.
3. 데이터 서비스 라이선스 탭에서 *라이선스 추가*를 선택합니다.



4. 라이선스 추가 페이지에서 일련 번호와 NetApp 지원 사이트 계정 정보를 입력합니다.
   - 콘솔 라이선스 일련 번호가 있고 NSS 계정을 알고 있는 경우 일련 번호 입력 옵션을 선택하고 해당 정보를 입력하세요.

     드롭다운 목록에서 NetApp 지원 사이트 계정을 사용할 수 없는 경우 "콘솔에 NSS 계정 추가" .
   - zvondolr 라이선스 파일(어두운 곳에 설치할 때 필요)이 있는 경우 라이선스 파일 업로드 옵션을 선택하고 화면의 지시에 따라 파일을 첨부하세요.
5. *라이선스 추가*를 선택하세요.

결과

Licenses and subscriptions 페이지에는 Ransomware Resilience에 라이선스가 있는 것으로 표시됩니다.

콘솔 라이선스가 만료되면 업데이트하세요.

라이선스 기간이 만료일에 가까워지거나 라이선스 용량이 한도에 도달하면 랜섬웨어 복원력 UI에서 알림을 받게 됩니다. 스캔한 데이터에 액세스하는 데 방해가 되지 않도록 랜섬웨어 복원력 라이선스가 만료되기 전에 업데이트할 수 있습니다.

이 메시지는 Licenses and subscriptions 에도 나타납니다. "알림 설정" .

단계

1. 라이선스 업데이트를 요청하려면 지원팀에 이메일을 보내세요.

   라이선스 비용을 지불하고 NetApp 지원 사이트에 라이선스를 등록하면 콘솔에서 자동으로 라이선스가 업데이트됩니다. 5~10분 안에 데이터 서비스 라이선스 페이지에 변경 사항이 반영됩니다.

2. 콘솔에서 라이선스를 자동으로 업데이트할 수 없는 경우 라이선스 파일을 수동으로 업로드해야 합니다.

   a. NetApp 지원 사이트에서 라이선스 파일을 얻을 수 있습니다.

   b. 콘솔에서 관리 > **Licenses and subscriptions**을 선택합니다.

   c. 데이터 서비스 라이선스 탭을 선택하고, 업데이트하려는 일련 번호에 대한 작업**...** 아이콘을 선택한 다음 *라이선스 업데이트*를 선택합니다.

PAYGO 구독 종료

PAYGO 구독을 종료하고 싶으면 언제든지 그렇게 할 수 있습니다.

단계

1. 랜섬웨어 복원력에서 오른쪽 상단에서 라이선스 옵션을 선택하세요.
2. *결제 방법 보기*를 선택하세요.
3. 드롭다운 세부정보에서 현재 결제 방법 만료 후 사용 상자의 선택을 취소하세요.
4. *저장*을 선택하세요.

NetApp Ransomware Resilience 에서 워크로드를 발견하세요

NetApp Ransomware Resilience 사용하려면 먼저 데이터를 검색해야 합니다. 발견 과정에서 Ransomware Resilience는 조직 내 모든 콘솔 에이전트와 프로젝트에 있는 시스템의 모든 볼륨과 파일을 분석합니다.

필수 콘솔 역할 이 작업을 수행하려면 조직 관리자, 폴더 또는 프로젝트 관리자, 랜섬웨어 복원력 관리자 역할이 필요합니다. "NetApp Console 의 랜섬웨어 복원력 역할에 대해 알아보세요" .

랜섬웨어 복원력은 무엇을 발견하나요**?** 랜섬웨어 복원력은 MySQL 애플리케이션, Oracle 애플리케이션, VMware 데이터 저장소, 파일 공유 및 블록 스토리지를 평가합니다.

랜섬웨어 복원력은 FlexGroup 사용하는 볼륨의 워크로드를 검색하지 않습니다.

랜섬웨어 복원력은 대시보드에서 지원되는 시스템 구성과 지원되지 않는 시스템 구성을 모두 검색하여 표시합니다.

랜섬웨어 복원력은 현재 백업 보호, 스냅샷 사본 및 NetApp Autonomous Ransomware Protection 옵션을 확인합니다. 그런 다음 랜섬웨어 보호를 개선하는 방법을 추천합니다.

작업 부하를 어떻게 발견할 수 있나요**?** 다음을 수행할 수 있습니다.

- 각 콘솔 에이전트 내에서 워크로드를 검색할 시스템을 선택합니다. 환경 내 특정 작업 부하만 보호하고 다른 작업 부하에는 영향을 미치지 않으려는 경우 이 기능이 유용할 수 있습니다.
- 이전에 선택한 시스템에 대해 새로 생성된 워크로드를 검색합니다.

- 새로운 시스템을 발견하세요.

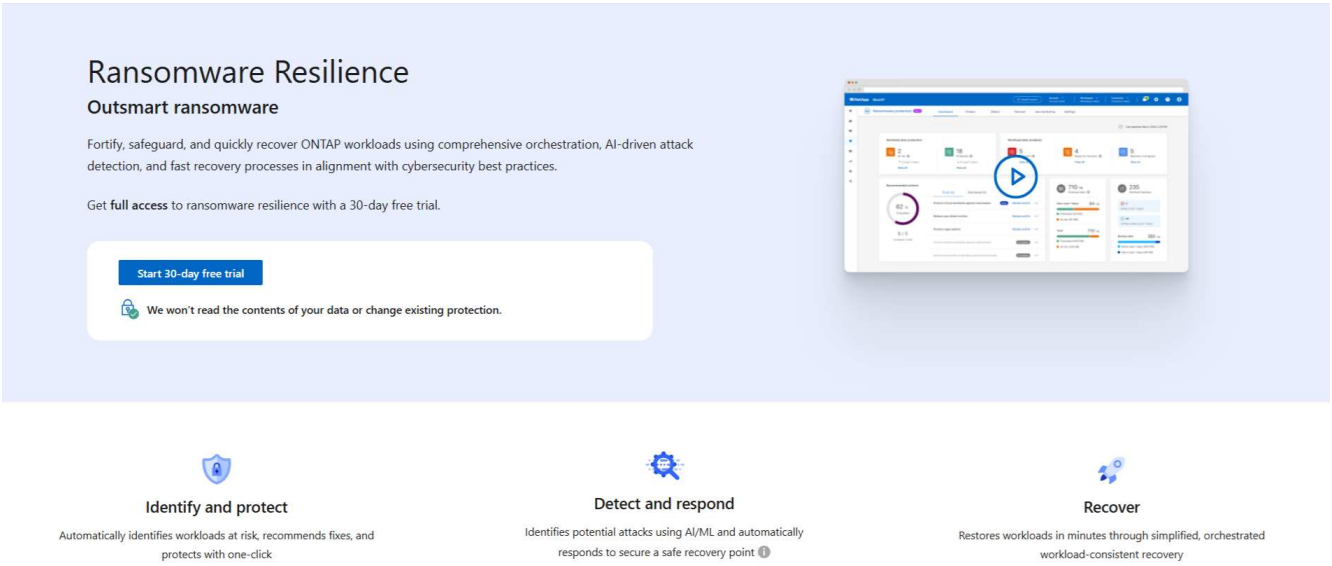
검색하고 보호할 작업 부하 선택

각 콘솔 에이전트 내에서 워크로드를 검색할 시스템을 선택합니다.

단계

1. NetApp Console 에서 보호 > *랜섬웨어 보호*를 선택합니다.

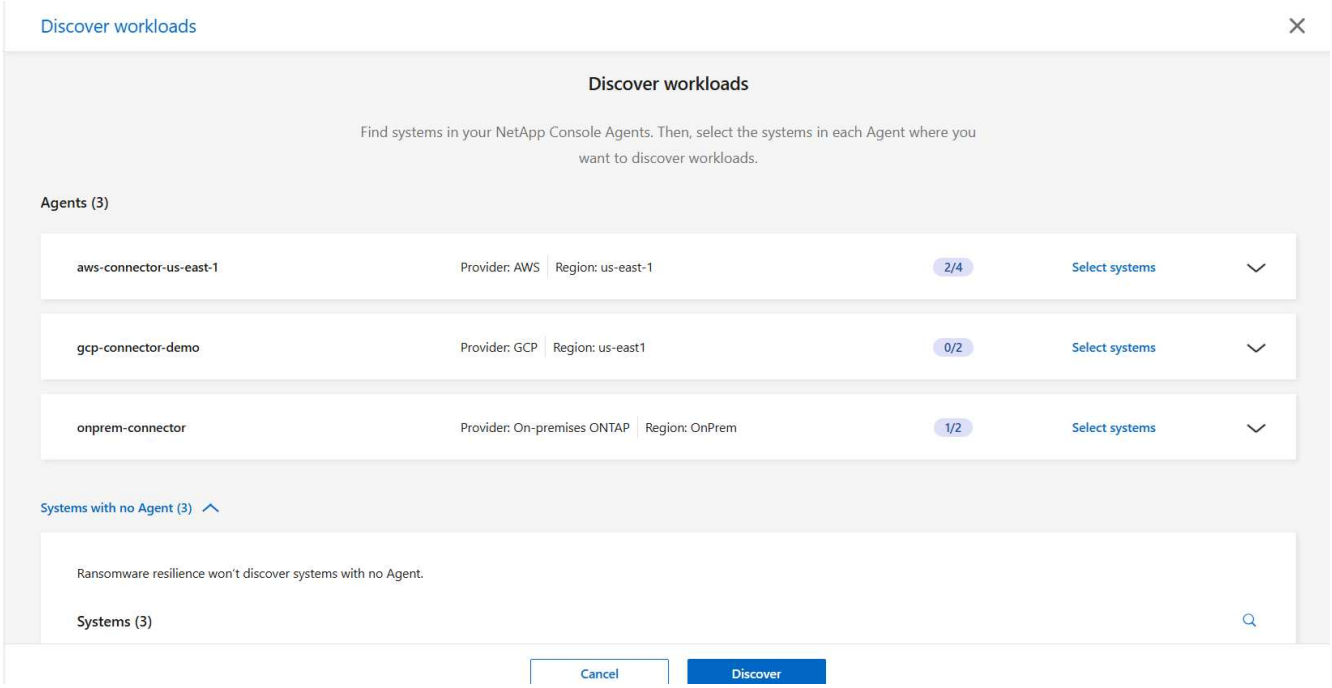
   처음으로 로그인하는 경우 랜딩 페이지가 나타납니다.



   무료 평가판을 시작한 경우 **30**일 무료 평가판 시작 버튼 레이블이 *워크로드 검색으로 시작*으로 변경됩니다.

2. 첫 번째 랜딩 페이지에서 *워크로드 검색으로 시작*을 선택합니다.

   랜섬웨어 복원력은 지원되는 시스템과 지원되지 않는 시스템을 모두 찾아냅니다. 이 과정은 몇 분 정도 걸릴 수 있습니다.

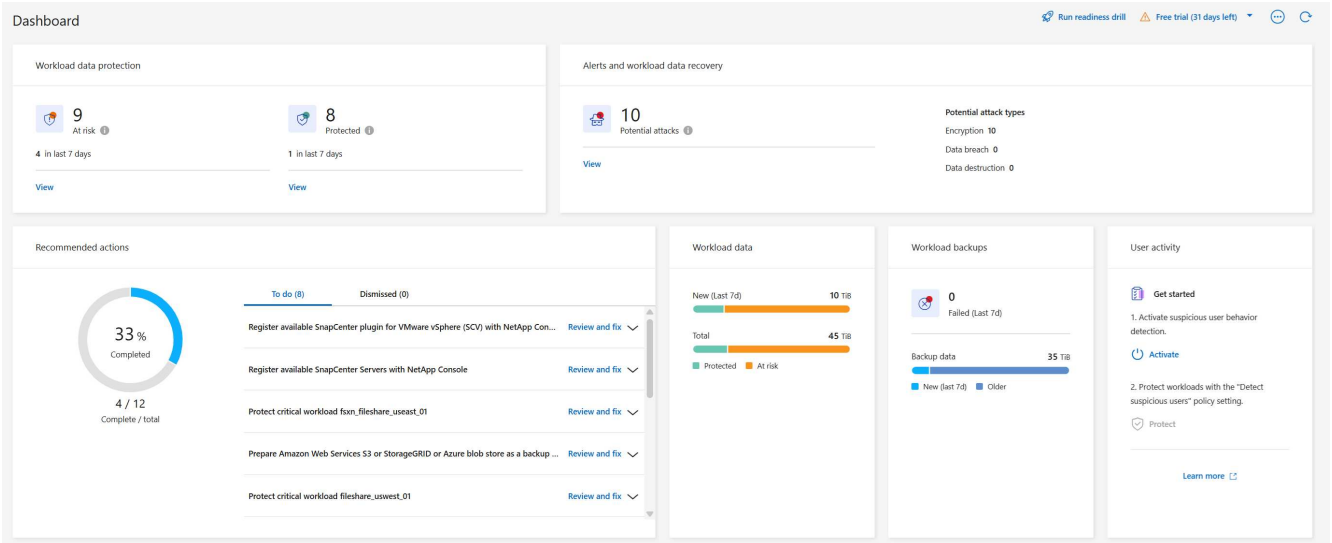


3. 특정 콘솔 에이전트의 워크로드를 검색하려면 워크로드를 검색하려는 콘솔 에이전트 옆에 있는 *시스템 선택*을 선택합니다.
4. 워크로드를 검색할 시스템을 선택하세요.
5. *발견*을 선택하세요.

   랜섬웨어 복원력은 선택된 시스템이 있는 콘솔 에이전트에 대해서만 워크로드 데이터를 검색합니다. 이 과정은 몇 분 정도 걸릴 수 있습니다.

6. 검색된 워크로드 목록을 다운로드하려면 *결과 다운로드*를 선택하세요.
7. 랜섬웨어 복원력 대시보드를 표시하려면 *대시보드로 이동*을 선택하세요.

   대시보드는 데이터 보호 상태를 보여줍니다. 새로운 워크로드가 발견되면 위험에 처한 워크로드나 보호된 워크로드의 수가 업데이트됩니다.



"대시보드가 무엇을 보여주는지 알아보세요."

이전에 선택한 시스템에 대해 새로 생성된 워크로드를 검색합니다.

검색할 시스템을 이미 선택한 경우 대시보드에서 해당 환경에 대해 새로 생성된 워크로드를 검색할 수 있습니다.

단계

1. 마지막 발견 날짜를 확인하려면 랜섬웨어 복원력 대시보드 오른쪽 상단에 있는 새로 고침 아이콘 옆에 있는 날짜와 시간 스탬프를 확인하세요.
2. 대시보드에서 *새로 고침 아이콘*을 선택하여 새로운 워크로드를 찾으세요.

새로운 시스템을 발견하세요

이미 시스템을 발견했다면 새로운 시스템이나 이전에 선택하지 않은 시스템을 찾을 수 있습니다.

단계

1. 랜섬웨어 복원력 메뉴에서 세로를 선택하세요. … 오른쪽 상단의 옵션. 드롭다운 메뉴에서 *설정*을 선택하세요.
2. 워크로드 검색 카드에서 *워크로드 검색*을 선택합니다.

   이 과정은 몇 분 정도 걸릴 수 있으며, 로딩 아이콘이 진행 상황을 보여줍니다.

3. 랜섬웨어 복원력은 지원되는 시스템과 지원되지 않는 시스템을 모두 발견합니다. 랜섬웨어 복원력은 ONTAP 버전이 필수 버전보다 낮으면 시스템을 지원하지 않습니다. 지원되지 않는 시스템 위에 마우스를 올리면 툴팁에 그 이유가 표시됩니다. 워크로드를 검색할 시스템을 선택하세요.
4. *발견*을 선택하세요.

NetApp Ransomware Resilience 에서 랜섬웨어 공격 대비 훈련을 실시하세요.

새로운 샘플 워크로드에 대한 공격을 시뮬레이션하여 랜섬웨어 공격 준비 훈련을 실행합니다. 시뮬레이션된 공격을 조사하고 작업 부하를 복구합니다. 이 기능을 사용하여 경고 알림, 대응 및 복구를 테스트하세요. 필요한 만큼 자주 훈련을 실시하세요.

실제 작업 부하 데이터에는 영향을 미치지 않습니다.

NFS 및 CIFS(SMB) 워크로드에 대한 준비 훈련을 실행할 수 있습니다.

랜섬웨어 공격 대비 훈련 구성

시뮬레이션을 실행하기 전에 설정 페이지에서 드릴을 설정하세요. 상단 메뉴의 작업 옵션에서 설정 페이지에 액세스하세요.

다음 상황에서는 사용자 이름과 비밀번호를 입력해야 합니다.

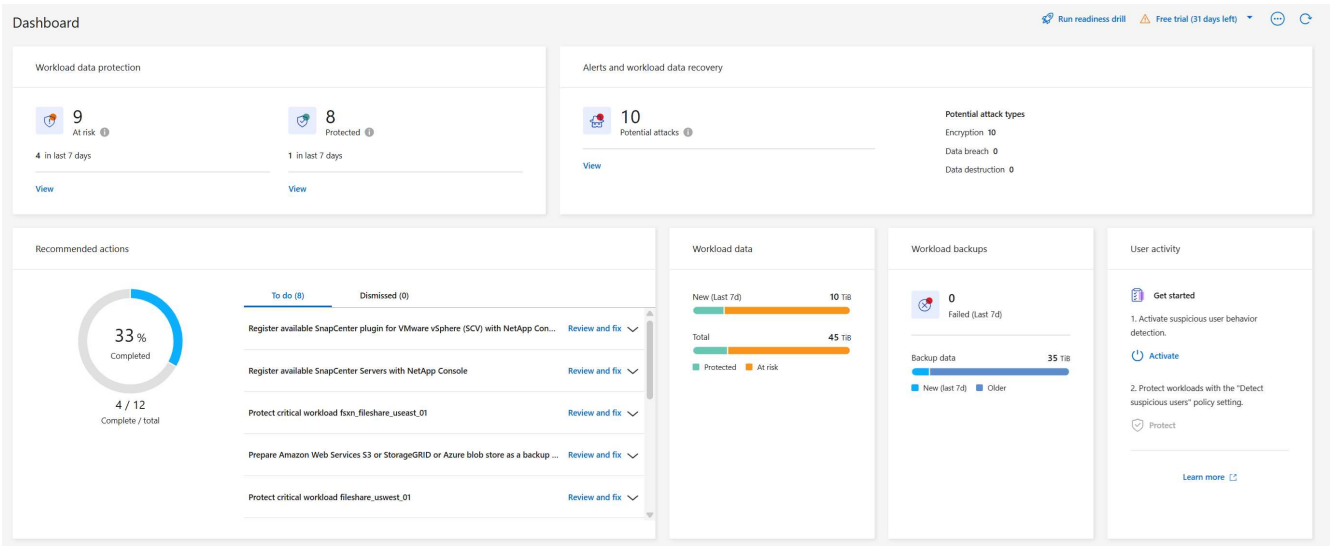
- 이전에 선택한 스토리지 VM에 대해 사용자 이름 또는 암호가 변경된 경우
- 다른 CIFS(SMB) 스토리지 VM을 선택하는 경우

- 다른 테스트 작업 이름을 입력하는 경우

필수 콘솔 역할 이 작업을 수행하려면 조직 관리자, 폴더 또는 프로젝트 관리자, 랜섬웨어 복원력 관리자 역할이 필요합니다. "NetApp Console 의 랜섬웨어 복원력 역할에 대해 알아보세요" .

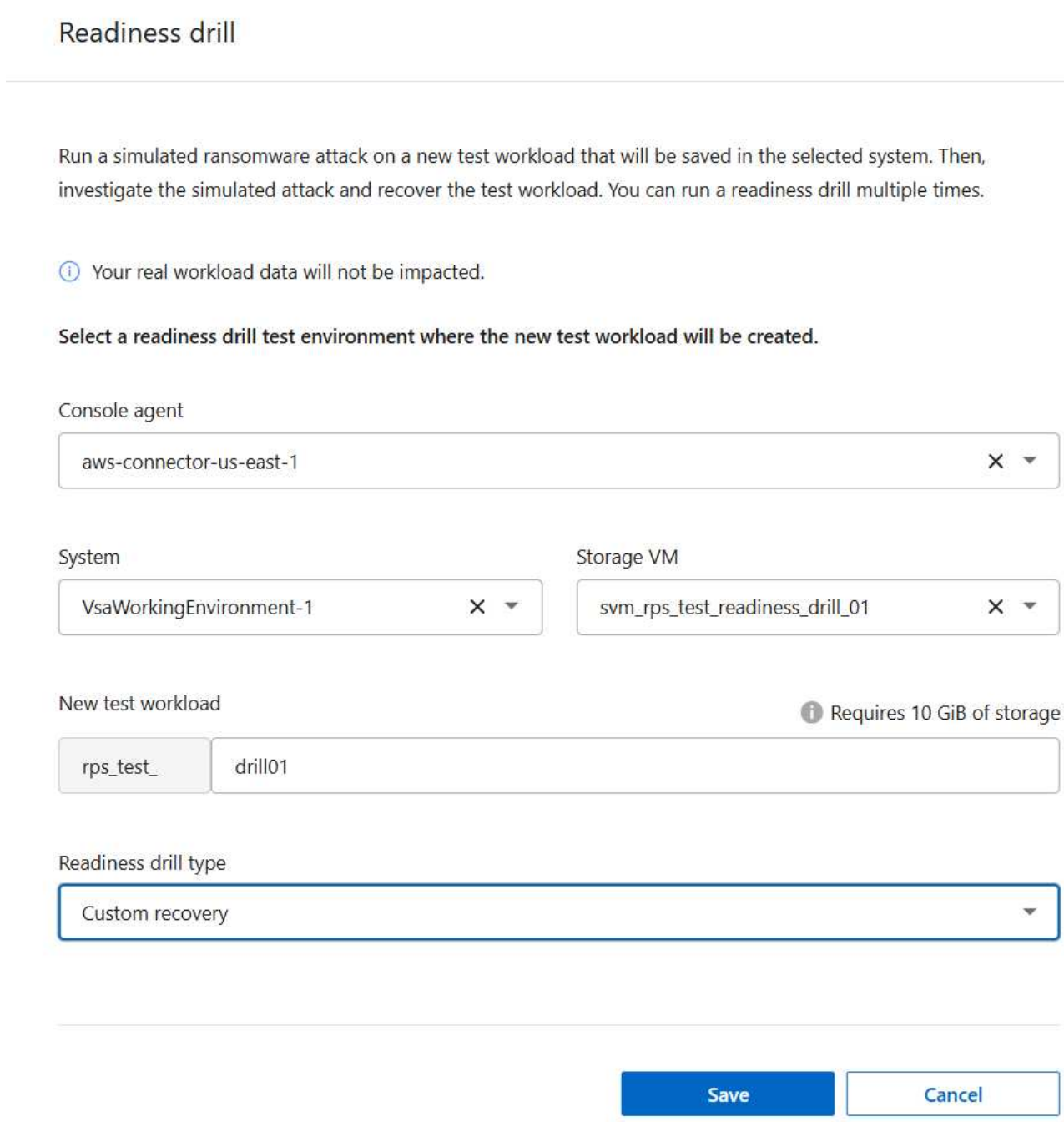
단계

1. NetApp Ransomware Resilience 메뉴에서 오른쪽 상단에 있는 준비 훈련 실행 버튼을 선택합니다.



2. 설정 페이지의 준비 훈련 카드에서 *구성*을 선택합니다.

   콘솔에 준비 훈련 구성 페이지가 표시됩니다.



3. 다음을 수행하세요.
   a. 준비 훈련에 사용할 콘솔 에이전트를 선택하세요.
   b. 테스트 시스템을 선택하세요.
   c. 테스트 스토리지 SVM을 선택하세요.
   d. CIFS(SMB) 스토리지 VM을 선택한 경우 사용자 이름 및 암호 필드가 나타납니다. 스토리지 VM의 사용자 이름과 비밀번호를 입력하세요.
   e. 준비 훈련 유형을 선택하세요. 암호화 데이터 침해로 인해 수동으로 복구하려면 사용자 지정 복구를 선택하세요. 의심스러운 사용자 활동으로부터 복구하려면 데이터 침해를 선택하세요.
   f. 생성할 새 테스트 워크로드의 이름을 입력하세요. 이름에 대시를 포함하지 마세요.

4. *저장*을 선택하세요.

나중에 설정 페이지를 사용하여 준비 훈련 구성을 편집할 수 있습니다.

준비 훈련을 시작하세요

준비 훈련을 구성한 후 훈련을 시작할 수 있습니다.

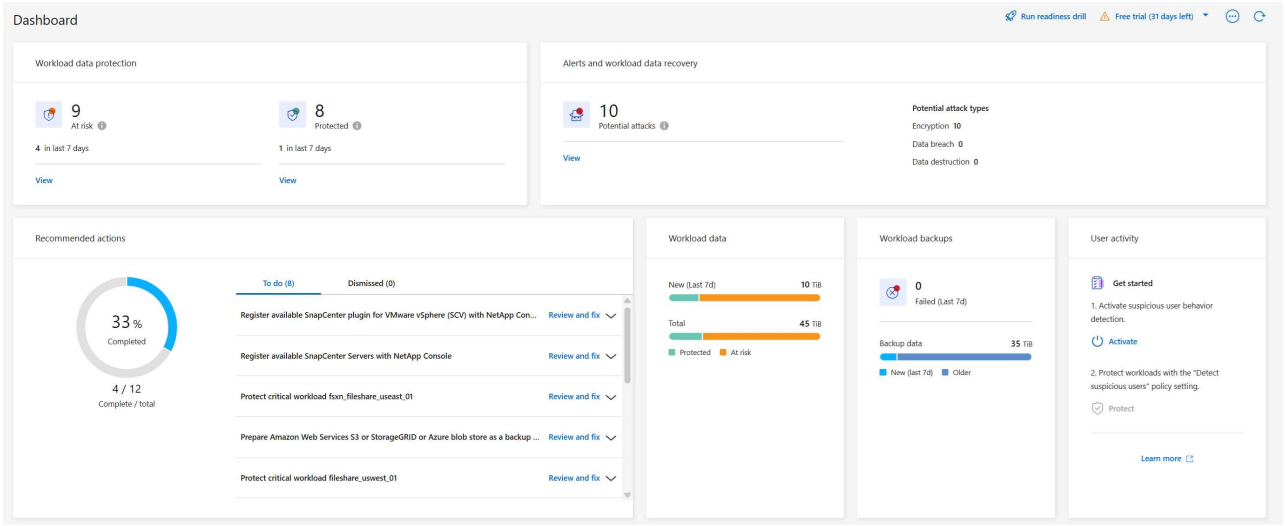
필수 콘솔 역할 이 작업을 수행하려면 조직 관리자, 폴더 또는 프로젝트 관리자, 랜섬웨어 복원력 관리자 역할이 필요합니다. "NetApp Console 의 랜섬웨어 복원력 역할에 대해 알아보세요" .

준비 훈련을 시작하면 Ransomware Resilience는 학습 모드를 건너뛰고 활성 모드에서 훈련을 시작합니다. 워크로드의 감지 상태가 활성입니다.

탐지 정책이 최근에 할당되고 랜섬웨어 복원력이 워크로드를 검사하는 경우 워크로드는 랜섬웨어 탐지 학습 모드 상태를 가질 수 있습니다.

단계

1. 다음 중 하나를 수행하세요.
   - 랜섬웨어 복원력 메뉴에서 오른쪽 상단에 있는 준비 훈련 실행 버튼을 선택하세요.



   - 또는 설정 페이지의 준비 훈련 카드에서 *시작*을 선택하세요.

훈련이 진행되는 동안에는 준비 훈련 구성을 편집할 수 없습니다. 드릴을 재설정하여 멈추고 구성을 수정할 수 있습니다.

준비 훈련 경고에 대응하세요

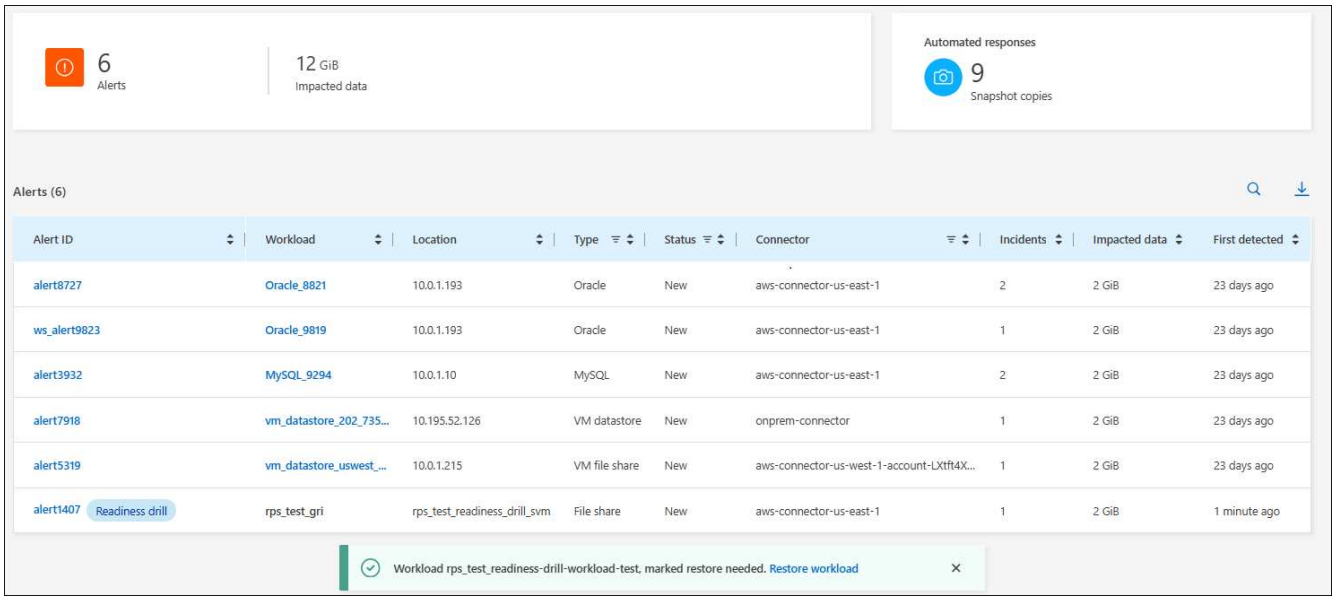
준비 훈련 알림에 응답하여 준비 상태를 테스트하세요.

필수 콘솔 역할 이 작업을 수행하려면 조직 관리자, 폴더 또는 프로젝트 관리자, 랜섬웨어 복원력 관리자 역할이 필요합니다. "NetApp Console 의 랜섬웨어 복원력 역할에 대해 알아보세요" .

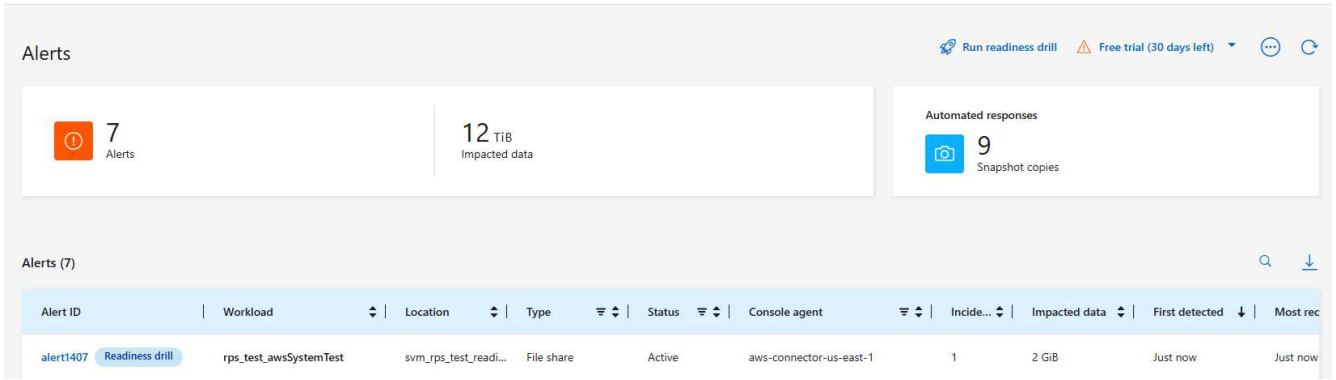
단계

1. 랜섬웨어 복원력 메뉴에서 *알림*을 선택합니다.

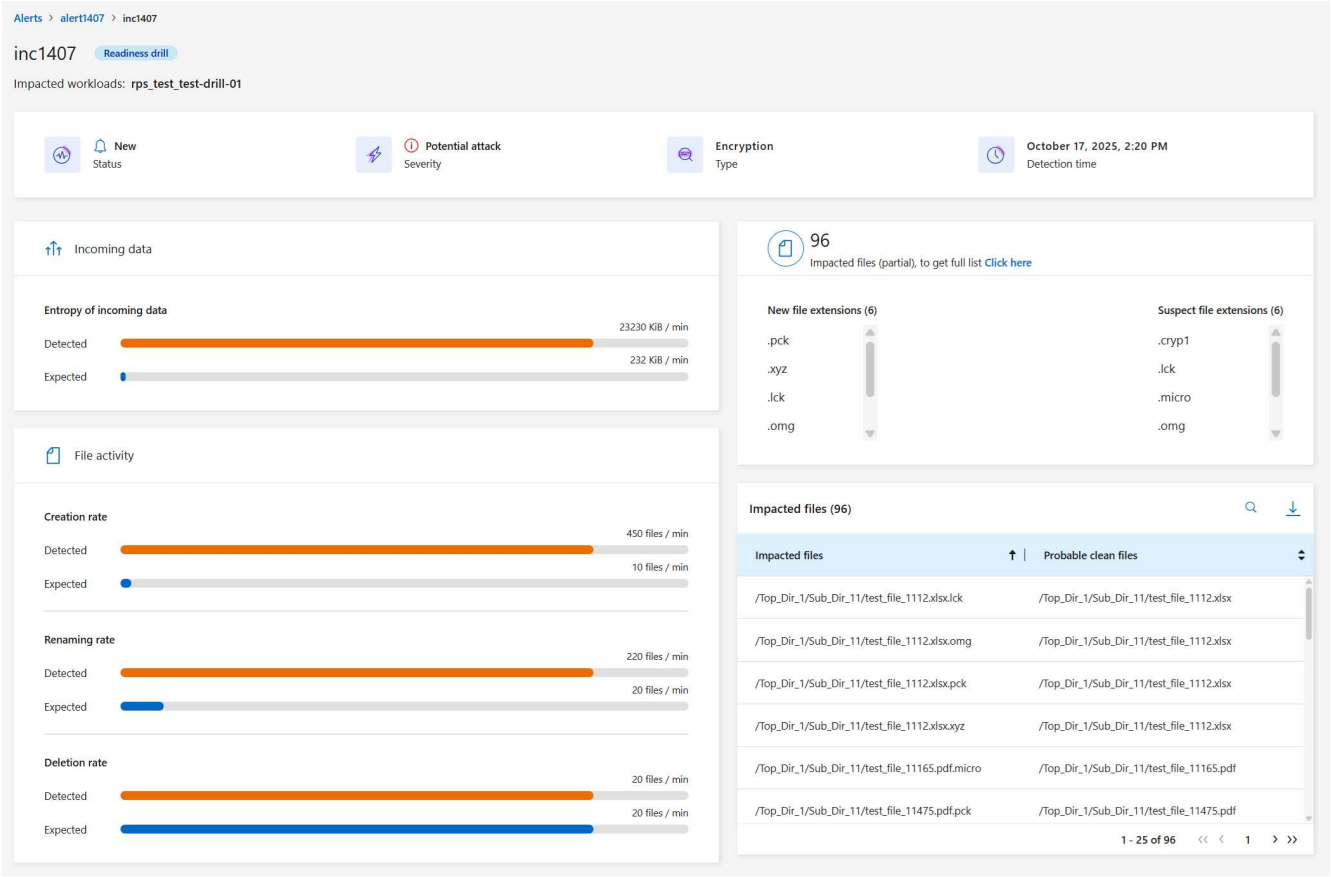
   콘솔에 알림 페이지가 표시됩니다. 알림 ID 열에서 ID 옆에 "준비 훈련"이 표시됩니다.



2. "준비 훈련" 표시가 있는 알림을 선택하세요. 사고 알림 목록은 알림 세부 정보 페이지에 나타납니다.



3. 경고 사건을 검토하세요.
4. 알림 사건을 선택하세요.



다음은 살펴봐야 할 몇 가지 사항입니다.

- 잠재적인 공격의 심각도를 살펴보세요.

  심각도가 사용자가 악의적인 활동을 했다고 의심되는 경우 사용자 이름을 검토하세요. 당신도 할 수 있습니다 "사용자를 차단합니다."

- 파일 활동과 의심되는 프로세스를 살펴보세요.
  - 감지된 수신 데이터를 예상 데이터와 비교해 보세요.
  - 감지된 파일의 생성률을 예상 속도와 비교하여 살펴보세요.
  - 예상 속도와 비교하여 감지된 파일 이름 변경 속도를 살펴보세요.
  - 예상 비율과 비교해서 삭제 비율을 살펴보세요.
- 영향을 받은 파일 목록을 살펴보세요. 공격을 일으킬 수 있는 확장 프로그램을 살펴보세요.
- 영향을 받은 파일과 디렉토리의 수를 검토하여 공격의 영향과 범위를 파악합니다.

테스트 작업 부하를 복원합니다.

준비 훈련 알림을 검토한 후 필요한 경우 테스트 작업 부하를 복원합니다.

필수 콘솔 역할 이 작업을 수행하려면 조직 관리자, 폴더 또는 프로젝트 관리자, 랜섬웨어 복원력 관리자 역할이 필요합니다. "NetApp Console 의 랜섬웨어 복원력 역할에 대해 알아보세요" .

단계

1. 알림 세부 정보 페이지로 돌아갑니다.
2. 테스트 작업 부하를 복구해야 하는 경우 다음을 수행하세요.
   - *복원 필요 표시*를 선택하세요.
   - 확인 내용을 검토하고 확인 상자에서 *복원 필요 표시*를 선택하세요.
     - 랜섬웨어 복원력 메뉴에서 *복구*를 선택합니다.
     - 복원하려는 "준비 훈련"으로 표시된 테스트 워크로드를 선택하세요.
     - *복원*을 선택하세요.
     - 복원 페이지에서 복원에 대한 정보를 제공합니다.
   - 소스 스냅샷 복사본을 선택합니다.
   - 대상 볼륨을 선택하세요.
3. 복원 검토 페이지에서 *복원*을 선택합니다.

   콘솔은 복구 페이지에서 준비 훈련 복원 상태를 "진행 중"으로 표시합니다.

   복원이 완료되면 콘솔은 워크로드 상태를 *복원됨*으로 변경합니다.

4. 복구된 작업 부하를 검토합니다.

복원 프로세스에 대한 자세한 내용은 다음을 참조하세요."랜섬웨어 공격으로부터 복구(사고가 해결된 후)" .

준비 훈련 후 알림 상태 변경

준비 훈련 알림을 검토하고 작업 부하를 복구한 후 필요한 경우 알림 상태를 변경합니다.

콘솔 역할이 필요합니다 조직 관리자, 폴더 또는 프로젝트 관리자, 랜섬웨어 복원력 관리자. "모든 서비스에 대한 콘솔 액세스 역할에 대해 알아보세요." .

단계

1. 알림 세부 정보 페이지로 돌아갑니다.
2. 알림을 다시 선택하세요.
3. *상태 편집*을 선택하여 상태를 표시하고 상태를 다음 중 하나로 변경하세요.
   - 해제됨: 해당 활동이 랜섬웨어 공격이 아니라고 의심되는 경우 상태를 해제됨으로 변경하세요.

     공격을 해제한 후에는 다시 되돌릴 수 없습니다. 작업 부하를 해제하면 잠재적인 랜섬웨어 공격에 대응하여 자동으로 생성된 모든 스냅샷 사본이 영구적으로 삭제됩니다. 경고를 무시하면 준비 훈련이 완료된 것으로 간주됩니다.

   - 해결됨: 사건이 완화되었습니다.

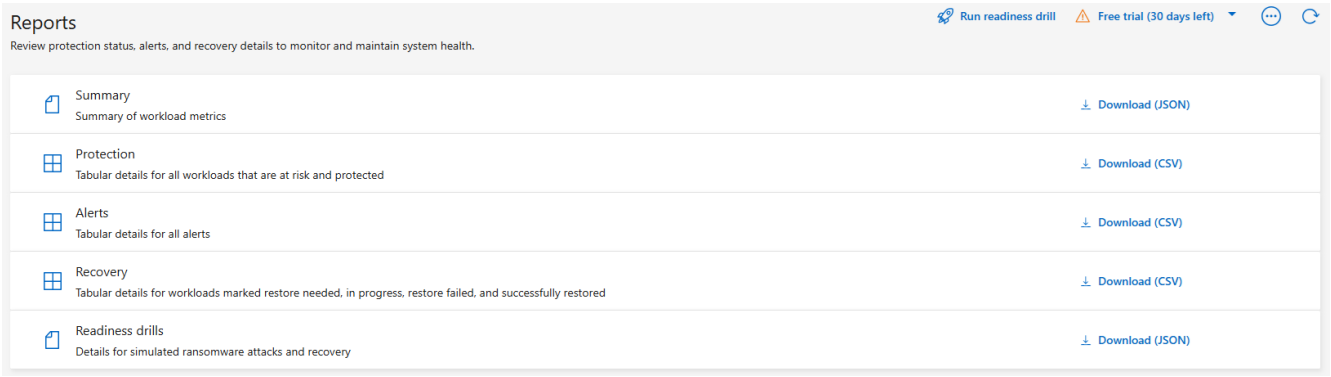
준비 훈련에 대한 검토 보고서

준비 훈련이 완료된 후 훈련 보고서를 검토하고 저장할 수 있습니다.

필수 콘솔 역할 이 작업을 수행하려면 조직 관리자, 폴더 또는 프로젝트 관리자, 랜섬웨어 복원력 관리자 또는 랜섬웨어 복원력 뷰어 역할이 필요합니다. "NetApp Console 의 랜섬웨어 복원력 역할에 대해 알아보세요" .

단계

1. 랜섬웨어 복원력 메뉴에서 *보고서*를 선택합니다.



2. *준비 훈련*과 *다운로드*를 선택하여 준비 훈련 보고서를 다운로드하세요.

NetApp Ransomware Resilience 에서 보호 설정 구성

설정 옵션에 액세스하여 백업 대상을 구성하고, 외부 보안 및 이벤트 관리(SIEM) 시스템으로 데이터를 보내고, 공격 준비 훈련을 실시하고, 워크로드 검색을 구성하거나, 의심스러운 사용자 활동 감지를 구성할 수 있습니다.

필수 콘솔 역할 이 작업을 수행하려면 조직 관리자, 폴더 또는 프로젝트 관리자, 랜섬웨어 복원력 관리자 역할이 필요합니다. "NetApp Console 의 랜섬웨어 복원력 역할에 대해 알아보세요" .

설정 페이지에서 무엇을 할 수 있나요**?** 설정 페이지에서 다음 작업을 수행할 수 있습니다.

- 랜섬웨어 공격을 시뮬레이션하기 위해 준비 훈련을 실시하고 시뮬레이션된 랜섬웨어 경고에 대응합니다. 자세한 내용은 다음을 참조하십시오. "랜섬웨어 공격 대비 훈련을 실시하세요" .
- 워크로드 검색을 구성합니다.
- 의심스러운 사용자 활동 보고를 구성합니다.
- 백업 대상을 추가합니다.
- 보안 및 이벤트 관리 시스템(SIEM)을 연결하여 위협 분석 및 감지를 수행하세요. 위협 감지를 활성화하면 위협 분석을 위해 SIEM으로 데이터가 자동으로 전송됩니다.

설정 페이지에 직접 액세스하세요

상단 메뉴 근처의 작업 옵션을 통해 설정 페이지에 쉽게 접근할 수 있습니다.

1. 랜섬웨어 복원력에서 세로를 선택하세요 … 오른쪽 상단의 옵션.
2. 드롭다운 메뉴에서 *설정*을 선택하세요.

랜섬웨어 공격 시뮬레이션

새로 생성된 샘플 워크로드에 대한 랜섬웨어 공격을 시뮬레이션하여 랜섬웨어 대비 훈련을 실시합니다. 그런 다음 시뮬레이션된 공격을 조사하고 샘플 작업 부하를 복구합니다. 이 기능은 경고 알림, 대응 및 복구 프로세스를 테스트하여 실제 랜섬웨어 공격이 발생할 경우 대비가 되어 있는지 확인하는 데 도움이 됩니다. 랜섬웨어 대비 훈련은 여러 번 실행할 수 있습니다.

자세한 내용은 다음을 참조하세요."랜섬웨어 공격 대비 훈련을 실시하세요" .

워크로드 검색 구성

환경에서 새로운 워크로드를 자동으로 검색하도록 워크로드 검색을 구성할 수 있습니다.

1. 설정 페이지에서 워크로드 검색 타일을 찾으세요.
2. 워크로드 검색 타일에서 *워크로드 검색*을 선택합니다.

   이 페이지에서는 이전에 선택하지 않은 시스템이 있는 콘솔 에이전트, 새로 사용 가능한 콘솔 에이전트, 새로 사용 가능한 시스템을 보여줍니다. 이 페이지에는 이전에 선택된 시스템이 표시되지 않습니다.
3. 워크로드를 검색할 콘솔 에이전트를 선택합니다.
4. 시스템 목록을 검토하세요.
5. 워크로드를 검색하려는 시스템을 선택하거나 표 상단의 상자를 선택하여 검색된 모든 워크로드 환경에서 워크로드를 검색합니다.
6. 필요에 따라 다른 시스템에도 이 작업을 수행하세요.
7. *검색*을 선택하면 Ransomware Resilience가 선택한 콘솔 에이전트에서 자동으로 새 워크로드를 검색합니다.

의심스러운 사용자 활동

사용자 활동 카드에서는 의심스러운 사용자 활동을 감지하는 데 필요한 사용자 활동 에이전트를 만들고 관리할 수 있습니다.

자세한 내용은 다음을 참조하세요. "의심스러운 사용자 활동" .

백업 대상 추가

랜섬웨어 복원력은 아직 백업이 없는 워크로드와 아직 백업 대상이 할당되지 않은 워크로드를 식별할 수 있습니다.

이러한 작업 부하를 보호하려면 백업 대상을 추가해야 합니다. 다음 백업 대상 중 하나를 선택할 수 있습니다.

- NetApp StorageGRID
- 아마존 웹 서비스(AWS)
- 구글 클라우드 플랫폼
- 마이크로소프트 애저

Amazon FSx for NetApp ONTAP 의 워크로드에는 백업 대상을 사용할 수 없습니다. FSx for ONTAP 백업 서비스를 사용하여 백업 작업을 수행합니다.

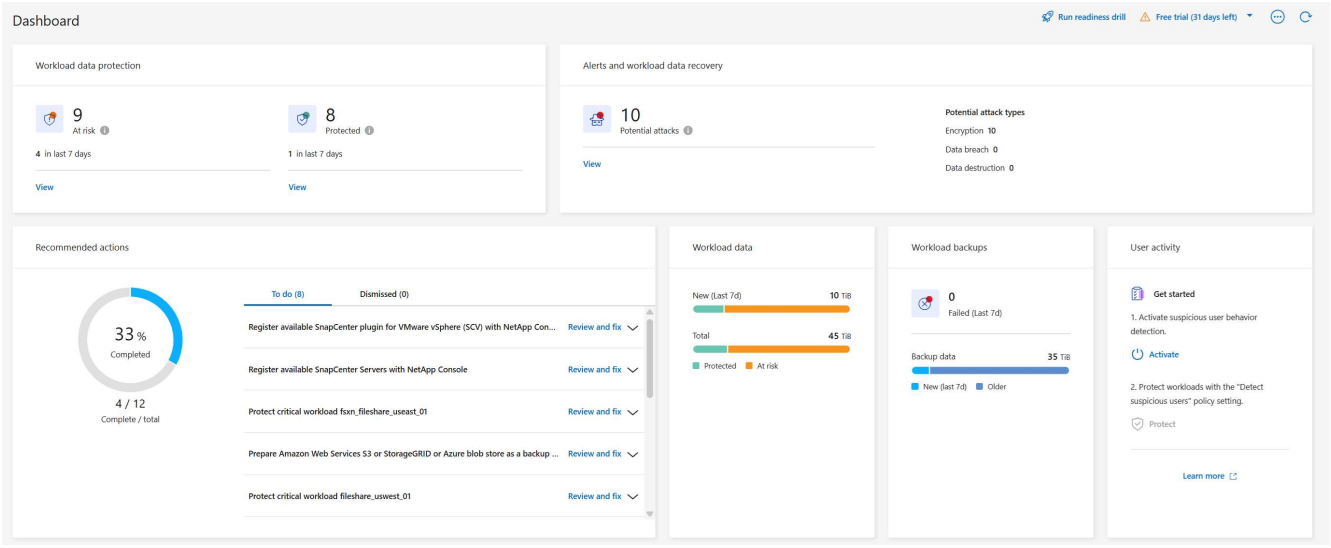
대시보드에서 권장하는 작업을 기반으로 백업 대상을 추가하거나 메뉴의 설정 옵션에 액세스하여 백업 대상을 추가할 수 있습니다.

대시보드의 권장 작업에서 백업 대상 옵션에 액세스합니다.

대시보드는 다양한 권장사항을 제공합니다. 한 가지 권장 사항은 백업 대상을 구성하는 것입니다.

단계

1. 랜섬웨어 복원력 대시보드에서 권장 작업 창을 검토하세요.



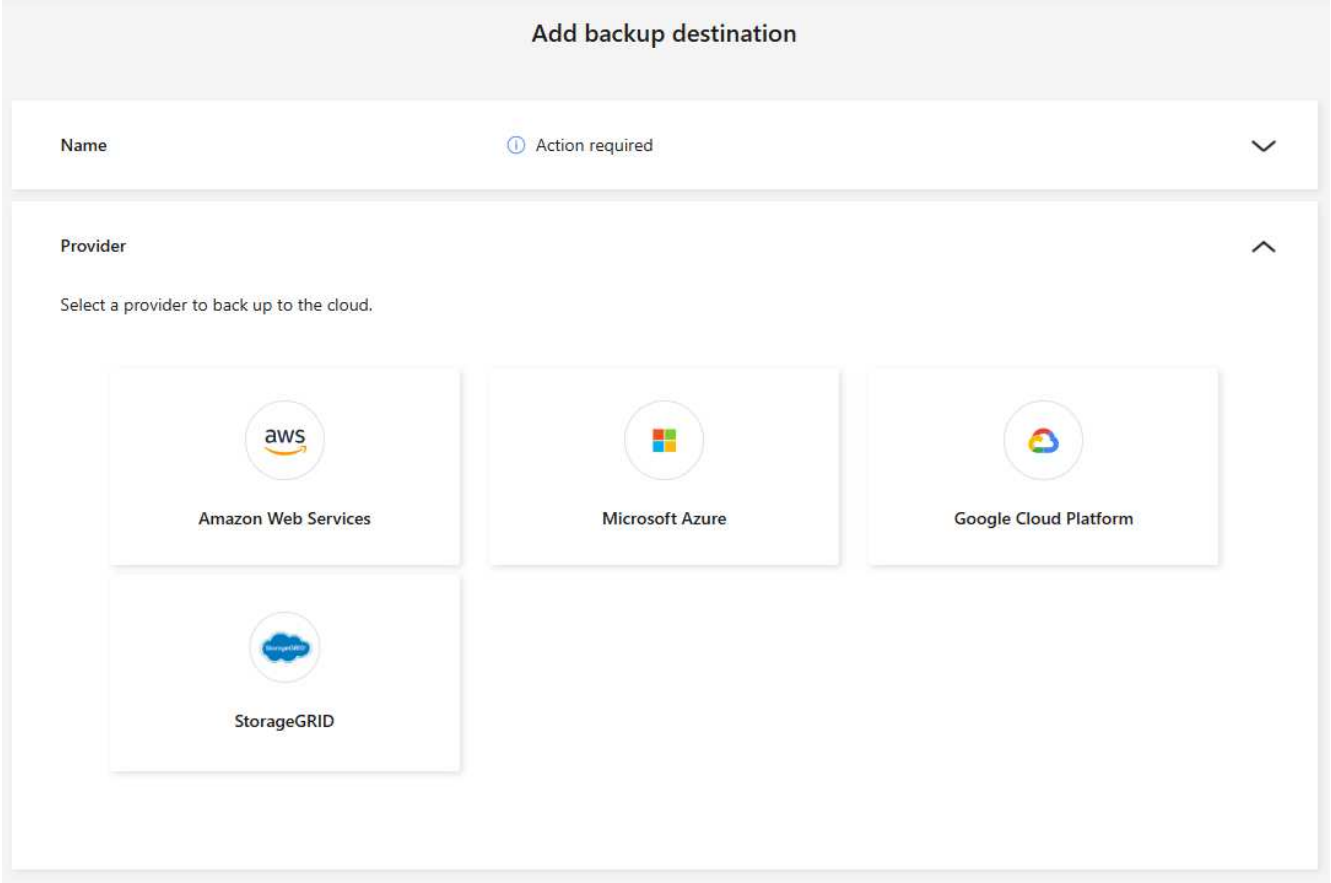
2. 대시보드에서 "[백업 제공업체]를 백업 대상으로 준비" 권장 사항에 대해 *검토 및 수정*을 선택합니다.
3. 백업 제공업체에 따라 지침을 계속 따르세요.

StorageGRID 백업 대상으로 추가

NetApp StorageGRID 백업 대상으로 설정하려면 다음 정보를 입력하세요.

단계

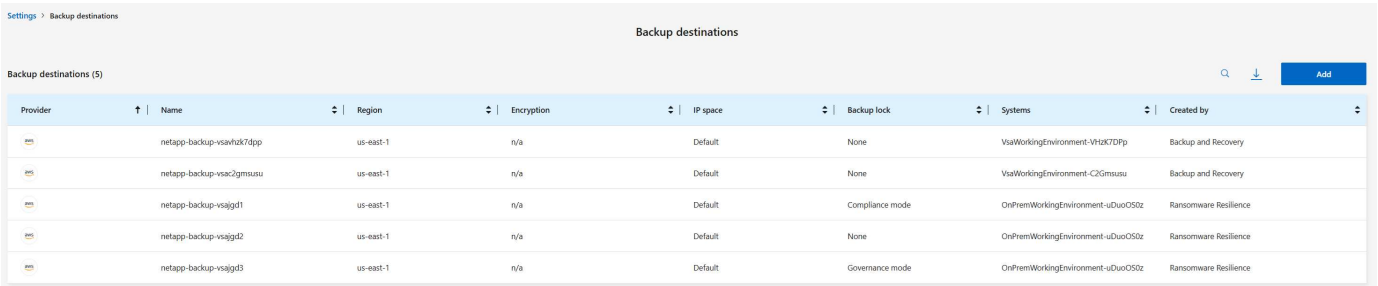
1. 설정 **>** 백업 대상 페이지에서 *추가*를 선택합니다.
2. 백업 대상의 이름을 입력하세요.



3. * StorageGRID*를 선택하세요.
4. 각 설정 옆에 있는 아래쪽 화살표를 선택하고 값을 입력하거나 선택하세요.
   - 공급자 설정:
     - 백업을 저장할 새 버킷을 만들거나 자신의 버킷을 가져오세요.
     - StorageGRID 게이트웨이 노드의 정규화된 도메인 이름, 포트, StorageGRID 액세스 키 및 비밀 키 자격 증명입니다.
   - 네트워킹: IP 공간을 선택하세요.
     - IPspace는 백업하려는 볼륨이 있는 클러스터입니다. 이 IP공간의 클러스터 간 LIF에는 아웃바운드 인터넷 액세스가 있어야 합니다.
5. *추가*를 선택하세요.

결과

새로운 백업 대상이 백업 대상 목록에 추가됩니다.



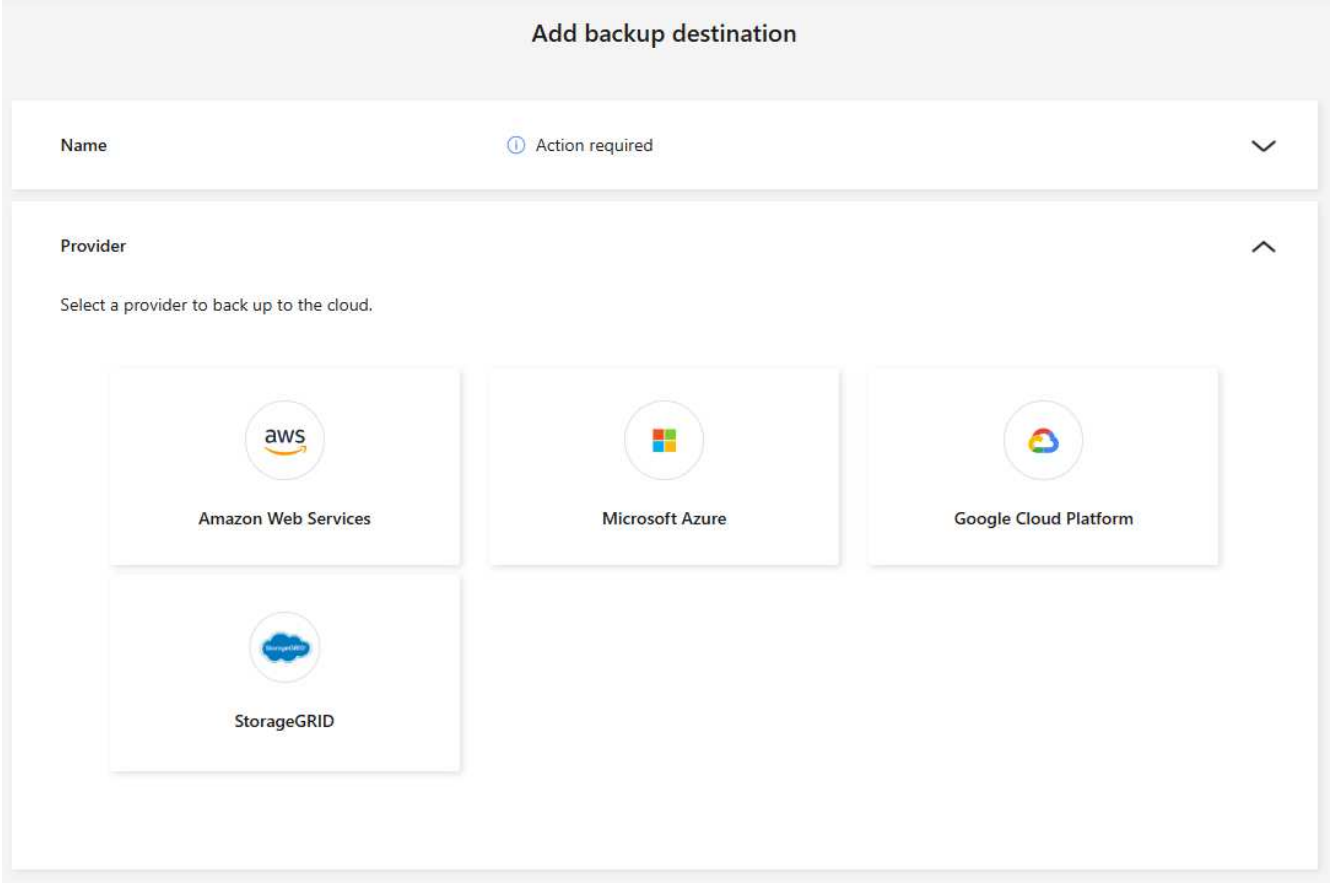
Amazon Web Services를 백업 대상으로 추가

AWS를 백업 대상으로 설정하려면 다음 정보를 입력하세요.

콘솔에서 AWS 스토리지를 관리하는 방법에 대한 자세한 내용은 다음을 참조하세요. "Amazon S3 버킷 관리" .

단계

1. 설정 > 백업 대상 페이지에서 *추가*를 선택합니다.
2. 백업 대상의 이름을 입력하세요.



3. *Amazon Web Services*를 선택하세요.
4. 각 설정 옆에 있는 아래쪽 화살표를 선택하고 값을 입력하거나 선택하세요.
   - 공급자 설정:
     - 새 버킷을 만들거나, 콘솔에 이미 버킷이 있는 경우 기존 버킷을 선택하거나, 백업을 저장할 자체 버킷을 가져옵니다.
     - AWS 자격 증명에 대한 AWS 계정, 지역, 액세스 키 및 비밀 키

       "자체 버킷을 가져오려면 S3 버킷 추가를 참조하세요." .
   - 암호화: 새로운 S3 버킷을 생성하는 경우 공급자로부터 받은 암호화 키 정보를 입력하세요. 기존 버킷을 선택한 경우 암호화 정보를 이미 사용할 수 있습니다.

     버킷의 데이터는 기본적으로 AWS 관리 키로 암호화됩니다. AWS에서 관리하는 키를 계속 사용할 수도 있고, 사용자 고유의 키를 사용하여 데이터 암호화를 관리할 수도 있습니다.

◦ 네트워킹: IP 공간을 선택하고 개인 엔드포인트를 사용할지 여부를 선택합니다.

- IPspace는 백업하려는 볼륨이 있는 클러스터입니다. 이 IP공간의 클러스터 간 LIF에는 아웃바운드 인터넷 액세스가 있어야 합니다.
- 선택적으로, 이전에 구성한 AWS 개인 엔드포인트(PrivateLink)를 사용할지 여부를 선택합니다.

  AWS PrivateLink를 사용하려면 다음을 참조하세요. "Amazon S3용 AWS PrivateLink" .

◦ 백업 잠금: 랜섬웨어 복원력을 사용하여 백업이 수정되거나 삭제되는 것을 방지할지 여부를 선택합니다. 이 옵션은 NetApp DataLock 기술을 사용합니다. 각 백업은 보존 기간 동안 또는 최소 30일 동안 잠기고, 최대 14일의 버퍼 기간이 추가됩니다.

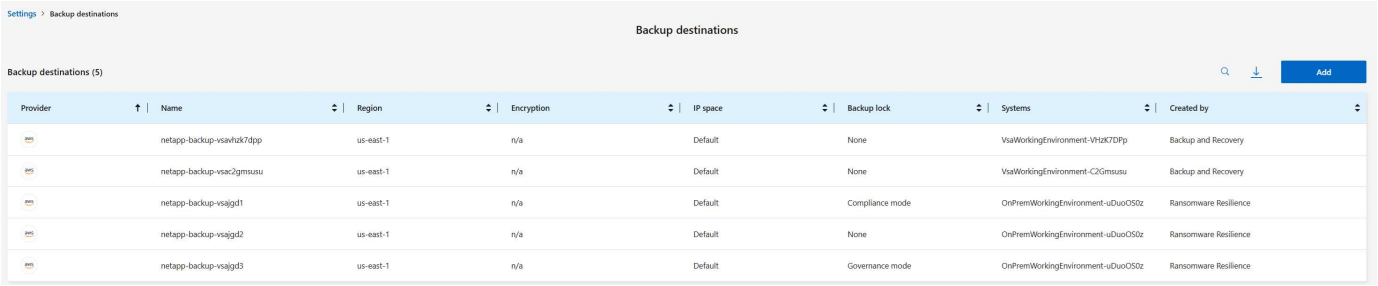
> ! 지금 백업 잠금 설정을 구성하면 나중에 백업 대상을 구성한 후에는 설정을 변경할 수 없습니다.

- 거버넌스 모드: 특정 사용자(s3:BypassGovernanceRetention 권한이 있는 사용자)는 보존 기간 동안 보호된 파일을 덮어쓰거나 삭제할 수 있습니다.
- 준수 모드: 사용자는 보존 기간 동안 보호된 백업 파일을 덮어쓰거나 삭제할 수 없습니다.

5. *추가*를 선택하세요.

결과

새로운 백업 대상이 백업 대상 목록에 추가됩니다.



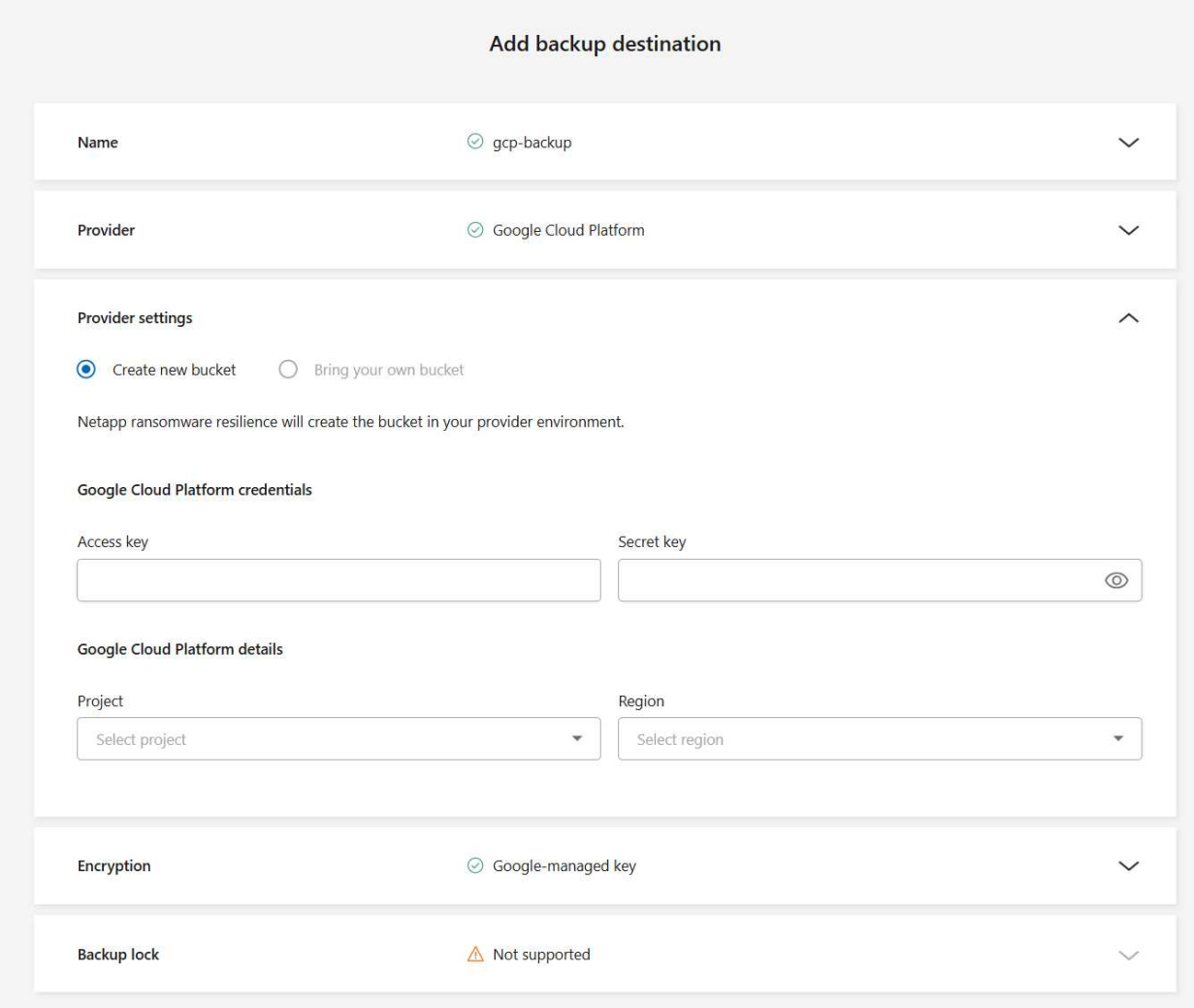
Google Cloud Platform을 백업 대상으로 추가

Google Cloud Platform(GCP)을 백업 대상으로 설정하려면 다음 정보를 입력하세요.

콘솔에서 GCP 스토리지를 관리하는 방법에 대한 자세한 내용은 다음을 참조하세요. "Google Cloud의 콘솔 에이전트 설치 옵션" .

단계

1. 설정 > 백업 대상 페이지에서 *추가*를 선택합니다.
2. 백업 대상의 이름을 입력하세요.
3. *Google Cloud Platform*을 선택하세요.
4. 각 설정 옆에 있는 아래쪽 화살표를 선택하고 값을 입력하거나 선택하세요.
   ◦ 공급자 설정:
   - 새로운 버킷을 만듭니다. 액세스 키와 비밀 키를 입력하세요.
   - Google Cloud Platform 프로젝트와 지역을 입력하거나 선택하세요.



◦ 암호화: 새 버킷을 만드는 경우 공급자로부터 받은 암호화 키 정보를 입력하세요. 기존 버킷을 선택한 경우 암호화 정보를 이미 사용할 수 있습니다.

버킷의 데이터는 기본적으로 Google에서 관리하는 키로 암호화됩니다. Google에서 관리하는 키를 계속 사용할 수 있습니다.

◦ 네트워킹: IP 공간을 선택하고 개인 엔드포인트를 사용할지 여부를 선택합니다.

- IPspace는 백업하려는 볼륨이 있는 클러스터입니다. 이 IP공간의 클러스터 간 LIF에는 아웃바운드 인터넷 액세스가 있어야 합니다.
- 선택적으로, 이전에 구성한 GCP 개인 엔드포인트(PrivateLink)를 사용할지 여부를 선택합니다.

5. *추가*를 선택하세요.

결과

새로운 백업 대상이 백업 대상 목록에 추가됩니다.

Microsoft Azure를 백업 대상으로 추가

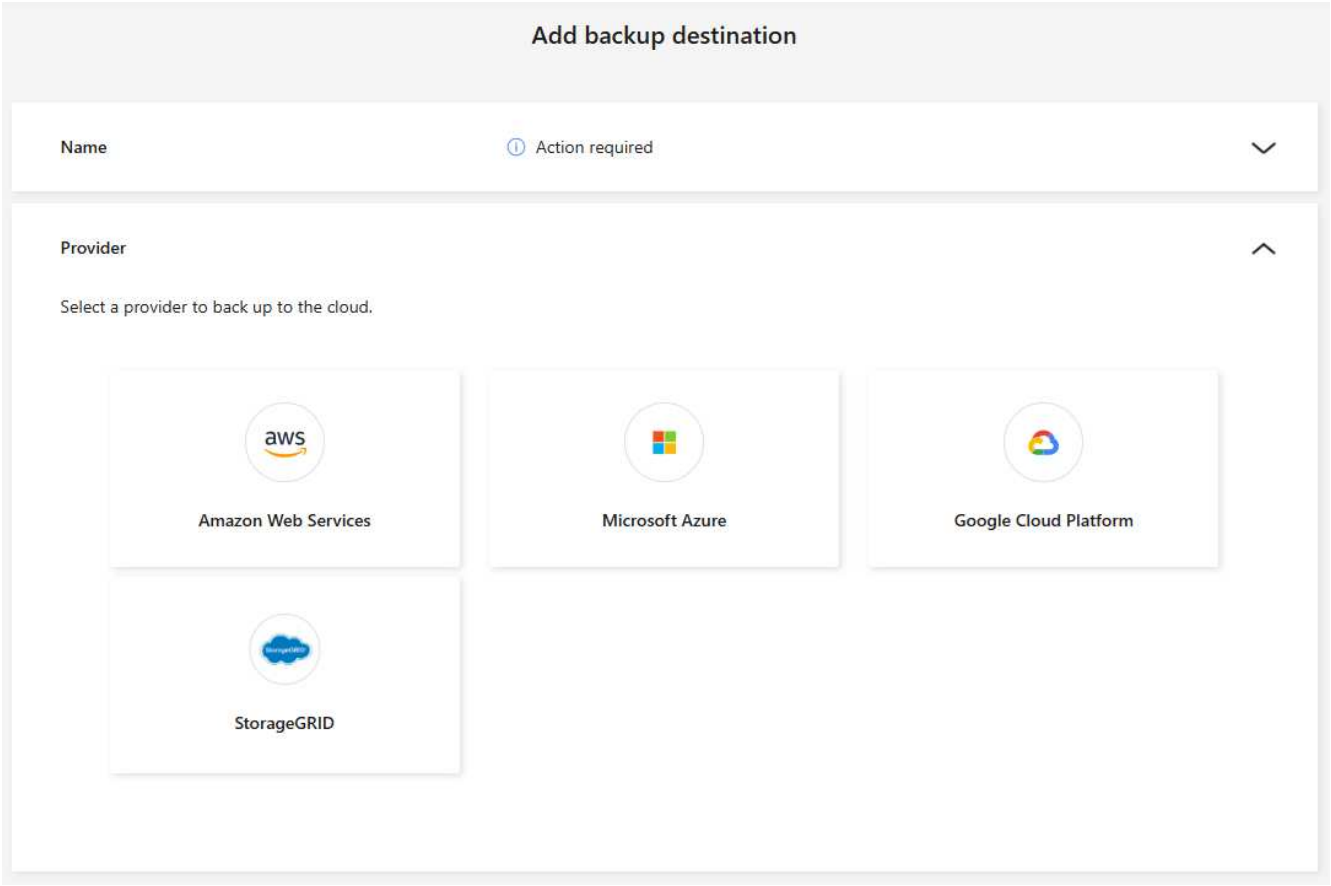
Azure를 백업 대상으로 설정하려면 다음 정보를 입력하세요.

콘솔에서 Azure 자격 증명 및 Marketplace 구독을 관리하는 방법에 대한 자세한 내용은 다음을 참조하세요. "Azure

자격 증명 및 Marketplace 구독 관리" .

단계

1. 설정 > 백업 대상 페이지에서 *추가*를 선택합니다.
2. 백업 대상의 이름을 입력하세요.



3. *Azure*를 선택하세요.
4. 각 설정 옆에 있는 아래쪽 화살표를 선택하고 값을 입력하거나 선택하세요.
   - 공급자 설정:
     - 새 스토리지 계정을 만들거나, 콘솔에 이미 있는 경우 기존 계정을 선택하거나, 백업을 저장할 자체 스토리지 계정을 가져오세요.
     - Azure 자격 증명에 대한 Azure 구독, 지역 및 리소스 그룹

       "자체 저장소 계정을 가져오려면 Azure Blob 저장소 계정 추가를 참조하세요." .
   - 암호화: 새로운 저장소 계정을 만드는 경우 공급업체에서 제공한 암호화 키 정보를 입력하세요. 기존 계정을 선택한 경우 암호화 정보를 이미 사용할 수 있습니다.

     기본적으로 계정의 데이터는 Microsoft에서 관리하는 키로 암호화됩니다. Microsoft에서 관리하는 키를 계속 사용할 수도 있고, 사용자 고유의 키를 사용하여 데이터 암호화를 관리할 수도 있습니다.
   - 네트워킹: IP 공간을 선택하고 개인 엔드포인트를 사용할지 여부를 선택합니다.
     - IPspace는 백업하려는 볼륨이 있는 클러스터입니다. 이 IP공간의 클러스터 간 LIF에는 아웃바운드 인터넷

액세스가 있어야 합니다.

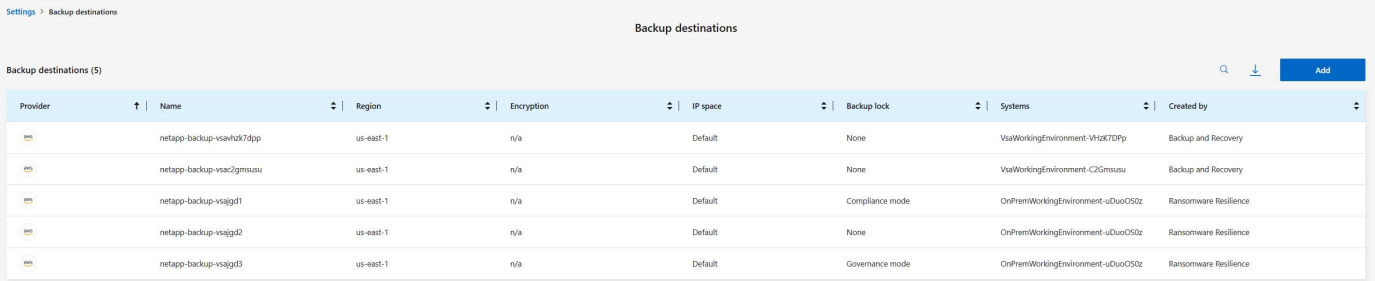
- 선택적으로, 이전에 구성한 Azure 개인 엔드포인트를 사용할지 여부를 선택합니다.

  Azure PrivateLink를 사용하려면 다음을 참조하세요. "Azure 프라이빗 링크" .

5. *추가*를 선택하세요.

결과

새로운 백업 대상이 백업 대상 목록에 추가됩니다.



위협 분석 및 탐지를 위해 보안 및 이벤트 관리 시스템(SIEM)에 연결합니다.

위협 분석 및 감지를 위해 보안 및 이벤트 관리 시스템(SIEM)에 자동으로 데이터를 전송할 수 있습니다. SIEM으로 AWS Security Hub, Microsoft Sentinel 또는 Splunk Cloud를 선택할 수 있습니다.

랜섬웨어 복원력에서 SIEM을 활성화하기 전에 SIEM 시스템을 구성해야 합니다.

SIEM에 전송되는 이벤트 데이터에 관하여

랜섬웨어 복원력은 다음과 같은 이벤트 데이터를 SIEM 시스템으로 전송할 수 있습니다.

- 문맥:
  - **os**: ONTAP 값을 갖는 상수입니다.
  - **os_version**: 시스템에서 실행 중인 ONTAP 버전입니다.
  - **connector_id**: 시스템을 관리하는 콘솔 에이전트의 ID입니다.
  - **cluster_id**: ONTAP 에서 시스템에 대해 보고한 클러스터 ID입니다.
  - **svm_name**: 경고가 발견된 SVM의 이름입니다.
  - **volume_name**: 경고가 발견된 볼륨의 이름입니다.
  - **volume_id**: ONTAP 에서 시스템에 대해 보고한 볼륨의 ID입니다.
- 사건:
  - **incident_id**: Ransomware Resilience에서 공격을 받는 볼륨에 대해 Ransomware Resilience에서 생성한 사고 ID입니다.
  - **alert_id**: Ransomware Resilience에서 워크로드에 대해 생성한 ID입니다.
  - 심각도: 다음 경보 수준 중 하나: "위험", "높음", "보통", "낮음".
  - 설명: 감지된 알림에 대한 세부 정보(예: "arp_learning_mode_test_2630 워크로드에서 잠재적인 랜섬웨어 공격이 감지되었습니다")

위협 탐지를 위해 **AWS Security Hub** 구성

랜섬웨어 복원력에서 AWS Security Hub를 활성화하기 전에 AWS Security Hub에서 다음과 같은 고급 단계를 수행해야 합니다.

- AWS Security Hub에서 권한을 설정합니다.
- AWS Security Hub에서 인증 액세스 키와 비밀 키를 설정합니다. (여기서는 이러한 단계를 제공하지 않습니다.)

AWS Security Hub에서 권한을 설정하는 단계

1. *AWS IAM 콘솔*로 이동합니다.
2. *정책*을 선택하세요.
3. 다음 코드를 JSON 형식으로 사용하여 정책을 만듭니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "NetAppSecurityHubFindings",
      "Effect": "Allow",
      "Action": [
        "securityhub:BatchImportFindings",
        "securityhub:BatchUpdateFindings"
      ],
      "Resource": [
        "arn:aws:securityhub:*:*:product/*/default",
        "arn:aws:securityhub:*:*:hub/default"
      ]
    }
  ]
}
```

위협 탐지를 위해 **Microsoft Sentinel** 구성

랜섬웨어 복원력에서 Microsoft Sentinel을 활성화하기 전에 Microsoft Sentinel에서 다음과 같은 고급 단계를 수행해야 합니다.

- 필수 조건
  - Microsoft Sentinel을 활성화합니다.
  - Microsoft Sentinel에서 사용자 지정 역할을 만듭니다.
- 등록
  - Microsoft Sentinel에서 이벤트를 받으려면 Ransomware Resilience를 등록하세요.
  - 등록을 위한 비밀을 생성하세요.
- 권한: 애플리케이션에 권한을 할당합니다.

- 인증: 애플리케이션에 대한 인증 자격 증명을 입력하세요.

Microsoft Sentinel을 활성화하는 단계

1. Microsoft Sentinel로 이동합니다.
2. *Log Analytics 작업 공간*을 만듭니다.
3. 방금 만든 Log Analytics 작업 영역을 Microsoft Sentinel에서 사용할 수 있도록 설정합니다.

Microsoft Sentinel에서 사용자 지정 역할을 만드는 단계

1. Microsoft Sentinel로 이동합니다.
2. 구독 > *액세스 제어(IAM)*를 선택합니다.
3. 사용자 지정 역할 이름을 입력하세요. *랜섬웨어 복원력 센티넬 구성기*라는 이름을 사용하세요.
4. 다음 JSON을 복사하여 **JSON** 탭에 붙여넣습니다.

```
{
  "roleName": "Ransomware Resilience Sentinel Configurator",
  "description": "",
  "assignableScopes":["/subscriptions/{subscription_id}"],
  "permissions": [

  ]
}
```

5. 설정을 검토하고 저장합니다.

Microsoft Sentinel에서 이벤트를 수신하기 위해 랜섬웨어 복원력을 등록하는 단계

1. Microsoft Sentinel로 이동합니다.
2. **Entra ID** > 애플리케이션 > *앱 등록*을 선택하세요.
3. 애플리케이션의 표시 이름*에 "*랜섬웨어 복원력"을 입력합니다.
4. 지원되는 계정 유형 필드에서 *이 조직 디렉토리의 계정만*을 선택합니다.
5. 이벤트가 푸시될 *기본 인덱스*를 선택하세요.
6. *리뷰*를 선택하세요.
7. *등록*을 선택하여 설정을 저장하세요.

   등록 후 Microsoft Entra 관리 센터에 애플리케이션 개요 창이 표시됩니다.

등록을 위한 비밀을 만드는 단계

1. Microsoft Sentinel로 이동합니다.
2. 인증서 및 비밀번호 > 클라이언트 비밀번호 > *새 클라이언트 비밀번호*를 선택합니다.
3. 애플리케이션 비밀번호에 대한 설명을 추가하세요.
4. 비밀에 대한 *만료*를 선택하거나 사용자 지정 수명을 지정합니다.

클라이언트 비밀번호의 수명은 2년(24개월) 이하로 제한됩니다. Microsoft에서는 만료 값을 12개월 미만으로 설정할 것을 권장합니다.

5. *추가*를 선택하여 비밀번호를 생성하세요.
6. 인증 단계에서 사용할 비밀번호를 기록합니다. 이 페이지를 벗어나면 비밀은 다시 표시되지 않습니다.

애플리케이션에 권한을 할당하는 단계

1. Microsoft Sentinel로 이동합니다.
2. 구독 > *액세스 제어(IAM)*를 선택합니다.
3. 추가 > *역할 할당 추가*를 선택합니다.
4. 권한 있는 관리자 역할 필드에서 *랜섬웨어 복원력 센티넬 구성기*를 선택합니다.

이는 이전에 만든 사용자 정의 역할입니다.

5. *다음*을 선택하세요.
6. 액세스 권한 할당 필드에서 *사용자, 그룹 또는 서비스 주체*를 선택합니다.
7. *멤버 선택*을 선택하세요. 그런 다음 *랜섬웨어 복원력 센티넬 구성기*를 선택하세요.
8. *다음*을 선택하세요.
9. 사용자가 할 수 있는 일 필드에서 *권한 있는 관리자 역할인 소유자, UAA, RBAC(권장)를 제외한 모든 역할을 사용자에게 할당하도록 허용*을 선택합니다.
10. *다음*을 선택하세요.
11. 권한을 할당하려면 *검토 및 할당*을 선택하세요.

애플리케이션에 대한 인증 자격 증명을 입력하는 단계

1. Microsoft Sentinel로 이동합니다.
2. 자격 증명을 입력하세요:
   a. 테넌트 ID, 클라이언트 애플리케이션 ID, 클라이언트 애플리케이션 비밀번호를 입력하세요.
   b. *인증*을 클릭하세요.

인증이 성공하면 "인증됨" 메시지가 나타납니다.

3. 애플리케이션에 대한 Log Analytics 작업 공간 세부 정보를 입력합니다.
   a. 구독 ID, 리소스 그룹 및 Log Analytics 작업 영역을 선택합니다.

위협 탐지를 위해 **Splunk Cloud** 구성

랜섬웨어 복원력에서 Splunk Cloud를 활성화하기 전에 Splunk Cloud에서 다음과 같은 고급 단계를 수행해야 합니다.

- Splunk Cloud에서 HTTP 이벤트 수집기를 활성화하여 콘솔에서 HTTP 또는 HTTPS를 통해 이벤트 데이터를 수신합니다.
- Splunk Cloud에서 이벤트 수집기 토큰을 만듭니다.

Splunk에서 **HTTP** 이벤트 수집기를 활성화하는 단계

1. Splunk Cloud로 이동하세요.
2. 설정 > *데이터 입력*을 선택하세요.
3. **HTTP** 이벤트 수집기 > *전역 설정*을 선택합니다.
4. 모든 토큰 토글에서 *활성화*를 선택합니다.
5. 이벤트 수집기가 HTTP가 아닌 HTTPS를 통해 수신하고 통신하도록 하려면 *SSL 사용*을 선택합니다.
6. HTTP 이벤트 수집기의 *HTTP 포트 번호*에 포트를 입력하세요.

Splunk에서 이벤트 수집기 토큰을 만드는 단계

1. Splunk Cloud로 이동하세요.
2. 설정 > *데이터 추가*를 선택하세요.
3. 모니터 > *HTTP 이벤트 수집기*를 선택합니다.
4. 토큰의 이름을 입력하고 *다음*을 선택합니다.
5. 이벤트가 푸시될 *기본 인덱스*를 선택한 다음 *검토*를 선택합니다.
6. 모든 엔드포인트 설정이 올바른지 확인한 후 *제출*을 선택합니다.
7. 토큰을 복사하여 다른 문서에 붙여넣어 인증 단계에 대비하세요.

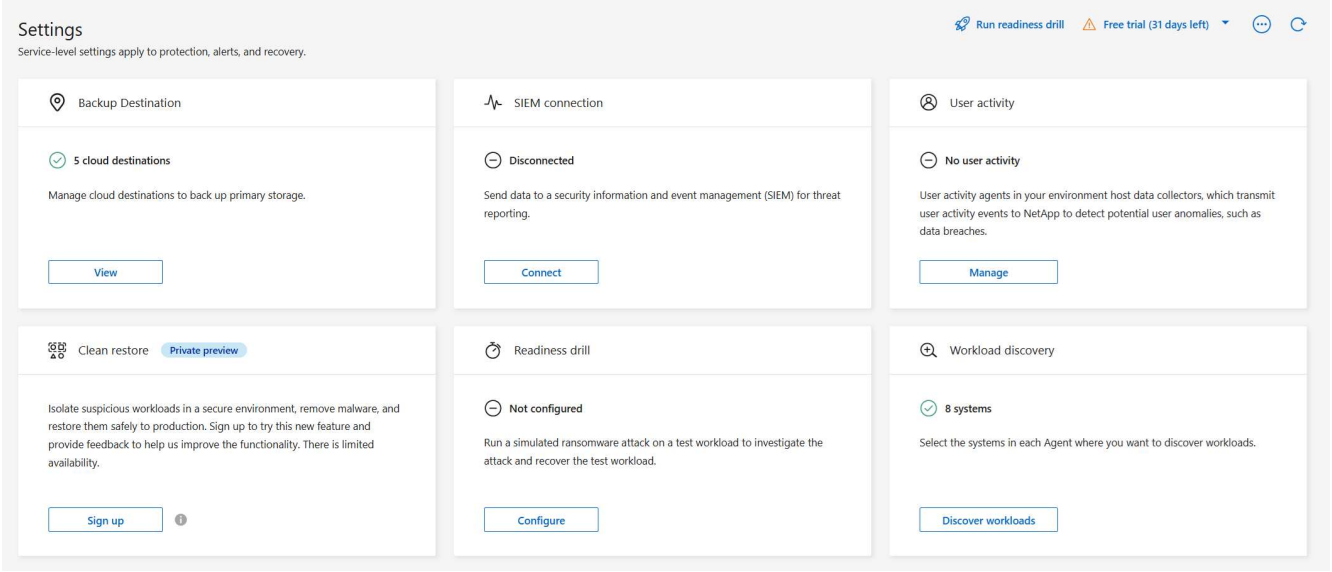
랜섬웨어 복원력에 **SIEM** 연결

SIEM을 활성화하면 랜섬웨어 복원력 데이터가 SIEM 서버로 전송되어 위협 분석 및 보고가 가능합니다.

단계

1. 콘솔 메뉴에서 보호 > *랜섬웨어 복원력*을 선택합니다.
2. 랜섬웨어 복원력 메뉴에서 세로를 선택하세요.  … 오른쪽 상단의 옵션.
3. *설정*을 선택하세요.

   설정 페이지가 나타납니다.



4. 설정 페이지에서 SIEM 연결 타일의 *연결*을 선택합니다.

5. SIEM 시스템 중 하나를 선택하세요.
6. AWS Security Hub 또는 Splunk Cloud에서 구성한 토큰 및 인증 세부 정보를 입력합니다.

   입력하는 정보는 선택한 SIEM에 따라 달라집니다.

7. *활성화*를 선택하세요.

   설정 페이지에 "연결됨"이 표시됩니다.

NetApp Ransomware Resilience 에서 의심스러운 사용자 활동 감지 구성

랜섬웨어 복원력은 탐지 정책에서 의심스러운 사용자 행동을 탐지하도록 지원하여 사용자 수준에서 랜섬웨어 사고를 해결할 수 있도록 합니다.

랜섬웨어 복원력은 ONTAP 의 FPolicy가 생성한 사용자 활동 이벤트를 분석하여 의심스러운 사용자 활동을 감지합니다. 사용자 활동 데이터를 수집하려면 하나 이상의 사용자 활동 에이전트를 배포해야 합니다. 에이전트는 테넌트의 장치에 연결할 수 있는 Linux 서버 또는 VM입니다.

에이전트와 수집가

Ransomware Resilience에서 의심스러운 사용자 활동 감지를 활성화하려면 최소 하나 이상의 사용자 활동 에이전트를 설치해야 합니다. 랜섬웨어 복원력 대시보드에서 의심스러운 사용자 활동 기능을 활성화하는 경우, 해당 기능을 활성화하려면 에이전트 호스트 정보를 제공해야 합니다.

에이전트는 여러 개의 데이터 수집기를 호스팅할 수 있습니다. 데이터 수집자는 분석을 위해 SaaS 위치로 데이터를 보냅니다. 수집가에는 두 가지 유형이 있습니다.

- 데이터 수집기는 ONTAP 에서 사용자 활동 데이터를 수집합니다.
- 사용자 디렉토리 커넥터는 디렉토리에 연결하여 사용자 ID를 사용자 이름에 매핑합니다.

수집기는 랜섬웨어 복원력 설정에서 구성됩니다.

의심스러운 사용자 활동 감지 활성화

필수 콘솔 역할 의심스러운 사용자 활동 감지를 활성화하려면 조직 관리자 역할이 필요합니다. 의심스러운 사용자 활동에 대한 후속 구성을 위해서는 랜섬웨어 복원력 사용자 동작 관리자 역할이 필요합니다. "NetApp Console 의 랜섬웨어 복원력 역할에 대해 알아보세요".

사용자 활동 에이전트 추가

사용자 활동 에이전트는 데이터 수집기를 위한 실행 가능한 환경이며, 데이터 수집기는 Ransomware Resilience와 사용자 활동 이벤트를 공유합니다. 의심스러운 사용자 활동을 감지하려면 최소한 하나의 사용자 활동 에이전트를 만들어야 합니다.

요구 사항

사용자 활동 에이전트를 설치하려면 다음 지원되는 운영 체제 및 서버 요구 사항을 충족하는 호스트 또는 VM이 필요합니다.

운영 체제 요구 사항

운영 체제	지원되는 버전
알마리눅스	9.4(64비트) ~ 9.5(64비트) 및 10(64비트), SELinux 포함
센트OS	CentOS Stream 9(64비트)
데비안	11(64비트), 12(64비트), SELinux 포함
오픈수세 리프	15.3(64비트) ~ 15.6(64비트)
오라클 리눅스	8.10(64비트) 및 9.1(64비트) ~ 9.6(64비트), SELinux 포함
레드햇	8.10(64비트), 9.1(64비트) ~ 9.6(64비트), 10(64비트), SELinux 포함
불안정한	SELinux를 포함한 Rocky 9.4(64비트)부터 9.6(64비트)까지

수세 엔터프라이즈 리눅스	15 SP4(64비트)부터 15 SP6(64비트), SELinux 포함
우분투	20.04 LTS(64비트), 22.04 LTS(64비트) 및 24.04 LTS(64비트)

서버 요구 사항

서버는 다음과 같은 최소 요구 사항을 충족해야 합니다.

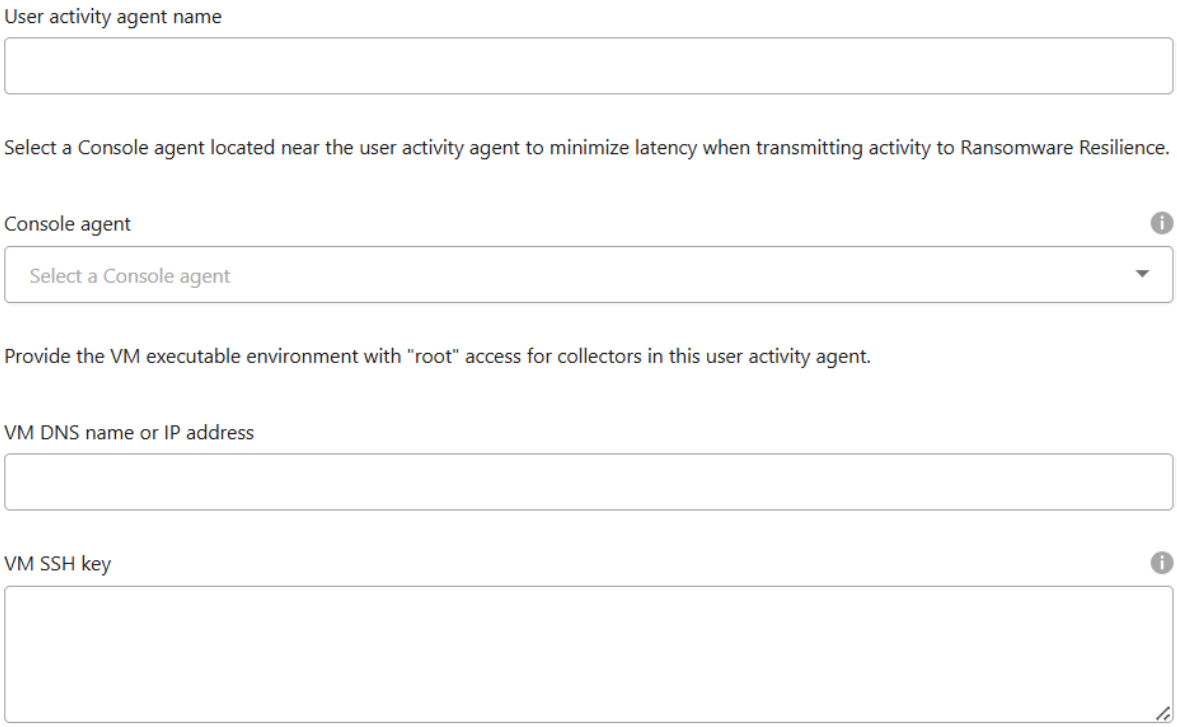
- **CPU**: 4코어
- **RAM**: 16GB RAM
- 디스크 공간: 35GB의 여유 디스크 공간

단계

1. 처음으로 사용자 활동 에이전트를 만드는 경우 대시보드로 이동하세요. 사용자 활동 타일에서 활성화를 선택합니다.

   추가 사용자 활동 에이전트를 추가하는 경우 *설정*으로 이동하여 사용자 활동 타일을 찾은 다음 관리를 선택합니다. 사용자 활동 화면에서 사용자 활동 에이전트 탭을 선택한 다음 추가를 선택합니다.

2. 클라우드 공급자를 선택한 다음 지역을 선택하세요. 다음을 선택하세요.
3. 사용자 활동 에이전트 세부 정보를 제공하세요.
   - 사용자 활동 에이전트 이름
   - 콘솔 에이전트 - 콘솔 에이전트는 사용자 활동 에이전트와 동일한 네트워크에 있어야 하며 사용자 활동 에이전트 IP 주소에 대한 SSH 연결이 있어야 합니다.
   - **VM DNS** 이름 또는 **IP** 주소
   - **VM SSH** 키



4. 다음을 선택하세요.
5. 설정을 검토하세요. *활성화*를 선택하여 사용자 활동 에이전트 추가를 완료합니다.
6. 사용자 활동 에이전트가 성공적으로 생성되었는지 확인하세요. 사용자 활동 타일에서 배포가 성공하면 '실행 중'으로 표시됩니다.

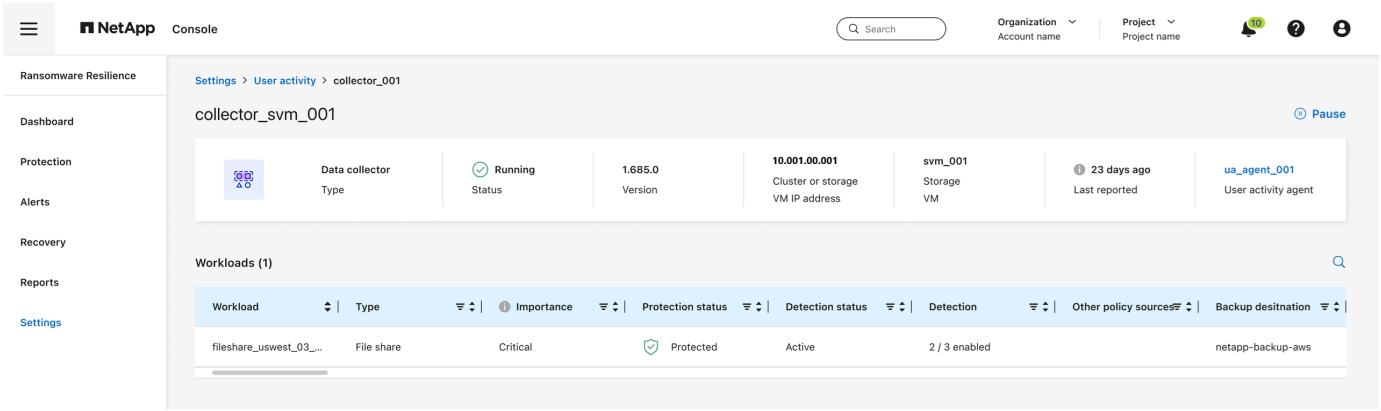
결과

사용자 활동 에이전트가 성공적으로 생성되면 설정 메뉴로 돌아간 다음 사용자 활동 타일에서 관리를 선택합니다. 사용자 활동 에이전트 탭을 선택한 다음 사용자 활동 에이전트를 선택하여 데이터 수집기 및 사용자 디렉터리 커넥터를 포함한 해당 에이전트에 대한 세부 정보를 확인합니다.

데이터 수집기 추가

의심스러운 사용자 활동 감지를 통해 랜섬웨어 보호 전략을 활성화하면 데이터 수집기가 자동으로 생성됩니다. 자세한 내용은 다음을 참조하세요. 탐지 정책 추가.

데이터 수집기의 세부 정보를 볼 수 있습니다. 설정에서 사용자 활동 타일의 관리를 선택합니다. 데이터 수집기 탭을 선택한 다음 데이터 수집기를 선택하여 세부 정보를 보거나 일시 중지합니다.

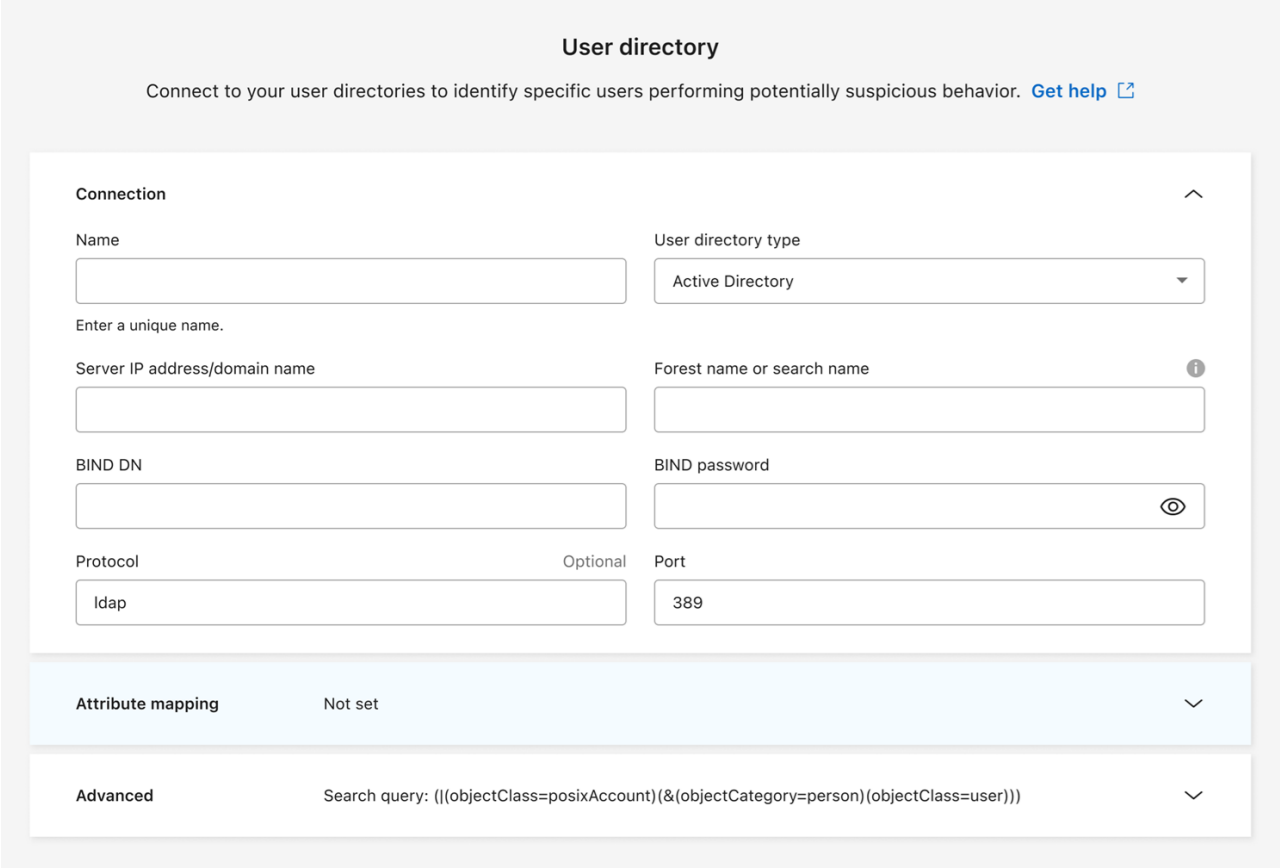


사용자 디렉토리 커넥터 추가

사용자 ID를 사용자 이름에 매핑하려면 사용자 디렉토리 커넥터를 만들어야 합니다.

단계

1. 랜섬웨어 복원력에서 *설정*으로 이동합니다.
2. 사용자 활동 타일에서 관리를 선택합니다.
3. 사용자 디렉터리 커넥터 탭을 선택한 다음 추가를 선택합니다.
4. 연결에 대한 세부 정보를 제공하세요.
    - 이름
    - 사용자 디렉토리 유형
    - 서버 **IP** 주소 또는 도메인 이름
    - 산림명 또는 검색명
    - **BIND** 도메인 이름
    - **BIND** 비밀번호
    - 프로토콜 (선택 사항입니다)
    - 포트



속성 매핑 세부 정보를 제공하세요.

- 표시 이름
- **SID** (LDAP를 사용하는 경우)
- 사용자 이름
- **Unix ID** (NFS를 사용하는 경우)
- *선택적 속성 포함*을 선택하세요. 이메일 주소, 전화번호, 역할, 주, 국가, 부서, 사진, 관리자 DN 또는 그룹을 포함할 수도 있습니다.

  *고급*을 선택하여 선택적 검색어를 추가하세요.

5. 추가를 선택합니다.
6. 사용자 디렉토리 커넥터 탭으로 돌아가서 사용자 디렉토리 커넥터의 상태를 확인하세요. 성공적으로 생성되면 사용자 디렉토리 커넥터의 상태가 *실행 중*으로 표시됩니다.

사용자 디렉토리 커넥터 삭제

1. 랜섬웨어 복원력에서 *설정*으로 이동합니다.
2. 사용자 활동 타일을 찾아 관리를 선택합니다.
3. 사용자 디렉토리 커넥터 탭을 선택합니다.
4. 삭제하려는 사용자 디렉토리 커넥터를 식별합니다. 줄 끝의 작업 메뉴에서 세 개의 점을 선택하세요. ... 그런 다음 삭제를 클릭합니다.

5. 팝업 대화 상자에서 삭제를 선택하여 작업을 확인합니다.

의심스러운 사용자 활동 알림에 대응

의심스러운 사용자 활동 감지를 구성한 후 알림 페이지에서 이벤트를 모니터링할 수 있습니다. 자세한 내용은 다음을 참조하세요. "악성 활동 및 비정상적인 사용자 동작 감지" .

랜섬웨어 복원력 활용

NetApp Ransomware Resilience 사용

NetApp Ransomware Resilience 사용하면 워크로드 상태를 확인하고 워크로드를 보호할 수 있습니다.

- "랜섬웨어 복원력에서 워크로드를 발견하세요" .
- "대시보드에서 보호 및 작업 부하 상태 확인" .
  - 랜섬웨어 보호 권장 사항을 검토하고 조치를 취하세요.
- "작업 부하 보호":
  - 워크로드에 랜섬웨어 보호 전략을 할당합니다.
  - 향후 랜섬웨어 공격을 방지하기 위해 애플리케이션 보호를 강화하세요.
  - 보호 전략을 생성, 변경 또는 삭제합니다.
- "잠재적인 랜섬웨어 공격 감지에 대응" .
- "공격으로부터 복구"(사건이 중립화된 후).
- "보호 설정 구성" .

NetAPp 랜섬웨어 복원력 대시보드를 사용하여 워크로드 상태 모니터링

NetApp Ransomware Resilience 보드는 워크로드의 보호 상태에 대한 정보를 한눈에 볼 수 있도록 제공합니다. 위험에 처해 있거나 보호되는 워크로드를 빠르게 파악하고, 사고로 인해 영향을 받거나 복구 중인 워크로드를 식별하고, 보호되거나 위험에 처한 스토리지의 양을 살펴보면서 보호 범위를 측정할 수 있습니다.

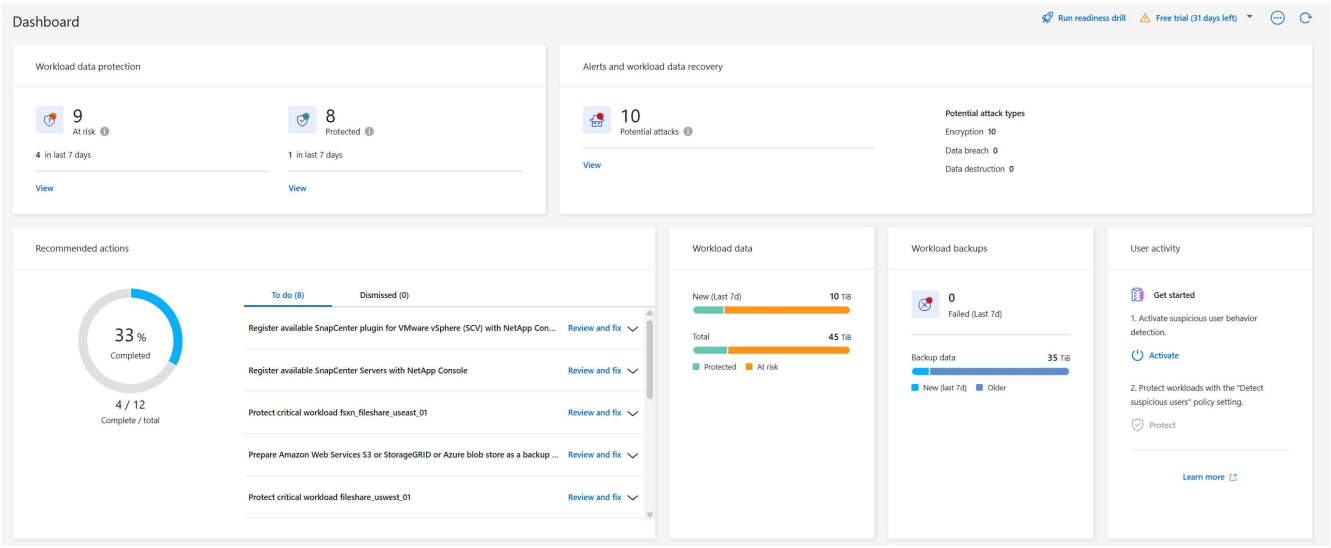
대시보드를 사용하여 보호 제안을 검토하고, 설정을 변경하고, 보고서를 다운로드하고, 문서를 확인하세요.

필수 콘솔 역할 이 작업을 수행하려면 조직 관리자, 폴더 또는 프로젝트 관리자, 랜섬웨어 복원력 관리자 또는 랜섬웨어 복원력 뷰어 역할이 필요합니다. "NetApp Console 의 랜섬웨어 복원력 역할에 대해 알아보세요" .

대시보드를 사용하여 작업 부하 상태 검토

단계

1. 콘솔이 워크로드를 검색한 후 랜섬웨어 복원력 대시보드에 워크로드 데이터 보호 상태가 표시됩니다.



2. 대시보드의 각 창에서 다음 작업을 수행할 수 있습니다.

   - 워크로드 데이터 보호: *모두 보기*를 선택하면 보호 페이지에서 위험에 처해 있거나 보호되는 모든 워크로드를 볼 수 있습니다. 보호 수준이 보호 정책과 일치하지 않으면 작업 부하가 위험에 처하게 됩니다. "작업 부하 보호" .

     이 데이터에 대한 팁을 보려면 "i" 도구 설명을 선택하세요. 작업 부하 한도를 늘리려면 이 i 노트에서 *작업 부하 한도 늘리기*를 선택하세요. 이 옵션을 선택하면 케이스 티켓을 생성할 수 있는 콘솔 지원 페이지로 이동합니다.

   - 알림 및 워크로드 데이터 복구: 워크로드에 영향을 준 활성 인시던트, 인시던트가 무력화된 후 복구 준비가 된 인시던트 또는 복구 중인 인시던트를 보려면 *모두 보기*를 선택하세요. "감지된 경고에 대응" .
     - 사건은 다음 상태 중 하나로 분류됩니다.
       - 새로운
       - 해고됨
       - 해고하다
       - 해결됨
     - 알림은 다음 상태 중 하나를 가질 수 있습니다.
       - 새로운
       - 비활성
     - 작업 부하에는 다음 복원 상태 중 하나가 있을 수 있습니다.
       - 복원이 필요합니다
       - 진행 중
       - 복원됨
       - 실패한
   - 권장 작업: 보호 수준을 높이려면 각 권장 사항을 검토한 다음 *검토 및 수정*을 선택하세요.

     보다 "대시보드에서 보호 제안 검토" 또는 "작업 부하 보호" .

랜섬웨어 복원력은 대시보드를 마지막으로 방문한 이후 24시간 동안 "신규" 태그와 함께 새로운 권장 사항을 표시합니다. 작업은 우선순위 순서대로 표시되며, 가장 중요한 작업이 맨 위에 표시됩니다. 각 권장 사항을 검토하고, 조치를 취하거나, 기각합니다.

총 작업 수에는 취소한 작업이 포함되지 않습니다.

- 작업량 데이터: 지난 7일 동안 보호 범위의 변화를 모니터링합니다.
- 워크로드 백업: 지난 7일 동안 Ransomware Resilience에서 생성한 워크로드 백업 중 실패하거나 성공적으로 완료된 백업의 변경 사항을 모니터링합니다.

대시보드에서 보호 권장 사항 검토

랜섬웨어 복원력은 워크로드에 대한 보호 수준을 평가하고 해당 보호 수준을 개선하기 위한 조치를 권장합니다.

권장 사항을 검토하고 조치를 취하면 권장 사항 상태가 완료로 변경됩니다. 나중에 조치를 취하고 싶다면 해당 조치를 취소할 수 있습니다. 작업을 취소하면 권장 사항이 취소된 작업 목록으로 이동되며, 나중에 검토할 수 있습니다.

Ransomware Resilience에서 제공하는 권장 사항의 샘플은 다음과 같습니다.

추천	설명	해결 방법
랜섬웨어 보호 정책을 추가합니다.	현재 작업 부하가 보호되지 않습니다.	작업 부하에 정책을 할당합니다. "랜섬웨어 공격으로부터 워크로드 보호" .
위협 보고를 위해 SIEM에 연결합니다.	위협 분석 및 감지를 위해 보안 및 이벤트 관리 시스템(SIEM)으로 데이터를 보냅니다.	위협 탐지를 활성화하려면 SIEM/XDR 서버 세부 정보를 입력하세요. "보호 설정 구성" .
애플리케이션이나 VMware에 대한 워크로드 일관성 보호를 활성화합니다.	이러한 작업 부하는 SnapCenter 소프트웨어나 SnapCenter Plug-in for VMware vSphere 으로 관리되지 않습니다.	SnapCenter 에서 관리하려면 작업 부하에 맞는 보호를 활성화하세요. "랜섬웨어 공격으로부터 작업 부하를 보호하세요" .
시스템의 보안 태세 개선	NetApp Digital Advisor 하나 이상의 높거나 심각한 보안 위험을 확인했습니다.	NetApp Digital Advisor 의 모든 보안 위험을 검토하세요. 참조하다 "Digital Advisor 문서" .
정책을 더욱 강화하세요.	일부 작업에는 충분한 보호가 없을 수 있습니다. 정책을 통해 작업 부하에 대한 보호를 강화하세요.	보존 기간을 늘리고, 백업을 추가하고, 변경할 수 없는 백업을 시행하고, 의심스러운 파일 확장자를 차단하고, 보조 저장소에서 감지 기능을 활성화하는 등의 작업이 가능합니다. "랜섬웨어 공격으로부터 워크로드 보호" .
워크로드 데이터를 백업하기 위해 <백업 공급자>를 백업 대상으로 준비합니다.	현재 작업 부하에 백업 대상이 없습니다.	이 작업 부하에 백업 대상을 추가하여 보호하세요. "보호 설정 구성" .
랜섬웨어로부터 중요하거나 매우 중요한 애플리케이션 워크로드를 보호하세요.	보호 페이지에는 보호되지 않은 중요 또는 매우 중요(할당된 우선순위 수준에 따라) 애플리케이션 워크로드가 표시됩니다.	이러한 작업 부하에 정책을 할당합니다. "랜섬웨어 공격으로부터 워크로드 보호" .

추천	설명	해결 방법
랜섬웨어로부터 중요하거나 매우 중요한 파일 공유 워크로드를 보호하세요.	보호 페이지에는 보호되지 않는 파일 공유 또는 데이터 저장소 유형의 중요하거나 매우 중요한 워크로드가 표시됩니다.	각 작업 부하에 정책을 할당합니다. "랜섬웨어 공격으로부터 워크로드 보호" .
콘솔을 사용하여 VMware vSphere(SCV)에 사용 가능한 SnapCenter 플러그인을 등록합니다.	VM 작업 부하가 보호되지 않습니다.	VMware vSphere용 SnapCenter 플러그인을 활성화하여 VM 워크로드에 VM 일관성 보호 기능을 할당합니다. "랜섬웨어 공격으로부터 워크로드 보호" .
콘솔에 사용 가능한 SnapCenter 서버 등록	애플리케이션이 보호되지 않았습니다.	SnapCenter Server를 활성화하여 워크로드에 애플리케이션 일관성 보호 기능을 할당합니다. "랜섬웨어 공격으로부터 워크로드 보호" .
새로운 알림을 확인하세요.	새로운 알림이 있습니다.	새로운 알림을 검토하세요. "감지된 랜섬웨어 경고에 대응하세요" .

단계

1. 랜섬웨어 복원력의 권장 작업 창에서 권장 사항을 선택한 다음 *검토 및 수정*을 선택합니다.
2. 작업을 나중에 취소하려면 *취소*를 선택하세요.

   해당 권장 사항이 할 일 목록에서 지워지고 취소 목록에 나타납니다.

   나중에 해제된 항목을 할 일 항목으로 변경할 수 있습니다. 항목을 완료로 표시하거나 취소된 항목을 할 일 작업으로 변경하면 총 작업 수가 1씩 증가합니다.

3. 권장 사항에 따라 조치를 취하는 방법에 대한 정보를 검토하려면 정보 아이콘을 선택하세요.

보호 데이터를 CSV 파일로 내보내기

보호, 알림 및 복구에 대한 세부 정보를 보여주는 CSV 파일을 다운로드하고 데이터를 내보낼 수 있습니다.

다음 메인 메뉴 옵션에서 CSV 파일을 다운로드할 수 있습니다.

- 보호: 랜섬웨어 복원력이 보호됨 또는 위험으로 표시한 워크로드의 총 수를 포함하여 모든 워크로드의 상태와 세부 정보가 포함됩니다.
- 알림: 모든 알림의 상태와 세부 정보, 총 알림 수 및 자동 스냅샷이 포함됩니다.
- 복구: 랜섬웨어 복원력에서 "복원 필요", "진행 중", "복원 실패", "복원 성공"으로 표시한 총 워크로드 수를 포함하여 복원이 필요한 모든 워크로드의 상태와 세부 정보가 포함됩니다.

페이지에서 CSV 파일을 다운로드하면 해당 페이지의 데이터만 포함됩니다.

CSV 파일에는 모든 콘솔 시스템의 모든 워크로드에 대한 데이터가 포함되어 있습니다.

단계

1. 랜섬웨어 복원력 대시보드에서 *새로 고침*을 선택하세요. 파일에 표시될 데이터를 새로 고치려면 오른쪽 상단의 옵션을 선택하세요.

2. 다음 중 하나를 수행하세요.
   - 해당 페이지에서 *다운로드*를 선택하세요  옵션.
   - 랜섬웨어 복원력 메뉴에서 *보고서*를 선택합니다.
3. 보고서 옵션을 선택한 경우 미리 구성된 이름이 지정된 파일 중 하나를 선택한 다음 다운로드**(CSV)** 또는 * 다운로드(JSON)*를 선택합니다.

기술 문서에 액세스

Ransomware Resilience 기술 문서는 다음에서 볼 수 있습니다."docs.netapp.com" 또는 랜섬웨어 복원력 내부에서.

단계

1. 랜섬웨어 복원력 대시보드에서 세로 *작업*을 선택하세요.  옵션.
2. 다음 옵션 중 하나를 선택하세요.
   - *새로운 기능*을 클릭하면 릴리스 노트에서 현재 또는 이전 릴리스의 기능에 대한 정보를 볼 수 있습니다.
   - 문서 랜섬웨어 복원력 설명서 홈페이지와 이 설명서를 확인하세요.

작업 부하 보호

NetApp Ransomware Resilience 보호 전략으로 워크로드를 보호하세요

NetApp Ransomware Resilience 에서 워크로드 일관성 보호를 활성화하거나 랜섬웨어 보호 전략을 생성하여 워크로드를 랜섬웨어 공격으로부터 보호할 수 있습니다.

필수 콘솔 역할 이 작업을 수행하려면 조직 관리자, 폴더 또는 프로젝트 관리자, 랜섬웨어 복원력 관리자 역할이 필요합니다. "NetApp Console 의 랜섬웨어 복원력 역할에 대해 알아보세요" .

랜섬웨어 보호 전략 이해

랜섬웨어 보호 전략에는 탐지 정책과 보호 정책이 모두 포함됩니다.

- 탐지 정책 랜섬웨어 위협을 탐지합니다.
- 보호 정책에는 스냅샷 및 백업 정책이 포함됩니다. 보호 전략에는 탐지 및 스냅샷 정책이 필요합니다. 백업 정책은 선택 사항입니다.

  다른 NetApp 제품을 사용하여 작업 부하를 보호하는 경우 Ransomware Resilience는 해당 제품을 검색하여 다음 옵션 중 하나를 제공합니다.
  - 랜섬웨어 탐지 정책을 사용하고 다른 NetApp 도구에서 만든 스냅샷 및 백업 정책을 계속 사용하거나
  - 랜섬웨어 복원력을 사용하여 탐지, 스냅샷, 백업을 관리합니다.

데이터 자산의 관리 및 보호를 강화하려면 다음을 생성할 수 있습니다."그룹 파일 공유" 하나의 전략으로 여러 볼륨을 공동으로 보호합니다.

다른 NetApp 관리 서비스와의 보호 정책

랜섬웨어 회복력 외에도 다음 서비스를 사용하여 보호 기능을 관리할 수 있습니다.

- 파일 공유, VM 파일 공유를 위한 NetApp Backup and Recovery
- VM 데이터 저장소를 위한 VMware용 SnapCenter
- Oracle 및 MySQL용 SnapCenter

이러한 서비스의 보호 정보는 랜섬웨어 복원력에 나타납니다. 랜섬웨어 복원력을 사용하면 이러한 서비스에 탐지 정책을 추가할 수 있습니다. 랜섬웨어 복원력을 갖춘 보호 정책을 추가하면 기존 보호 정책이 대체됩니다.

랜섬웨어 탐지 정책이 ONTAP 버전에 따라 ARP 또는 ARP/AI(Autonomous Ransomware Protection)와 ONTAP 의 FPolicy에 의해 관리되는 경우 해당 작업 부하가 보호되고 ARP와 FPolicy에 의해 계속 관리됩니다.

> Amazon FSx for NetApp ONTAP 의 워크로드에는 백업 대상을 사용할 수 없습니다. FSx for ONTAP 백업 서비스를 사용하여 백업 작업을 수행합니다. AWS의 FSx for ONTAP 에서 워크로드에 대한 백업 정책을 설정하는 반면, Ransomware Resilience에서는 그렇지 않습니다. 백업 정책은 Ransomware Resilience에 나타나며 AWS와 동일하게 유지됩니다.

NetApp 애플리케이션으로 보호되지 않는 워크로드에 대한 보호 정책

워크로드가 백업 및 복구, 랜섬웨어 복원력, SnapCenter 또는 SnapCenter Plug-in for VMware vSphere 으로 관리되지 않는 경우 ONTAP 또는 다른 제품의 일부로 스냅샷이 생성되었을 수 있습니다. ONTAP FPolicy 보호가 적용된 경우 ONTAP 사용하여 FPolicy 보호를 변경할 수 있습니다.

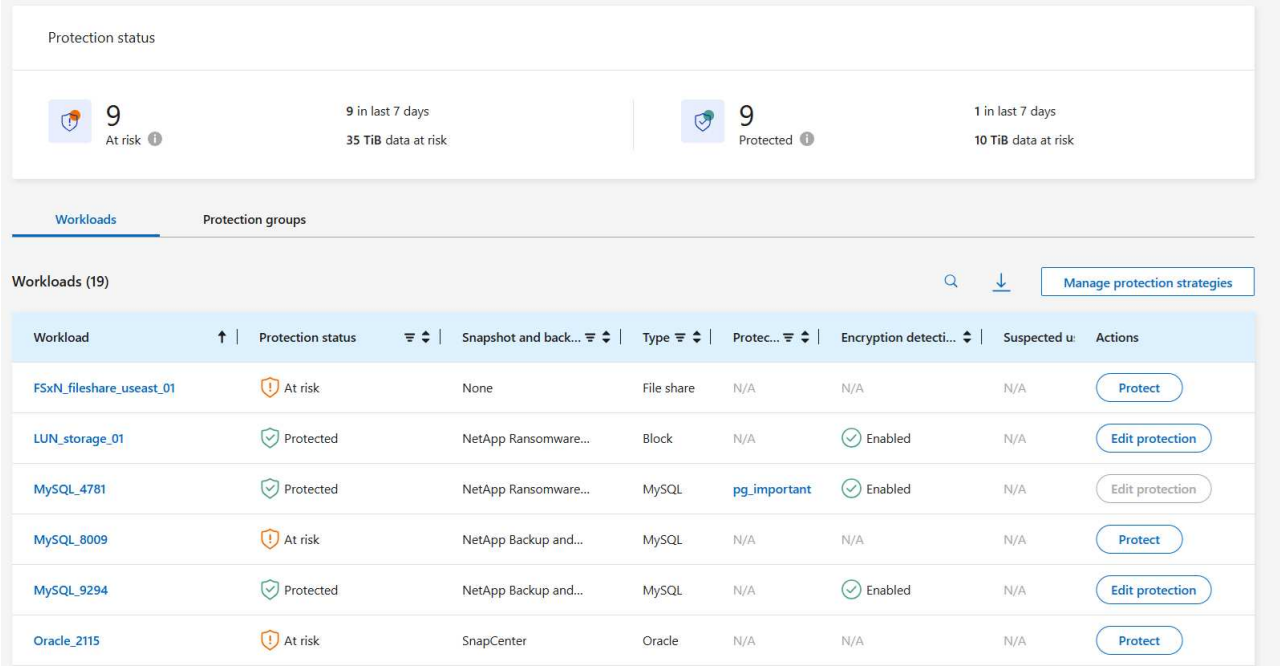
워크로드에서 랜섬웨어 보호 보기

워크로드를 보호하기 위한 첫 번째 단계 중 하나는 현재 워크로드와 해당 보호 상태를 확인하는 것입니다. 다음 유형의 작업 부하를 볼 수 있습니다.

- 애플리케이션 워크로드
- 블록 워크로드
- 파일 공유 워크로드
- VM 워크로드

단계

1. 콘솔 왼쪽 탐색에서 보호 > *랜섬웨어 복원력*을 선택합니다.
2. 다음 중 하나를 수행하세요.
    - 대시보드의 데이터 보호 창에서 *모두 보기*를 선택합니다.
    - 메뉴에서 *보호*를 선택하세요.



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

보다"랜섬웨어 보호 전략 추가" SnapCenter 또는 백업 및 복구에 기존 보호 정책이 있는 경우 랜섬웨어 복원력을 사용하는 방법에 대해 알아보세요.

보호 페이지 이해

보호 페이지에는 워크로드 보호에 대한 다음 정보가 표시됩니다.

보호 상태: 워크로드는 정책이 적용되는지 여부를 나타내기 위해 다음 보호 상태 중 하나를 표시할 수 있습니다.

- 보호됨: 정책이 적용됩니다. 모든 작업 부하 관련 볼륨에서 ARP(또는 ONTAP 버전에 따라 ARP/AI)가 활성화됩니다.
- 위험: 정책이 적용되지 않습니다. 워크로드에 기본 감지 정책이 활성화되어 있지 않으면 스냅샷 및 백업 정책이 활성화되어 있어도 "위험에 처해 있습니다".
- 진행 중: 정책이 적용 중이지만 아직 완료되지 않았습니다.
- 실패: 정책이 적용되었지만 작동하지 않습니다.

탐지 상태: 워크로드는 다음 랜섬웨어 탐지 상태 중 하나를 가질 수 있습니다.

- 학습: 랜섬웨어 탐지 정책이 최근 워크로드에 할당되었으며 Ransomware Resilience가 워크로드를 스캔하고 있습니다.
- 활성: 랜섬웨어 탐지 보호 정책이 할당되었습니다.
- 설정되지 않음: 랜섬웨어 탐지 보호 정책이 할당되지 않았습니다.
- 오류: 랜섬웨어 탐지 정책이 할당되었지만 랜섬웨어 복원력에서 오류가 발생했습니다.

랜섬웨어 복원력에서 보호 기능이 활성화된 경우 랜섬웨어 감지 정책 상태가 학습 모드에서 활성 모드로 변경된 후 경고 감지 및 보고가 시작됩니다.

탐지 정책: 랜섬웨어 탐지 정책이 할당된 경우 해당 정책의 이름이 표시됩니다. 탐지 정책이 할당되지 않은 경우 "N/A"가 나타납니다.

스냅샷 및 백업 정책: 이 열은 워크로드에 적용된 스냅샷 및 백업 정책과 해당 정책을 관리하는 제품 또는 서비스를 보여줍니다.

- SnapCenter 에서 관리
- SnapCenter Plug-in for VMware vSphere 으로 관리됨
- 백업 및 복구로 관리됨
- 스냅샷 및 백업을 관리하는 랜섬웨어 보호 정책의 이름
- None

업무량 중요도

랜섬웨어 복원력은 각 워크로드에 대한 분석을 기반으로 검색 중에 각 워크로드에 중요도 또는 우선순위를 지정합니다. 작업 부하 중요도는 다음 스냅샷 빈도에 따라 결정됩니다.

- 중요: 시간당 1개 이상 스냅샷 복사본이 생성됨(매우 공격적인 보호 일정)
- 중요: 스냅샷 복사본은 시간당 1개 미만, 하루 1개 이상 생성됩니다.
- 표준: 하루에 1개 이상 촬영된 스냅샷 사본

사전 정의된 탐지 정책 [[사전 정의]]

워크로드 중요도에 맞춰 사전 정의된 다음 랜섬웨어 복원력 정책 중 하나를 선택할 수 있습니다.

암호화 사용자 확장 정책은 의심스러운 사용자 동작 감지를 지원하는 유일한 사전 정의된 정책입니다.

정책 수준	스냅샷	빈도	보존 기간(일)	스냅샷 복사본 수	스냅샷 복사본의 총 최대 수
중요 작업 정책	15분마다	15분마다	3	288	309
	일일	1일마다	14	14	309
	주간	1주일마다	35	5	309
	월간 간행물	30일마다	60	2	309
중요 업무 정책	15분마다	30분마다	3	144	165
	일일	1일마다	14	14	165
	주간	1주일마다	35	5	165
	월간 간행물	30일마다	60	2	165

정책 수준	스냅샷	빈도	보존 기간(일)	스냅샷 복사본 수	스냅샷 복사본의 총 최대 수
표준 작업량 정책	15분마다	30분마다	3	72	93
	일일	1일마다	14	14	93
	주간	1주일마다	35	5	93
	월간 간행물	30일마다	60	2	93
암호화 사용자 확장	15분마다	30분마다	3	72	93
	일일	1일마다	14	14	93
	주간	1주일마다	35	5	93
	월간 간행물	30일마다	60	2	93

SnapCenter 사용하여 애플리케이션 또는 **VM**과 일관된 보호 기능 활성화

애플리케이션 또는 VM 일관성 보호를 활성화하면 일관된 방식으로 애플리케이션 또는 VM 워크로드를 보호하여 나중에 복구가 필요할 경우 잠재적인 데이터 손실을 방지하기 위해 조용하고 일관된 상태를 유지할 수 있습니다.

이 프로세스는 백업 및 복구를 사용하여 애플리케이션용 SnapCenter 소프트웨어 서버 또는 VM용 SnapCenter Plug-in for VMware vSphere 등록하는 것을 시작합니다.

워크로드에 맞는 보호를 활성화한 후에는 랜섬웨어 복원력에서 보호 전략을 관리할 수 있습니다. 보호 전략에는 Ransomware Resilience에서 관리하는 랜섬웨어 탐지 정책과 함께 다른 곳에서 관리되는 스냅샷 및 백업 정책이 포함됩니다.

백업 및 복구를 사용하여 VMware vSphere용 SnapCenter 또는 SnapCenter Plug-in for VMware vSphere 등록하는 방법에 대해 알아보려면 다음 정보를 참조하세요.

- "SnapCenter 서버 소프트웨어 등록"
- "SnapCenter Plug-in for VMware vSphere 등록"

단계

1. 랜섬웨어 복원력 메뉴에서 *대시보드*를 선택합니다.
2. 권장 사항 창에서 다음 권장 사항 중 하나를 찾아 *검토 및 수정*을 선택하세요.
   - NetApp Console 사용하여 사용 가능한 SnapCenter 서버 등록
   - NetApp Console 사용하여 SnapCenter Plug-in for VMware vSphere 등록합니다.
3. 백업 및 복구를 사용하여 SnapCenter 또는 SnapCenter Plug-in for VMware vSphere 등록하려면 다음 정보를 따르세요.
4. 랜섬웨어 회복력으로 돌아가기.

5. 랜섬웨어 복원력에서 대시보드로 이동하여 검색 프로세스를 다시 시작합니다.
6. 랜섬웨어 복원력에서 *보호*를 선택하여 보호 페이지를 확인하세요.
7. 보호 페이지의 스냅샷 및 백업 정책 열에서 세부 정보를 검토하여 해당 정책이 다른 곳에서 관리되는지 확인하세요.

랜섬웨어 보호 전략 추가

랜섬웨어 보호 전략을 추가하는 데는 세 가지 접근 방식이 있습니다.

- 스냅샷이나 백업 정책이 없는 경우 랜섬웨어 보호 전략을 수립하세요.

  랜섬웨어 보호 전략에는 다음이 포함됩니다.

  - 스냅샷 정책
  - 랜섬웨어 탐지 정책
  - 백업 정책

- **SnapCenter** 또는 백업 및 복구 보호의 기존 스냅샷 또는 백업 정책을 **Ransomware Resilience**가 관리하는 보호 전략으로 대체합니다.

  랜섬웨어 보호 전략에는 다음이 포함됩니다.

  - 스냅샷 정책
  - 랜섬웨어 탐지 정책
  - 백업 정책

- 다른 **NetApp** 제품이나 서비스에서 관리되는 기존 스냅샷 및 백업 정책이 있는 워크로드에 대한 감지 정책을 만듭니다.

  탐지 정책은 다른 제품에서 관리되는 정책을 변경하지 않습니다.

  탐지 정책은 다른 서비스에서 이미 활성화된 경우 Autonomous Ransomware Protection 및 FPolicy 보호를 활성화합니다. 자세히 알아보세요"자율형 랜섬웨어 보호" ,"백업 및 복구" , 그리고"ONTAP 정책" .

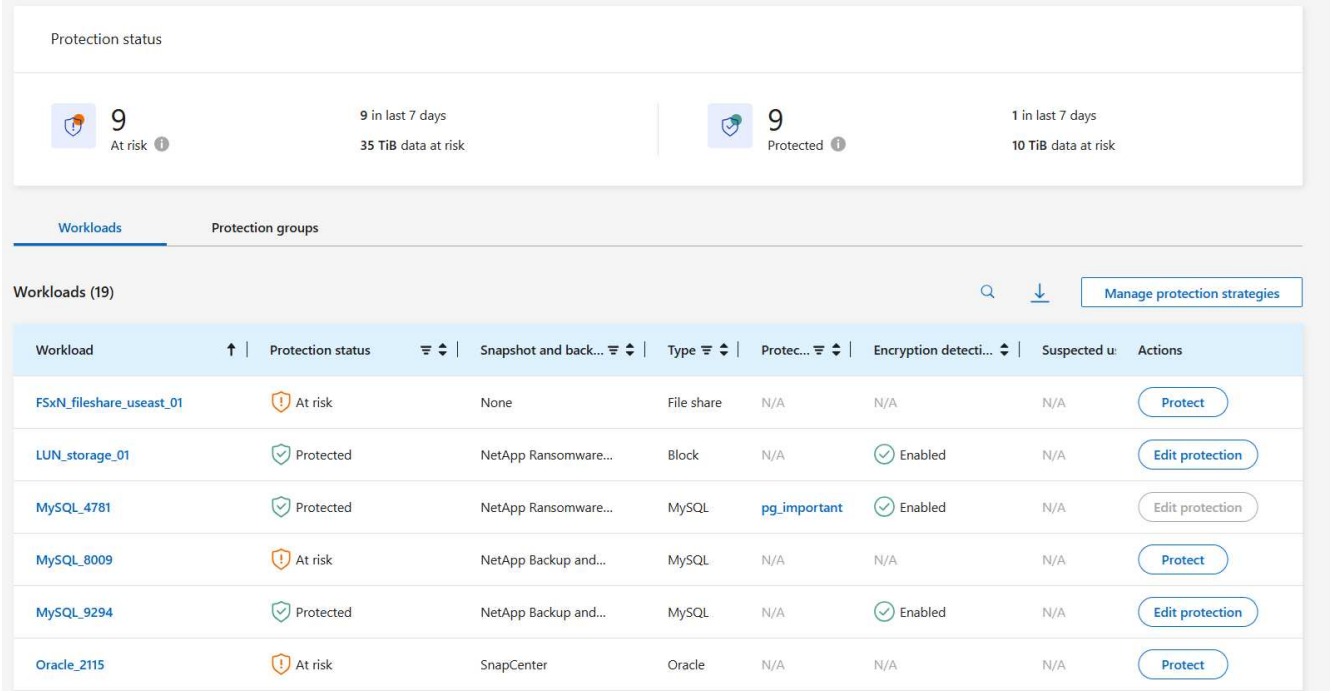
랜섬웨어 보호 전략을 수립하세요(스냅샷이나 백업 정책이 없는 경우)

워크로드에 스냅샷이나 백업 정책이 없는 경우 랜섬웨어 보호 전략을 만들 수 있습니다. 이 전략에는 Ransomware Resilience에서 만든 다음 정책이 포함될 수 있습니다.

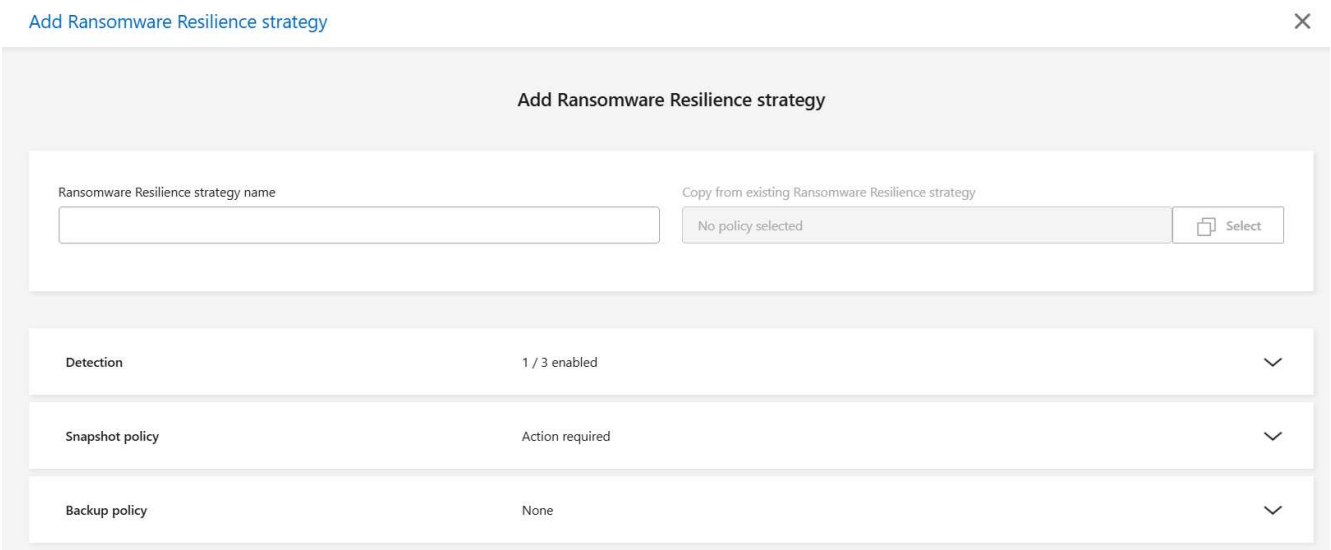
- 스냅샷 정책
- 백업 정책
- 랜섬웨어 탐지 정책

랜섬웨어 보호 전략을 만드는 단계

1. 랜섬웨어 복원력 메뉴에서 *보호*를 선택합니다.



2. 보호 페이지에서 작업 부하를 선택한 다음 *보호*를 선택합니다.
3. 랜섬웨어 보호 전략 페이지에서 *추가*를 선택합니다.



4. 새로운 전략 이름을 입력하거나 기존 이름을 입력하여 복사합니다. 기존 이름을 입력하는 경우 복사할 이름을 선택하고 *복사*를 선택하세요.

> 기존 전략을 복사하여 수정하기로 선택하면 Ransomware Resilience는 원래 이름에 "_copy"를 추가합니다. 고유하게 만들려면 이름과 하나 이상의 설정을 변경해야 합니다.

5. 각 항목에 대해 *아래쪽 화살표*를 선택하세요.
   - 탐지 정책:
     - 정책: 미리 설계된 탐지 정책 중 하나를 선택합니다.

- **1**차 감지: 랜섬웨어 감지 기능을 활성화하면 랜섬웨어 복원력이 잠재적인 랜섬웨어 공격을 감지합니다.
- 의심스러운 사용자 행동 감지: 사용자 행동 감지 기능을 활성화하여 사용자 활동 이벤트를 Ransomware Resilience로 전송하고 데이터 침해와 같은 의심스러운 이벤트를 감지합니다.
- 파일 확장자 차단: 랜섬웨어 복원력이 알려진 의심스러운 파일 확장자를 차단하도록 설정합니다. 랜섬웨어 복원력은 기본 감지가 활성화된 경우 자동으로 스냅샷 복사본을 만듭니다.

  차단된 파일 확장자를 변경하려면 시스템 관리자에서 편집하세요.

◦ 스냅샷 정책:

- 스냅샷 정책 기반 이름: 정책을 선택하거나 *생성*을 선택하고 스냅샷 정책의 이름을 입력합니다.
- 스냅샷 잠금: 이 기능을 활성화하면 랜섬웨어 공격이 백업 저장소 대상까지 침투하더라도 일정 기간 동안 스냅샷 사본을 수정하거나 삭제할 수 없도록 기본 저장소에 잠급니다. 이를 _변경 불가능한 저장소_라고도 합니다. 이렇게 하면 복구 시간이 더 빨라집니다.

  스냅샷이 잠기면 볼륨 만료 시간은 스냅샷 복사본의 만료 시간으로 설정됩니다.

스냅샷 복사 잠금 기능은 ONTAP 9.12.1 이상에서 사용할 수 있습니다. SnapLock 에 대해 자세히 알아보려면 다음을 참조하세요. "ONTAP 의 SnapLock" .

- 스냅샷 일정: 일정 옵션과 보관할 스냅샷 사본 수를 선택하고 일정을 활성화할지 선택합니다.

◦ 백업 정책:

- 백업 정책 기본 이름: 새 이름을 입력하거나 기존 이름을 선택하세요.
- 백업 일정: 보조 저장소에 대한 일정 옵션을 선택하고 일정을 활성화합니다.

보조 저장소에서 백업 잠금을 활성화하려면 설정 옵션을 사용하여 백업 대상을 구성하세요. 자세한 내용은 다음을 참조하십시오. "설정 구성" .

6. *추가*를 선택하세요.

SnapCenter 또는 **Backup and Recovery**에서 관리하는 기존 스냅샷 및 백업 정책이 있는 워크로드에 감지 정책을 추가합니다.

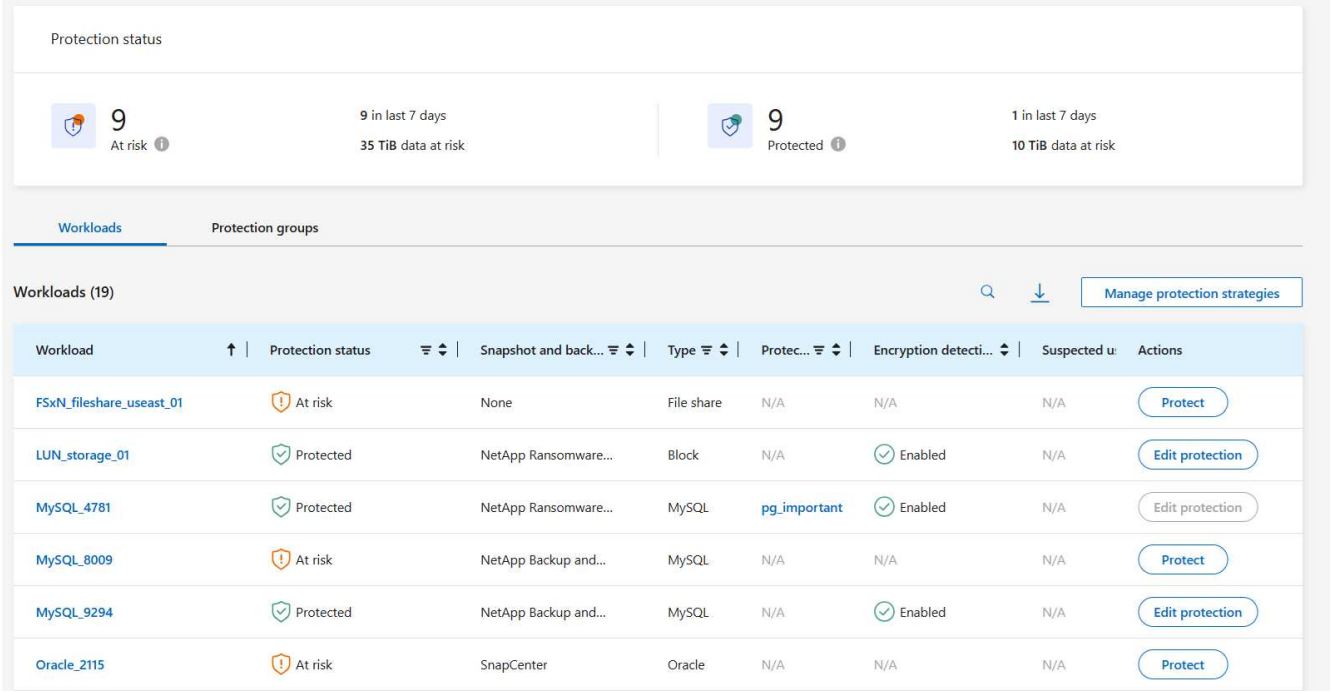
랜섬웨어 복원력을 사용하면 다른 NetApp 제품이나 서비스에서 관리되는 기존 스냅샷 및 백업 보호가 있는 워크로드에 탐지 정책이나 보호 정책을 할당할 수 있습니다. 백업 및 복구, SnapCenter 와 같은 다른 서비스는 스냅샷, 보조 스토리지로의 복제 또는 개체 스토리지로의 백업을 관리하는 정책을 사용합니다.

기존 백업 또는 스냅샷 정책이 있는 워크로드에 감지 정책 추가

Backup and Recovery 또는 SnapCenter 에 기존 스냅샷 또는 백업 정책이 있는 경우 랜섬웨어 공격을 감지하는 정책을 추가할 수 있습니다. 랜섬웨어 복원력을 사용하여 보호 및 탐지를 관리하려면 다음을 참조하세요.랜섬웨어 복원력으로 보호하세요 .

단계

1. 랜섬웨어 복원력 메뉴에서 *보호*를 선택합니다.



2. 보호 페이지에서 작업 부하를 선택한 다음 *보호*를 선택합니다.
3. 랜섬웨어 복원력은 기존에 활성화된 SnapCenter 또는 백업 및 복구 정책이 있는지 감지합니다.
4. 기존 백업 및 복구 또는 SnapCenter 정책을 그대로 두고 탐지 정책만 적용하려면 기존 정책 바꾸기 상자를 선택하지 마세요.
5. SnapCenter 정책에 대한 자세한 내용을 보려면 *아래쪽 화살표*를 선택하세요.
6. 원하는 탐지 설정을 선택하세요: 암호화 탐지 의심스러운 사용자 동작 탐지 의심스러운 파일 확장자 차단
7. 다음을 선택하세요.
8. *의심스러운 사용자 동작 감지*를 감지 설정으로 선택한 경우 사용자 활동 에이전트를 선택하거나"또는 하나 만드세요" .

   사용자 활동 에이전트는 새로운 데이터 수집기를 호스팅합니다. 랜섬웨어 복원력은 사용자 활동 이벤트를 랜섬웨어 복원력으로 자동으로 전송하여 비정상적인 사용자 행동을 감지하는 데이터 수집기를 생성합니다.

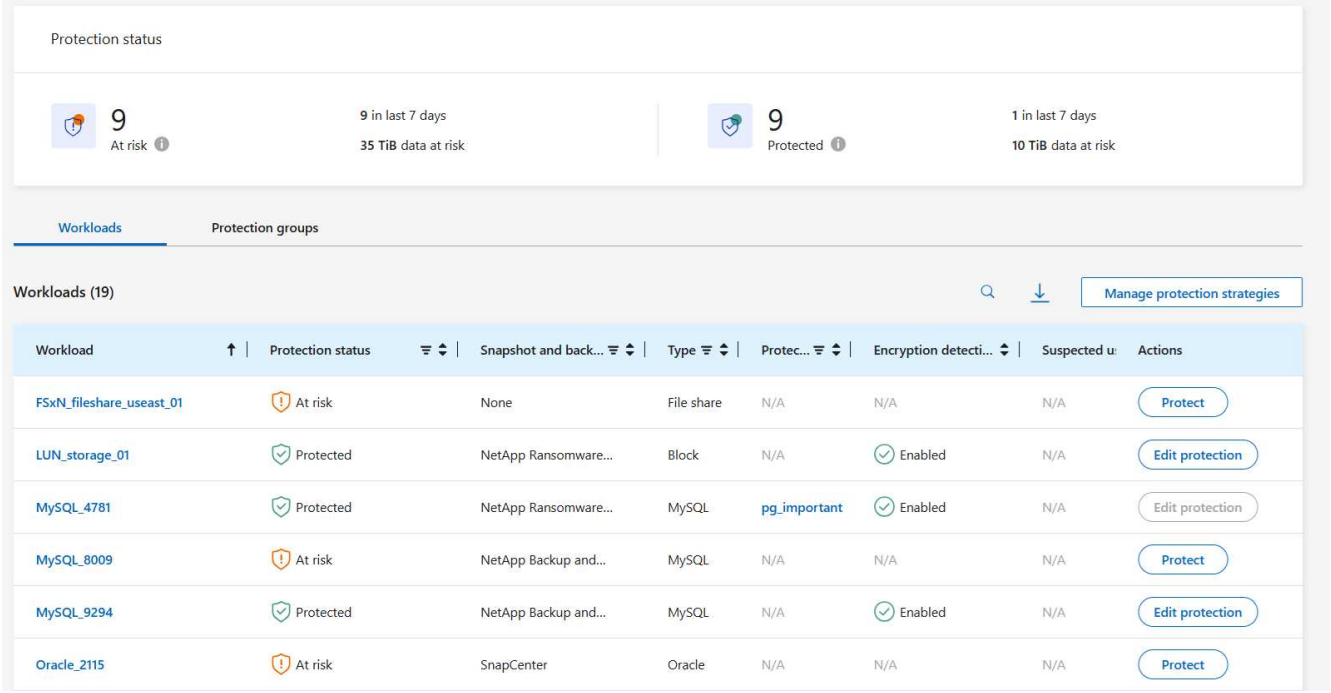
9. 다음을 선택하세요.
10. 선택 사항을 검토하세요. 감지 기능을 활성화하려면 만들기를 선택하세요.
11. 보호 페이지에서 탐지 상태를 검토하여 탐지가 활성화되어 있는지 확인하세요.

기존 백업 또는 스냅샷 정책을 랜섬웨어 보호 전략으로 교체

기존 백업이나 스냅샷 정책을 랜섬웨어 보호 전략으로 대체할 수 있습니다. 이 접근 방식을 사용하면 외부에서 관리되는 보호 기능이 제거되고 랜섬웨어 복원력에서 탐지 및 보호 기능이 구성됩니다.

단계

1. 랜섬웨어 복원력 메뉴에서 *보호*를 선택합니다.



2. 보호 페이지에서 작업 부하를 선택한 다음 *보호*를 선택합니다.
3. 랜섬웨어 복원력은 기존에 활성화된 백업 및 복구 또는 SnapCenter 정책이 있는지 감지합니다. 기존 백업 및 복구 또는 SnapCenter 정책을 바꾸려면 기존 정책 바꾸기 상자를 선택하세요. 상자를 선택하면 랜섬웨어 복원력이 탐지 정책 목록을 탐지 정책으로 바꿉니다.
4. 보호 정책을 선택하세요. 보호 정책이 없으면 추가를 선택하여 새 정책을 만듭니다. 정책 생성에 대한 정보는 다음을 참조하세요.보호 정책 만들기 . 다음을 선택하세요.
5. 백업 대상을 선택하거나 새 대상을 만듭니다. 다음을 선택하세요.
   a. 보호 전략에 사용자 동작 감지가 포함된 경우 환경에서 새 데이터 수집기를 호스팅할 사용자 활동 에이전트를 선택하세요. 랜섬웨어 복원력은 사용자 활동 이벤트를 랜섬웨어 복원력으로 자동으로 전송하여 비정상적인 사용자 행동을 감지하는 데이터 수집기를 생성합니다.
6. 새로운 보호 전략을 검토한 다음 보호를 선택하여 적용합니다.
7. 보호 페이지에서 탐지 상태를 검토하여 탐지가 활성화되어 있는지 확인하세요.

다른 정책을 할당합니다

기존 정책을 다른 정책으로 대체할 수 있습니다.

단계

1. 랜섬웨어 복원력 메뉴에서 *보호*를 선택합니다.
2. 보호 페이지의 작업 부하 행에서 *보호 편집*을 선택합니다.
3. 워크로드에 유지 관리하려는 기존 백업 및 복구 또는 SnapCenter 정책이 있는 경우 기존 정책 바꾸기의 선택을 취소합니다. 기존 정책을 바꾸려면 기존 정책 바꾸기를 선택하세요.
4. 정책 페이지에서 할당하려는 정책의 아래쪽 화살표를 선택하여 세부 정보를 검토합니다.
5. 할당하려는 정책을 선택하세요.
6. *보호*를 선택하여 변경을 완료하세요.

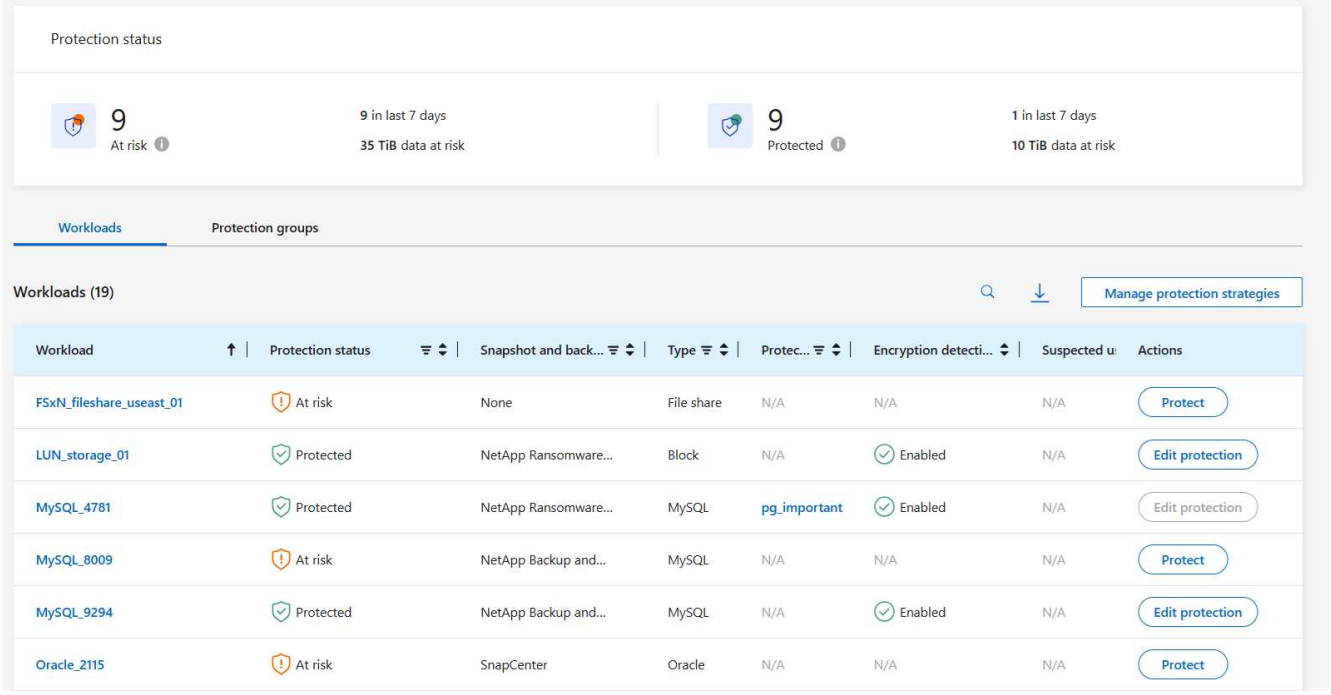
보호 그룹 생성

파일 공유를 보호 그룹으로 그룹화하면 데이터 자산을 보호하기가 더 쉬워집니다. 랜섬웨어 복원력은 각 볼륨을 개별적으로 보호하는 대신, 그룹의 모든 볼륨을 동시에 보호할 수 있습니다.

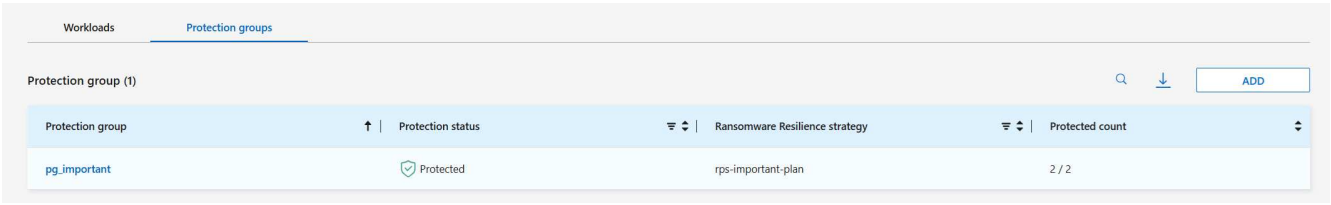
보호 상태(즉, 보호되지 않는 그룹과 보호되는 그룹)에 관계없이 그룹을 만들 수 있습니다. 보호 그룹에 보호 정책을 추가하면 새 보호 정책이 SnapCenter 및 NetApp Backup and Recovery 에서 관리하는 정책을 포함한 모든 기존 정책을 대체합니다.

단계

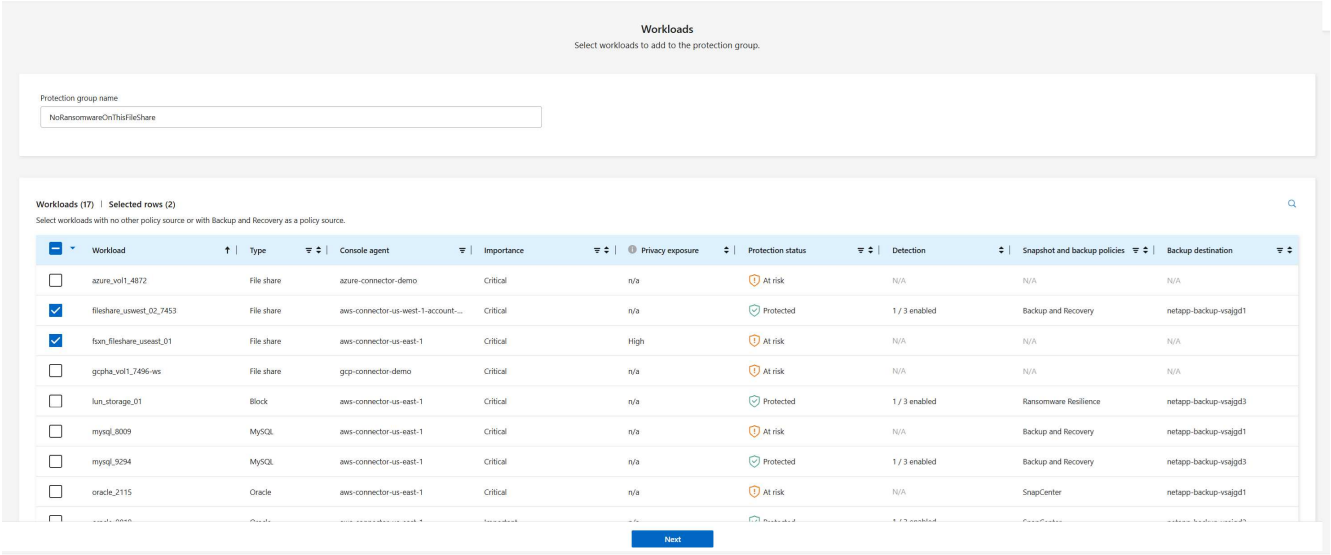
1. 랜섬웨어 복원력 메뉴에서 *보호*를 선택합니다.



2. 보호 페이지에서 보호 그룹 탭을 선택합니다.



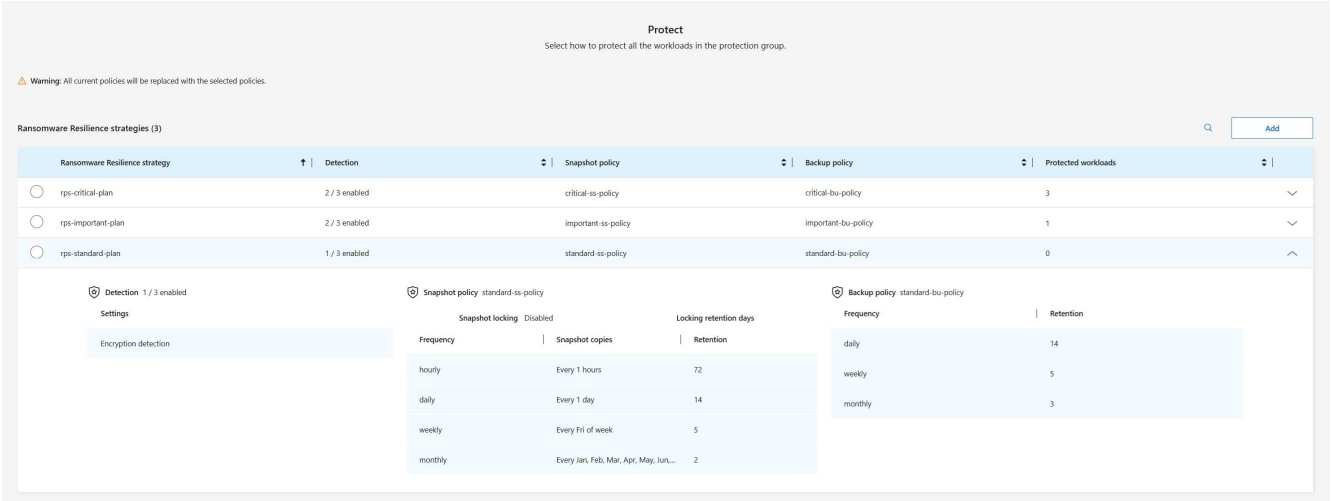
3. *추가*를 선택하세요.



4. 보호 그룹의 이름을 입력하세요.
5. 그룹에 추가할 작업 부하를 선택합니다.

   작업 부하에 대한 자세한 내용을 보려면 오른쪽으로 스크롤하세요.

6. *다음*을 선택하세요.



7. 이 그룹에 대한 보호를 관리하는 정책을 선택하세요. 확인하려면 *다음*을 선택하세요.
   a. 백업 정책을 구성해야 하는 경우, 정책을 선택한 후 다음을 선택하세요.
   b. 탐지 정책에 사용자 동작 탐지가 포함된 경우 사용할 데이터 수집기를 선택한 후 다음을 클릭합니다.
8. 보호 그룹에 대한 선택 사항을 검토합니다.
9. 보호 그룹 생성을 완료하려면 *추가*를 선택하세요.

그룹 보호 편집

기존 그룹의 탐지 정책을 변경할 수 있습니다.

단계

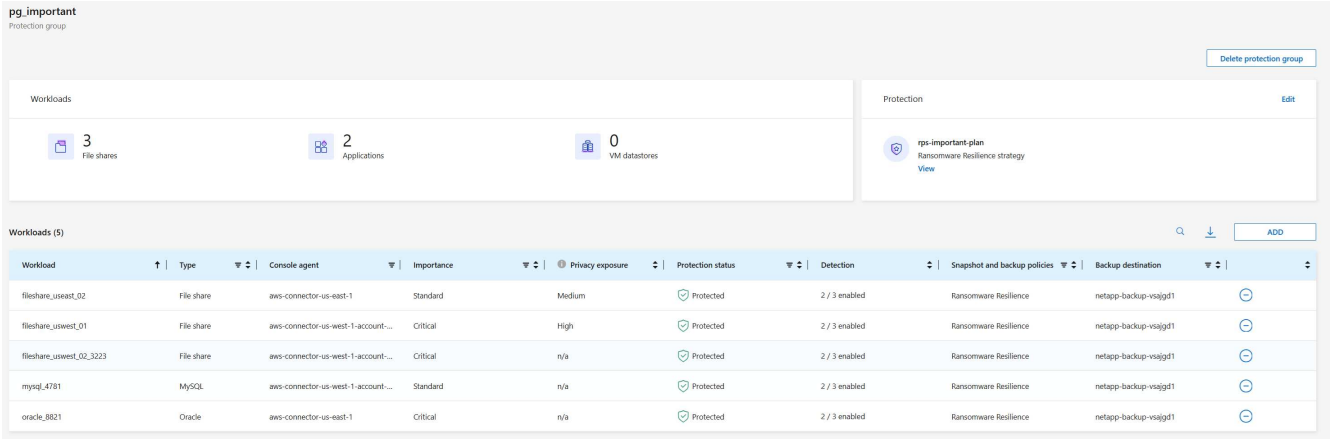
1. 랜섬웨어 복원력 메뉴에서 *보호*를 선택합니다.
2. 보호 페이지에서 보호 그룹 탭을 선택한 다음 정책을 수정할 그룹을 선택합니다.
3. 보호 그룹의 개요 페이지에서 *보호 편집*을 선택합니다.
4. 적용할 기존 보호 정책을 선택하거나 추가를 선택하여 새 보호 정책을 만듭니다. 보호 정책 추가에 대한 자세한 내용은 다음을 참조하세요.보호 정책 만들기 . 그런 다음 저장을 선택합니다.
5. 백업 대상 개요에서 기존 백업 대상을 선택하거나 새 백업 대상 추가를 클릭합니다.
6. 다음을 선택하여 변경 사항을 검토하세요.

그룹에서 작업 부하 제거

나중에 기존 그룹에서 작업 부하를 제거해야 할 수도 있습니다.

단계

1. 랜섬웨어 복원력 메뉴에서 *보호*를 선택합니다.
2. 보호 페이지에서 보호 그룹 탭을 선택합니다.
3. 하나 이상의 작업 부하를 제거할 그룹을 선택합니다.



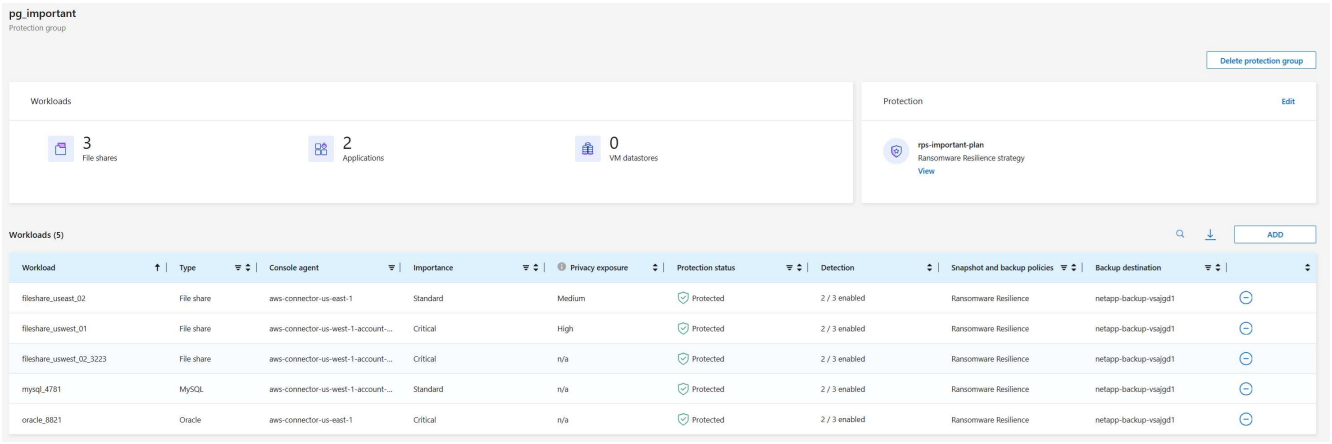
4. 선택한 보호 그룹 페이지에서 그룹에서 제거할 작업 부하를 선택하고 *작업*을 선택합니다.••• 옵션.
5. 작업 메뉴에서 *작업 부하 제거*를 선택합니다.
6. 작업 부하를 제거할 것인지 확인하고 *제거*를 선택합니다.

보호 그룹 삭제

보호 그룹을 삭제하면 그룹과 해당 보호 기능은 제거되지만 개별 작업 부하가 제거되지는 않습니다.

단계

1. 랜섬웨어 복원력 메뉴에서 *보호*를 선택합니다.
2. 보호 페이지에서 보호 그룹 탭을 선택합니다.
3. 하나 이상의 작업 부하를 제거할 그룹을 선택합니다.



4. 선택한 보호 그룹 페이지의 오른쪽 상단에서 *보호 그룹 삭제*를 선택합니다.
5. 그룹을 삭제하고 싶은지 확인하고 *삭제*를 선택하세요.

랜섬웨어 보호 전략 관리

랜섬웨어 전략을 삭제할 수 있습니다.

랜섬웨어 보호 전략으로 보호되는 워크로드 보기

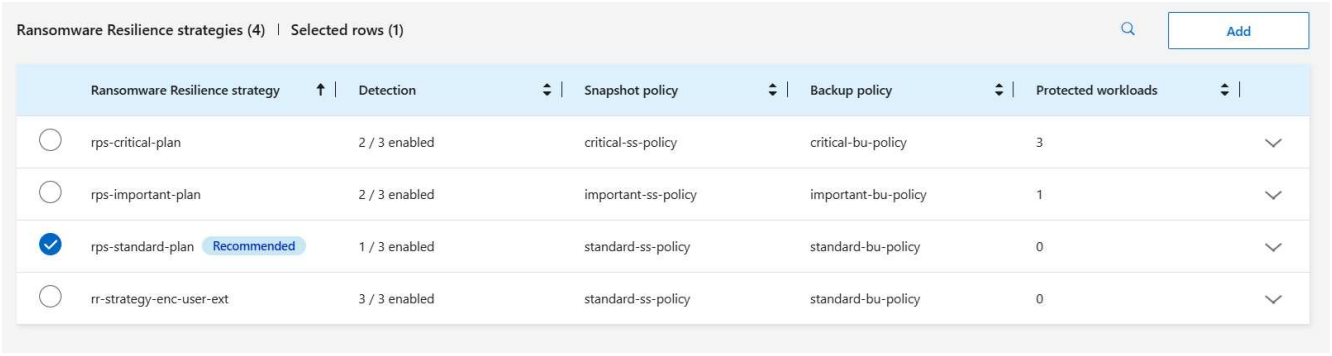
랜섬웨어 보호 전략을 삭제하기 전에 해당 전략으로 보호되는 워크로드를 확인하는 것이 좋습니다.

전략 목록에서 워크로드를 볼 수도 있고, 특정 전략을 편집할 때도 워크로드를 볼 수 있습니다.

전략을 보는 단계

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

   랜섬웨어 보호 전략 페이지에는 전략 목록이 표시됩니다.



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

랜섬웨어 보호 전략 삭제

현재 어떤 워크로드와도 연관되지 않은 보호 전략을 삭제할 수 있습니다.

단계

1. 랜섬웨어 복원력 메뉴에서 *보호*를 선택합니다.
2. 보호 페이지에서 *보호 전략 관리*를 선택합니다.
3. 전략 관리 페이지에서 *작업*을 선택하세요.••• 삭제하려는 전략에 대한 옵션입니다.
4. 작업 메뉴에서 *정책 삭제*를 선택합니다.

랜섬웨어 복원력에서 **NetApp Data Classification** 사용하여 개인 식별 정보를 스캔하세요

NetApp Ransomware Resilience 내에서 NetApp Data Classification 사용하여 파일 공유 워크로드의 데이터를 스캔하고 분류할 수 있습니다. 데이터를 분류하면 데이터 세트에 개인 식별 정보(PII)가 포함되어 있는지 확인하는 데 도움이 되며, PII가 포함되어 있으면 보안 위험이 커질 수 있습니다. 데이터 분류는 NetApp Console 의 핵심 구성 요소이며 추가 비용 없이 사용할 수 있습니다.

"데이터 분류"AI 기반 자연어 처리를 활용해 상황에 맞는 데이터를 분석하고 분류하여, 규정 준수 요구 사항을 충족하고, 보안 취약성을 탐지하고, 비용을 최적화하고, 마이그레이션을 가속화할 수 있는 실행 가능한 데이터 통찰력을 제공합니다.

이 프로세스는 작업 부하의 중요도에 영향을 미쳐 적절한 보호가 이루어지도록 하는 데 도움이 됩니다.

필수 콘솔 역할 이 작업을 수행하려면 조직 관리자, 폴더 또는 프로젝트 관리자, 랜섬웨어 복원력 관리자 역할이 필요합니다. "NetApp Console 의 랜섬웨어 복원력 역할에 대해 알아보세요" .

데이터 분류를 통해 개인 정보 노출 식별

랜섬웨어 복원력 내에서 데이터 분류를 사용하기 전에 다음이 필요합니다."데이터 분류를 활성화하여 데이터를 스캔합니다." .

랜섬웨어 복원력의 보호 페이지에서 데이터 분류를 배포할 수 있습니다. 개인정보 노출을 식별하기 위한 절차를 따르세요. 노출 식별을 선택할 때 아직 데이터 분류를 배포하지 않은 경우 대화 상자가 나타나 데이터 분류를 활성화할 수 있습니다.

데이터 분류에 대한 자세한 내용은 다음을 참조하세요.

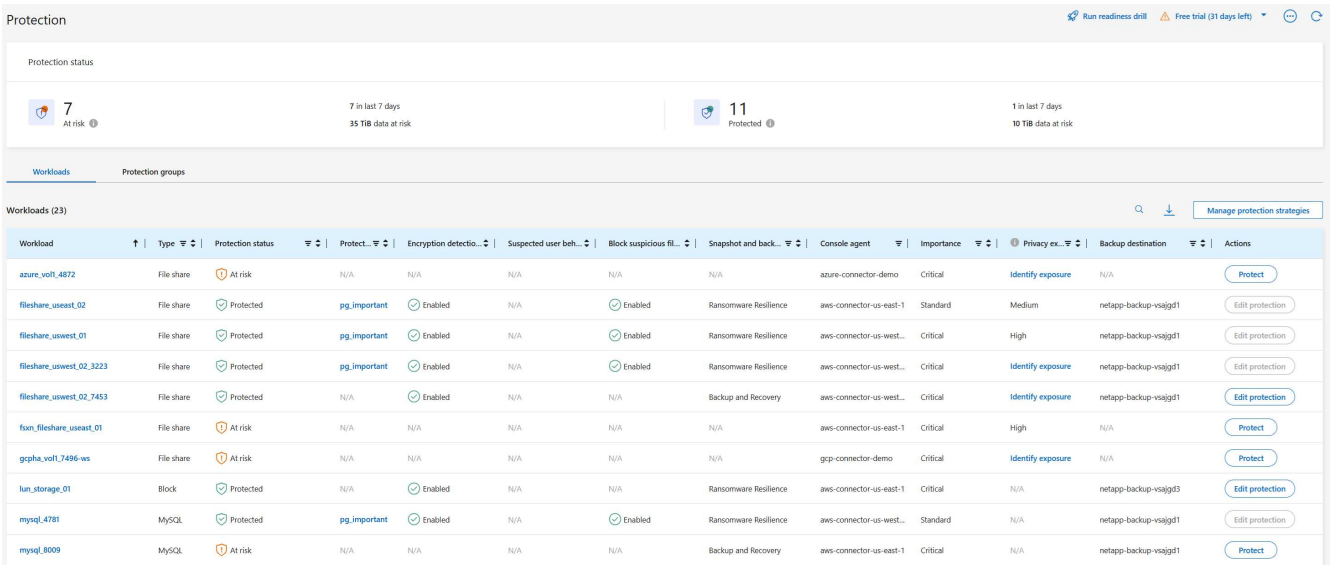
- "데이터 분류에 대해 알아보세요"
- "개인 정보의 범주"
- "귀하의 조직에 저장된 데이터를 조사하세요"

시작하기 전에

랜섬웨어 복원력에서 PII 데이터 스캔은 다음 경우에 사용할 수 있습니다."배포된 데이터 분류" . 데이터 분류는 추가 비용 없이 콘솔의 일부로 제공되며 온프레미스 또는 고객 클라우드에 배포할 수 있습니다.

단계

1. 랜섬웨어 복원력 메뉴에서 *보호*를 선택합니다.
2. 보호 페이지에서 작업 부하 열에서 파일 공유 작업 부하를 찾습니다.



3. 데이터 분류를 활성화하여 PII에 대한 데이터를 검사하려면 개인 정보 노출 열에서 *노출 식별*을 선택합니다.

데이터 분류를 배포하지 않은 경우 *노출 식별*을 선택하면 데이터 분류를 배포하기 위한 대화 상자가 열립니다. *배포*를 선택합니다. 데이터 분류를 배포한 후 보호 페이지로 돌아와서 *노출 식별*을 선택할 수 있습니다.

결과

스캔은 파일의 크기와 수에 따라 몇 분 정도 걸릴 수 있습니다. 검사하는 동안 보호 페이지에는 파일이 식별되고 파일 개수가 제공됩니다. 스캐닝이 완료되면 개인 정보 노출 열에서 노출 수준을 낮음, 보통, 높음으로 평가합니다.

개인정보 노출 검토

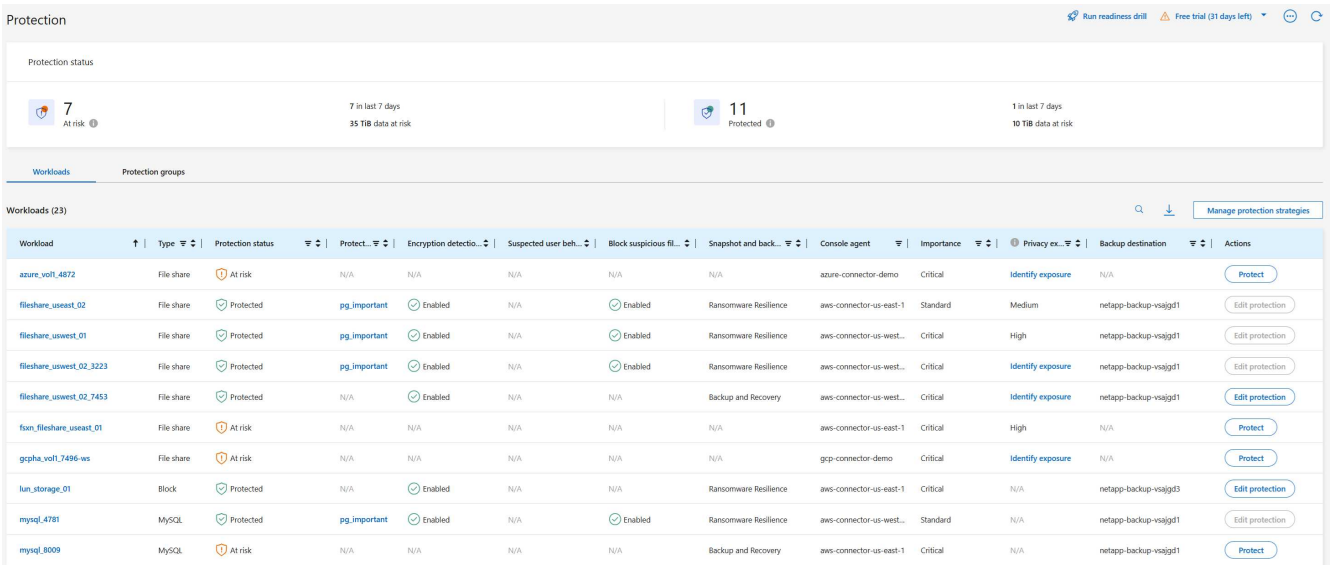
PII에 대한 데이터 분류 스캔 후 위험을 평가합니다.

PII 데이터는 다음 세 가지 명칭 중 하나로 분류됩니다.

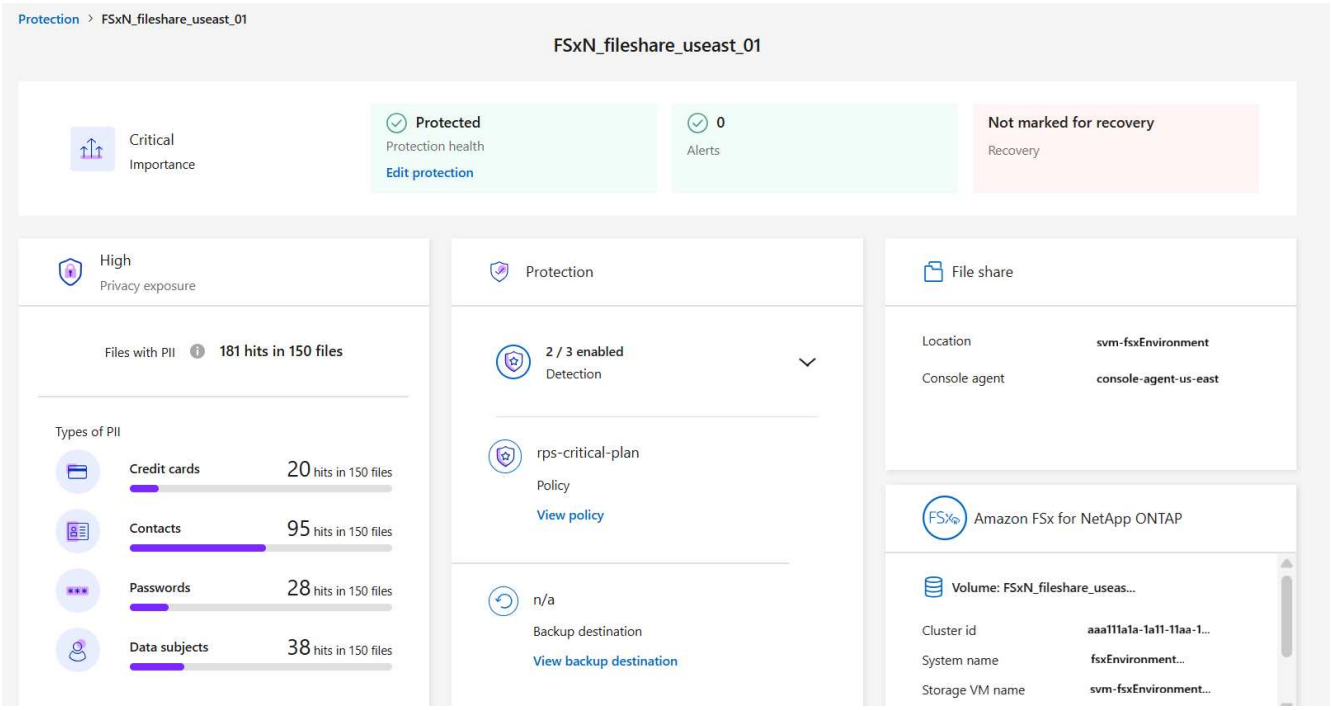
- 높음: 파일의 70% 이상이 PII를 포함합니다.
- 중간: 파일의 30% 이상, 70% 미만에 PII가 포함되어 있음
- 낮음: 0% 초과, 30% 미만의 파일에 PII가 포함되어 있음

단계

1. 랜섬웨어 복원력 메뉴에서 *보호*를 선택합니다.
2. 보호 페이지에서 개인 정보 노출 열에 상태가 표시되는 작업 부하 열에서 파일 공유 작업 부하를 찾습니다.



3. 작업 부하 열에서 작업 부하 링크를 선택하면 작업 부하 세부 정보를 볼 수 있습니다.



4. 작업 부하 세부 정보 페이지에서 개인 정보 노출 타일의 세부 정보를 확인하세요.

개인정보 노출이 업무 중요도에 미치는 영향

개인정보 노출 변경은 작업 부하의 중요도에 영향을 미칠 수 있습니다.

개인정보 노출 시:	이러한 개인정보 노출로 인해:	이러한 개인정보 노출에 대하여:	그러면 작업 부하 중요도는 다음과 같습니다.
감소	높음, 중간 또는 낮음	중간, 낮음 또는 없음	동일하게 유지됩니다

개인정보 노출 시:	이러한 개인정보 노출로 인해:	이러한 개인정보 노출에 대하여:	그러면 작업 부하 중요도는 다음과 같습니다.
증가합니다	None	낮은	표준으로 유지됩니다
	낮은	중간	표준에서 중요로의 변경 사항
	낮음 또는 중간	높은	표준 또는 중요에서 중요로의 변경

더 많은 정보를 원하시면

데이터 분류에 대한 자세한 내용은 데이터 분류 설명서를 참조하세요.

- "데이터 분류에 대해 알아보세요"
- "개인 정보의 범주"
- "귀하의 조직에 저장된 데이터를 조사하세요"

NetApp Ransomware Resilience 사용하여 감지된 랜섬웨어 알림을 처리하세요

NetApp Ransomware Resilience 잠재적인 공격을 감지하면 대시보드와 알림 영역에 경고가 표시됩니다. 랜섬웨어 복원력은 즉시 스냅샷을 찍습니다. 랜섬웨어 복원력 알림 탭에서 잠재적 위험을 검토하세요.

랜섬웨어 복원력이 잠재적인 공격을 감지하면 콘솔 알림 설정에 알림이 나타나고 구성된 주소로 이메일이 전송됩니다. 이메일에는 심각도, 영향을 받는 작업 부하, 랜섬웨어 복원력 알림 탭의 알림에 대한 링크에 대한 정보가 포함되어 있습니다.

거짓 양성 결과를 무시하거나 즉시 데이터를 복구하기로 결정할 수 있습니다.

알림을 해제하면 랜섬웨어 복원력이 이러한 동작을 학습하고 이를 일반적인 작업과 연관시켜 다시 알림을 발생시키지 않습니다.

데이터 복구를 시작하려면 알림을 복구 준비 완료로 표시하여 스토리지 관리자가 복구 프로세스를 시작할 수 있도록 하세요.

각 알림에는 다양한 볼륨과 상태에 대한 여러 사건이 포함될 수 있습니다. 모든 사건을 검토하세요.

랜섬웨어 복원력은 다음과 같이 경고가 발행된 원인에 대한 _증거_라고 하는 정보를 제공합니다.

- 파일 확장자가 생성되거나 변경되었습니다.
- 감지된 비율과 예상 비율을 비교하여 파일 생성
- 감지된 비율과 예상 비율을 비교하여 파일을 삭제합니다.
- 암호화 수준이 높고 파일 확장자가 변경되지 않은 경우

알림은 다음 중 하나로 분류됩니다.

- 잠재적 공격: Autonomous Ransomware Protection이 새로운 확장 프로그램을 감지하고 해당 현상이 지난 24시간 동안 20회 이상 반복되면 경고가 발생합니다(기본 동작).
- 경고: 다음과 같은 동작이 발생할 경우 경고가 발생합니다.
  - 이전에 새로운 확장 프로그램이 감지된 적이 없으며, 동일한 동작이 공격으로 선언할 만큼 충분히 반복되지 않습니다.
  - 높은 엔트로피가 관찰됩니다.
  - 파일 읽기, 쓰기, 이름 바꾸기 또는 삭제 활동이 일반 수준에 비해 두 배로 증가했습니다.

SAN 환경의 경우 경고는 높은 엔트로피에만 기반합니다.

증거는 ONTAP 의 Autonomous Ransomware Protection에서 얻은 정보를 기반으로 합니다. 자세한 내용은 다음을 참조하세요. "자율형 랜섬웨어 보호 개요" .

알림은 다음 상태 중 하나를 가질 수 있습니다.

- 새로운
- 비활성

경고 사건은 다음 상태 중 하나를 가질 수 있습니다.

- 새로운: 모든 사건은 처음 확인되면 "새로운"으로 표시됩니다.
- 해제됨: 해당 활동이 랜섬웨어 공격이 아니라고 의심되는 경우 상태를 "해제됨"으로 변경할 수 있습니다.

공격을 해제한 후에는 다시 변경할 수 없습니다. 작업 부하를 해제하면 잠재적인 랜섬웨어 공격에 대응하여 자동으로 생성된 모든 스냅샷 사본이 영구적으로 삭제됩니다.

- 기각: 사건이 기각되는 과정에 있습니다.
- 해결됨: 문제가 해결되었습니다.
- 자동 해결: 우선순위가 낮은 알림의 경우, 5일 이내에 아무런 조치가 취해지지 않으면 사고가 자동으로 해결됩니다.

설정 페이지에서 랜섬웨어 복원력에 보안 및 이벤트 관리 시스템(SIEM)을 구성한 경우 랜섬웨어 복원력이 SIEM 시스템으로 경고 세부 정보를 보냅니다.

알림 보기

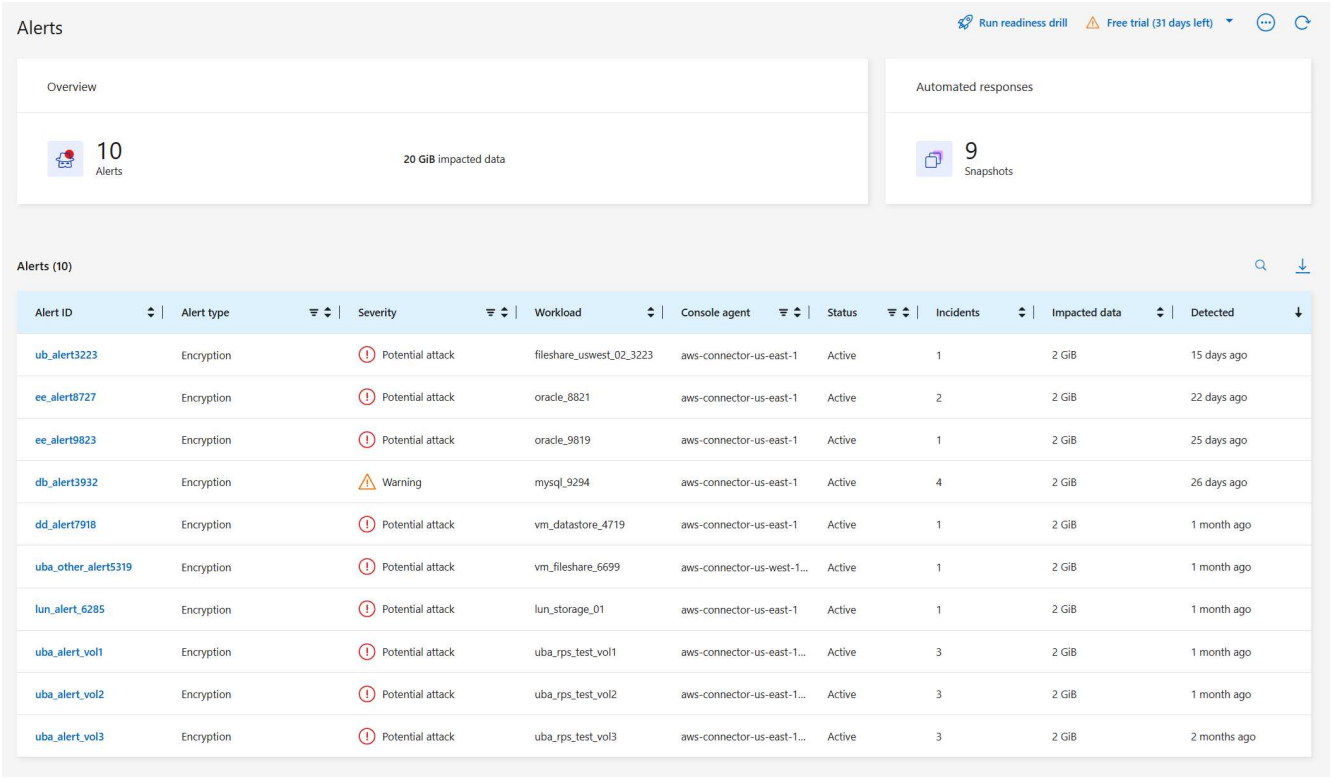
랜섬웨어 복원력 대시보드 또는 알림 탭에서 알림에 액세스할 수 있습니다.

필수 콘솔 역할 이 작업을 수행하려면 조직 관리자, 폴더 또는 프로젝트 관리자, 랜섬웨어 복원력 관리자 또는 랜섬웨어 복원력 뷰어 역할이 필요합니다. "NetApp Console 의 랜섬웨어 복원력 역할에 대해 알아보세요" .

단계

1. 랜섬웨어 복원력 대시보드에서 알림 창을 검토하세요.
2. 상태 중 하나에서 *모두 보기*를 선택하세요.
3. 각 알림에 대한 각 볼륨의 모든 인시던트를 검토하려면 알림을 선택하세요.

4. 추가 알림을 검토하려면 왼쪽 상단의 탐색 경로에서 *알림*을 선택하세요.
5. 알림 페이지에서 알림을 검토하세요.



6. 다음 중 하나를 계속하세요.
   - 악성 활동 및 비정상적인 사용자 동작 감지 .
   - 랜섬웨어 사고를 복구 준비로 표시(사고가 무력화된 후) .
   - 잠재적 공격이 아닌 사건은 기각합니다. .

알림 이메일에 응답하세요

랜섬웨어 레질리언스가 잠재적인 공격을 감지하면 구독 알림 기본 설정에 따라 구독한 사용자에게 이메일 알림을 보냅니다. 이메일에는 경고에 대한 정보, 심각도, 영향을 받는 리소스 등이 포함되어 있습니다.

랜섬웨어 복원력 경고에 대한 이메일 알림을 받을 수 있습니다. 이 기능을 사용하면 알림, 알림의 심각도, 영향을 받는 리소스에 대한 정보를 얻을 수 있습니다.

이메일 알림을 구독하려면 다음을 참조하세요. "이메일 알림 설정" .

1. 랜섬웨어 복원력에서 설정 페이지로 이동합니다.
2. *알림*에서 이메일 알림 설정을 찾으세요.
3. 알림을 받으려는 이메일 주소를 입력하세요.
4. 변경 사항을 저장합니다.

이제 새로운 알림이 생성되면 이메일 알림을 받게 됩니다.

필수 콘솔 역할 이 작업을 수행하려면 조직 관리자, 폴더 또는 프로젝트 관리자, 랜섬웨어 복원력 관리자 또는 랜섬웨어 복원력 뷰어 역할이 필요합니다. "NetApp Console 의 랜섬웨어 복원력 역할에 대해 알아보세요" .

단계

1. 이메일을 확인하세요.
2. 이메일에서 *알림 보기*를 선택하고 Ransomware Resilience에 로그인하세요.

   알림 페이지가 나타납니다.

3. 각 경고에 대한 각 권의 모든 사건을 검토합니다.
4. 추가 알림을 검토하려면 왼쪽 상단의 빵가루 모양에서 *알림*을 클릭하세요.
5. 다음 중 하나를 계속하세요.
   - 악성 활동 및 비정상적인 사용자 동작 감지 .
   - 랜섬웨어 사고를 복구 준비로 표시(사고가 무력화된 후) .
   - 잠재적 공격이 아닌 사건은 기각합니다. .

악성 활동 및 비정상적인 사용자 동작 감지

알림 탭을 살펴보면 악의적인 활동이나 비정상적인 사용자 동작이 있는지 확인할 수 있습니다.

사용자 수준 알림을 보려면 사용자 활동 에이전트를 구성하고 사용자 동작 감지를 통한 보호 정책을 활성화해야 합니다. 사용자 동작 감지가 활성화되면 의심스러운 사용자 열이 알림 대시보드에 나타납니다. 사용자 동작 감지가 활성화되지 않은 경우에는 표시되지 않습니다. 의심스러운 사용자 감지를 활성화하려면 다음을 참조하세요."의심스러운 사용자 활동" .

> NetApp Data Infrastructure Insights (DII) 워크로드 보안을 사용하는 경우 랜섬웨어 복원력에 동일한 워크로드 보안 에이전트를 사용하는 것이 좋습니다. 랜섬웨어 복원력을 위해 별도의 워크로드 보안 에이전트를 배포할 필요는 없지만, 동일한 워크로드 보안 에이전트를 사용하려면 랜섬웨어 복원력 콘솔 조직과 DII 스토리지 워크로드 보안 테넌트 간에 페어링 관계가 필요합니다. 이 페어링을 활성화하려면 계정 담당자에게 문의하세요.

악성 활동 보기

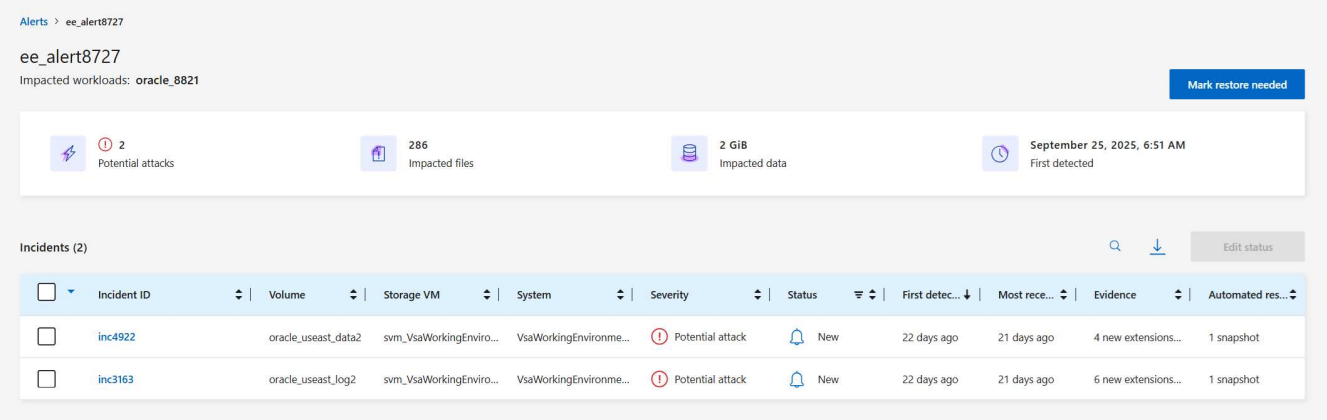
자율형 랜섬웨어 보호가 랜섬웨어 복원력에서 알림을 트리거하면 다음 세부 정보를 볼 수 있습니다.

- 수신 데이터의 엔트로피
- 감지된 비율과 비교한 새 파일의 예상 생성 비율
- 감지된 비율과 비교한 예상 파일 삭제 비율
- 감지된 비율과 비교한 예상 파일 이름 변경 비율
- 영향을 받은 파일 및 디렉토리

> 이러한 세부 정보는 NAS 워크로드에 대해 볼 수 있습니다. SAN 환경에서는 엔트로피 데이터만 사용할 수 있습니다.

단계

1. 랜섬웨어 복원력 메뉴에서 *알림*을 선택합니다.
2. 알림을 선택하세요.
3. 알림에서 발생한 사건을 검토하세요.



4. 사고를 선택하여 사고의 세부 정보를 검토하세요.

비정상적인 사용자 동작 보기

비정상적인 사용자 동작을 확인하기 위해 의심스러운 사용자 감지 기능을 구성한 경우 사용자 수준 데이터를 보고 특정 사용자를 차단할 수 있습니다. 의심스러운 사용자 설정을 활성화하려면 다음을 참조하세요."랜섬웨어 복원력 설정 구성" .

단계

1. 랜섬웨어 복원력 메뉴에서 *알림*을 선택합니다.
2. 알림을 선택하세요.
3. 알림에서 발생한 사건을 검토하세요.
4. 사용자 환경에서 의심되는 사용자를 차단하려면 사용자 이름 아래에서 *차단*을 선택하세요.

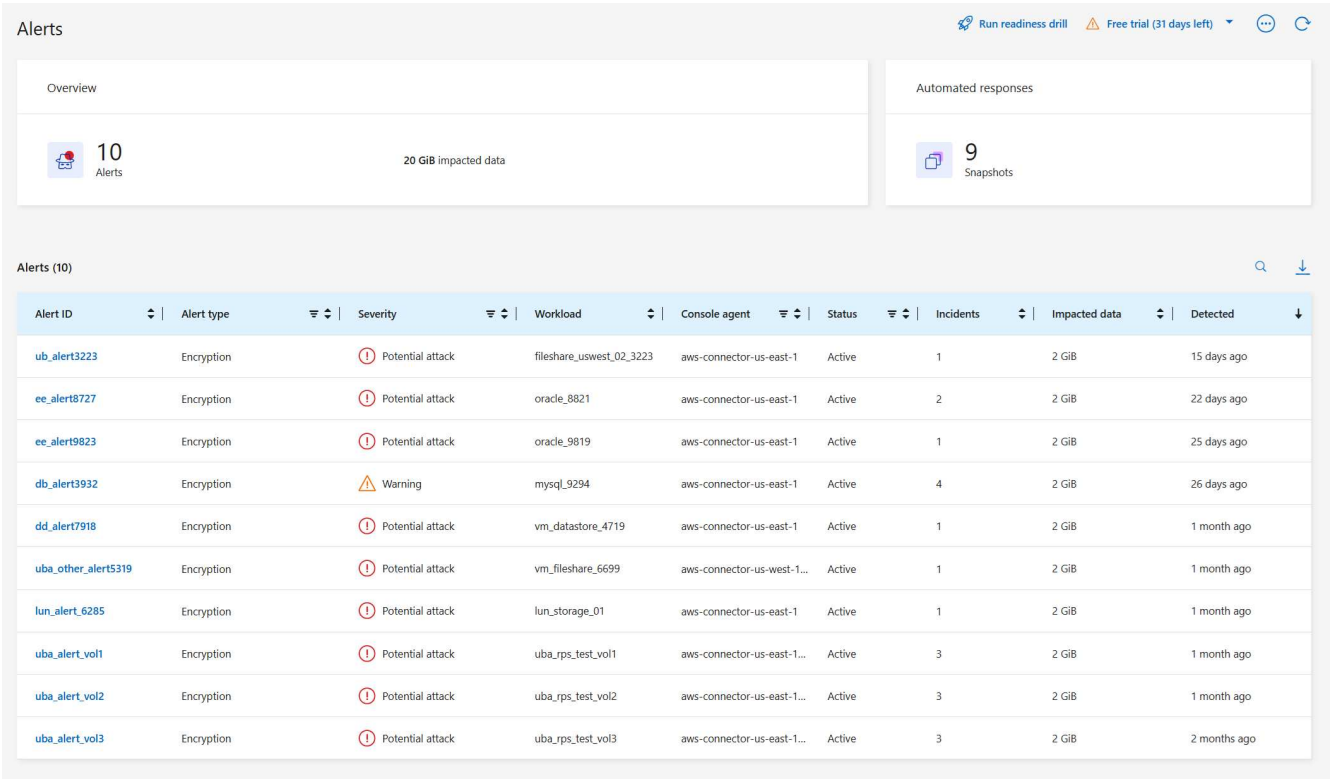
랜섬웨어 사고를 복구 준비로 표시(사고가 무력화된 후)

공격을 중단한 후 스토리지 관리자에게 데이터가 준비되었다고 알려 복구를 시작하세요.

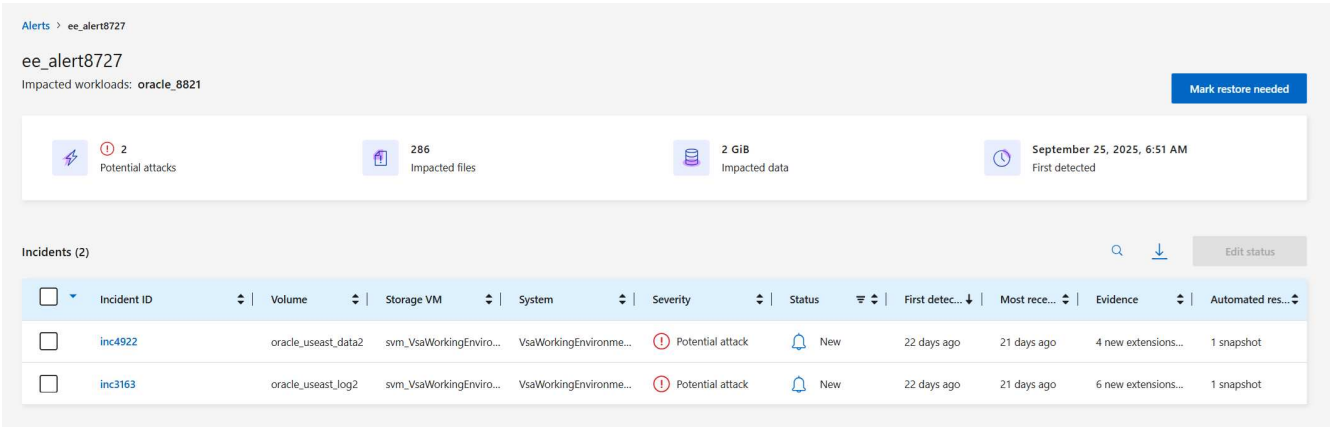
필수 콘솔 역할 이 작업을 수행하려면 조직 관리자, 폴더 또는 프로젝트 관리자, 랜섬웨어 복원력 관리자 역할이 필요합니다. "NetApp Console 의 랜섬웨어 복원력 역할에 대해 알아보세요" .

단계

1. 랜섬웨어 복원력 메뉴에서 *알림*을 선택합니다.



2. 알림 페이지에서 알림을 선택합니다.
3. 알림에서 발생한 사건을 검토하세요.



4. 사고를 복구할 준비가 되었다고 판단되면 *복원 필요 표시*를 선택합니다.
5. 작업을 확인하고 *복원 필요 표시*를 선택하세요.
6. 작업 부하 복구를 시작하려면 메시지에서 작업 부하 복구*를 선택하거나 *복구 탭을 선택하세요.

결과

알림이 복원으로 표시된 후 알림은 알림 탭에서 복구 탭으로 이동합니다.

잠재적 공격이 아닌 사건은 기각합니다.

사고를 검토한 후에는 해당 사고가 잠재적인 공격인지 여부를 판단해야 합니다. 실제 위협이 아니라면 무시해도 됩니다.

거짓 양성 결과를 무시하거나 즉시 데이터를 복구하기로 결정할 수 있습니다. 알림을 해제하면 랜섬웨어 복원력이

이러한 동작을 학습하고 이를 일반적인 작업과 연관시키며 이러한 동작에 대해 다시 알림을 시작하지 않습니다.

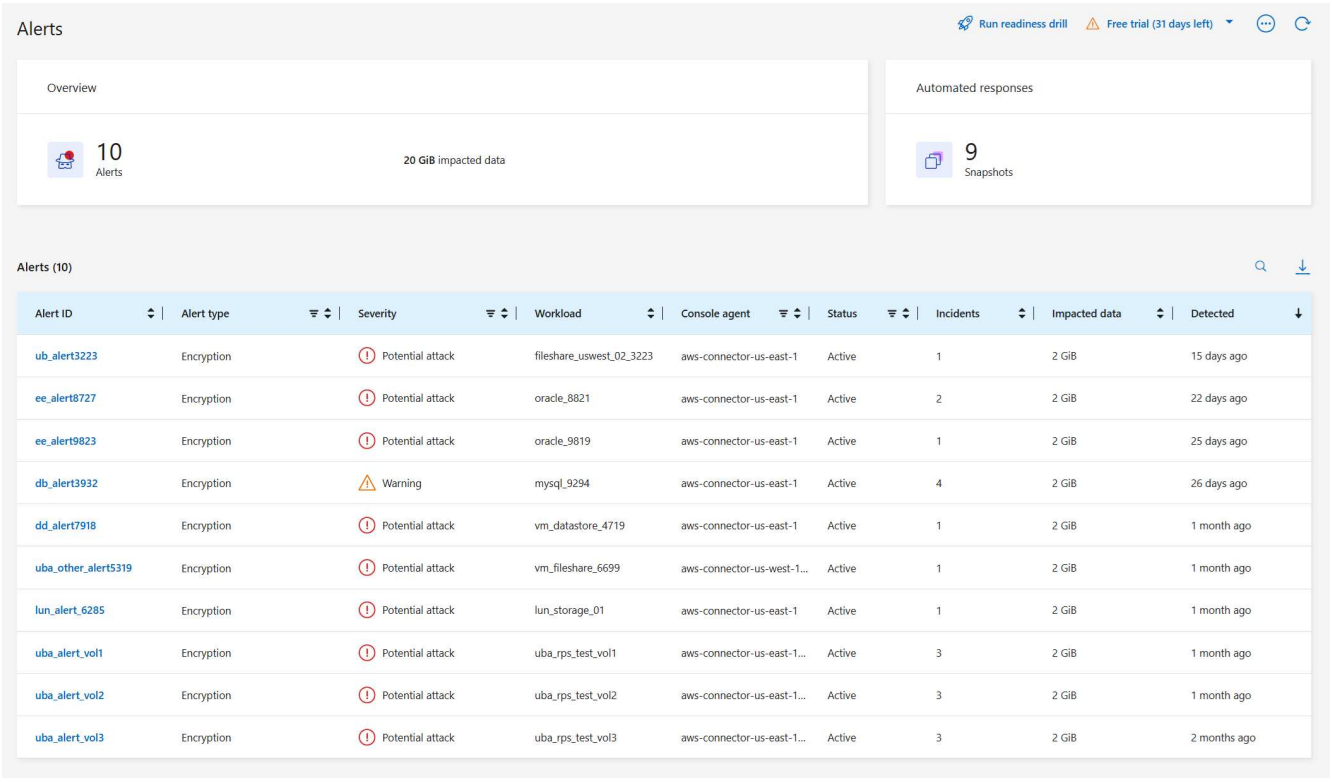
작업 부하를 해제하면 잠재적인 랜섬웨어 공격에 대응하여 자동으로 생성된 모든 스냅샷 사본이 영구적으로 삭제됩니다.

알림을 해제하면 알림 상태를 변경하거나 변경 사항을 취소할 수 없습니다.

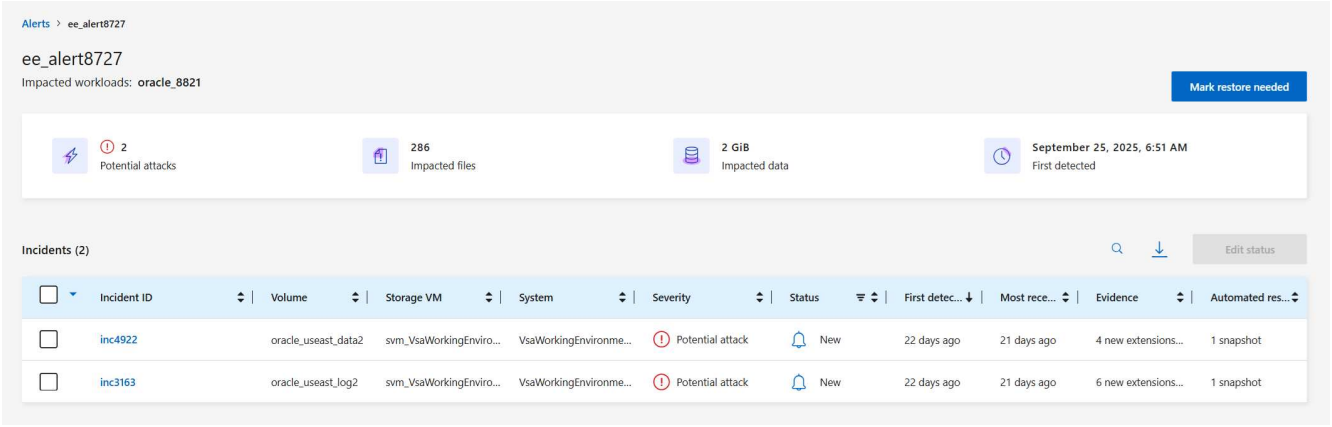
필수 콘솔 역할 이 작업을 수행하려면 조직 관리자, 폴더 또는 프로젝트 관리자, 랜섬웨어 복원력 관리자 역할이 필요합니다. "NetApp Console 의 랜섬웨어 복원력 역할에 대해 알아보세요" .

단계

1. 랜섬웨어 복원력 메뉴에서 *알림*을 선택합니다.

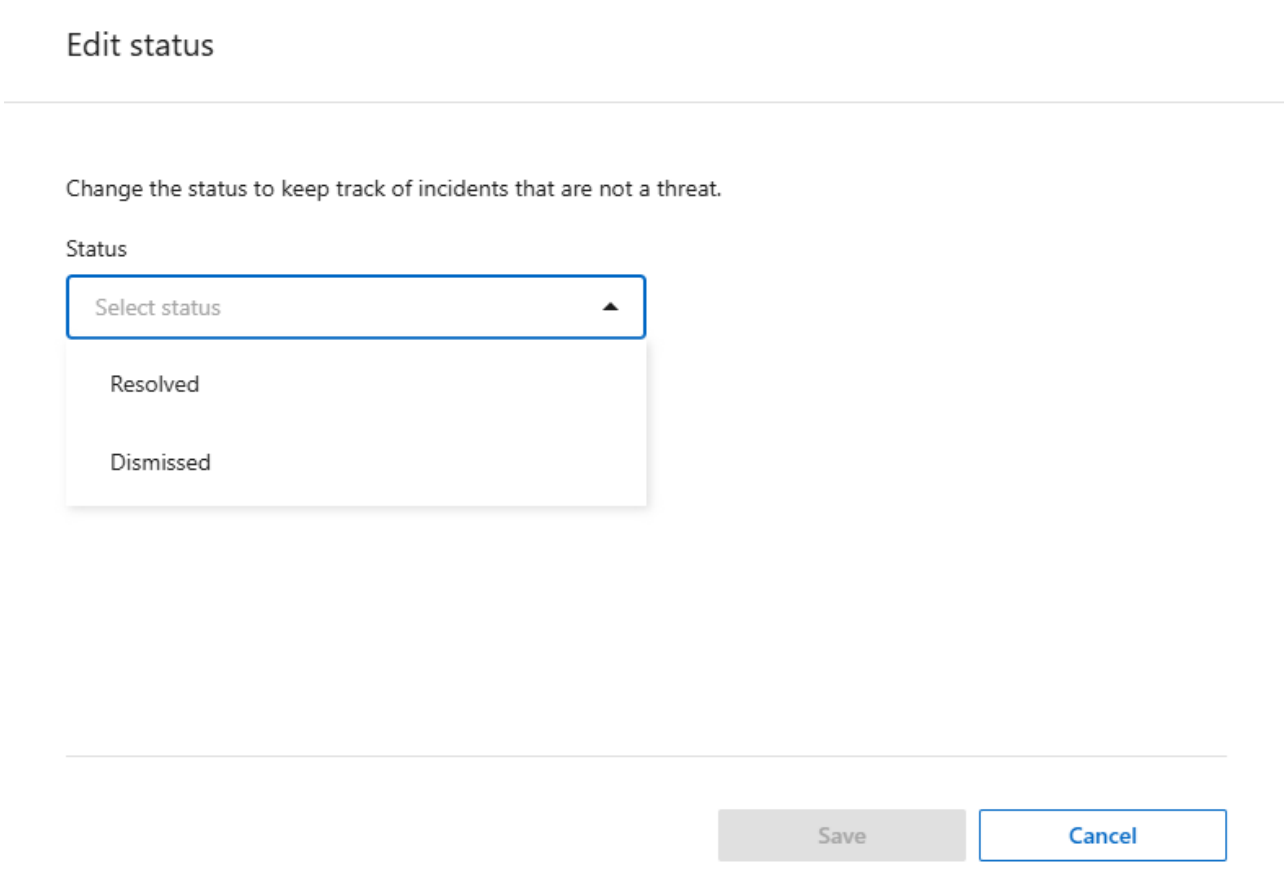


2. 알림 페이지에서 알림을 선택합니다.



3. 하나 이상의 사건을 선택하세요. 또는 표 왼쪽 상단에 있는 사건 ID 상자를 선택하여 모든 사건을 선택하세요.

4. 사건이 위협이 아니라고 판단되면 이를 거짓 긍정으로 간주하여 기각합니다.
    - 사건을 선택하세요.
    - 표 위에 있는 상태 편집 버튼을 선택하세요.



5. 상태 편집 상자에서 “기각됨” 상태를 선택합니다.

    작업 부하와 스냅샷 복사본이 삭제된다는 추가 정보가 나타납니다.

6. *저장*을 선택하세요.

    사건의 상태가 "해제됨"으로 변경됩니다.

영향을 받은 파일 목록 보기

파일 수준에서 애플리케이션 워크로드를 복원하기 전에 영향을 받은 파일 목록을 볼 수 있습니다. 영향을 받은 파일 목록을 다운로드하려면 알림 페이지에 접속하세요. 그런 다음 복구 페이지를 사용하여 목록을 업로드하고 복원할 파일을 선택합니다.

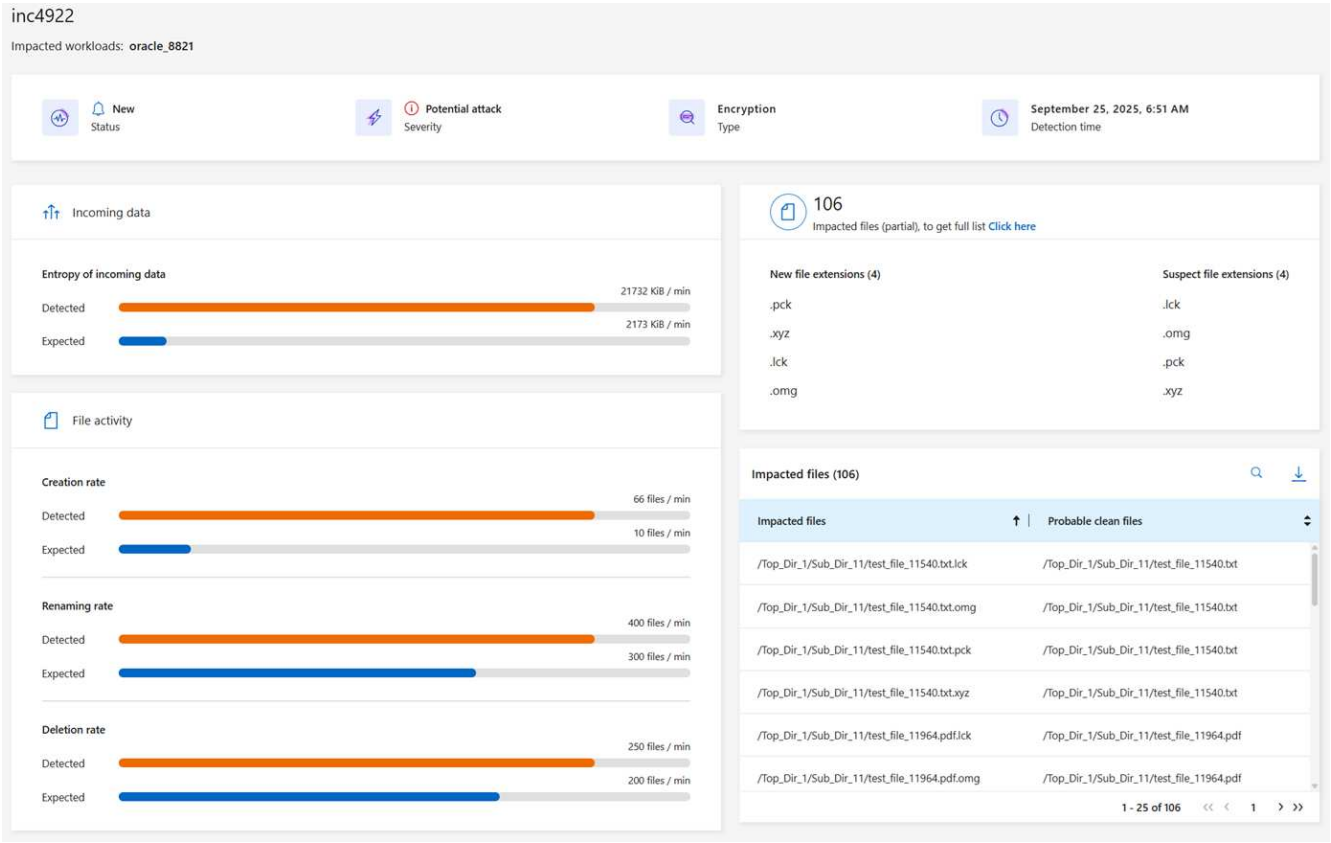
필수 콘솔 역할 이 작업을 수행하려면 조직 관리자, 폴더 또는 프로젝트 관리자, 랜섬웨어 복원력 관리자 역할이 필요합니다. "NetApp Console 의 랜섬웨어 복원력 역할에 대해 알아보세요" .

단계

알림 페이지를 사용하여 영향을 받은 파일 목록을 검색하세요.

볼륨에 여러 개의 알림이 있는 경우 각 알림에 대해 영향을 받는 파일의 CSV 목록을 다운로드해야 할 수도 있습니다.

1. 랜섬웨어 복원력 메뉴에서 *알림*을 선택합니다.
2. 알림 페이지에서 결과를 작업 부하별로 정렬하여 복원하려는 애플리케이션 작업 부하에 대한 알림을 표시합니다.
3. 해당 작업 부하에 대한 알림 목록에서 알림을 선택합니다.
4. 해당 알림에 대해 단일 사건을 선택하세요.



5. 해당 사건에 대해 다운로드 아이콘을 선택하여 영향을 받은 파일 목록을 CSV 형식으로 다운로드하세요.

NetApp Ransomware Resilience 사용하여 랜섬웨어 공격으로부터 복구(사고가 해결된 후)

워크로드가 "복원 필요"로 표시된 후 NetApp Ransomware Resilience 실제 복구 지점(RPA)을 권장하고 충돌 방지 복구를 위한 워크플로를 조정합니다.

- 애플리케이션이나 VM이 SnapCenter 에서 관리되는 경우 Ransomware Resilience는 애플리케이션 일관성 또는 VM 일관성 프로세스를 사용하여 애플리케이션이나 VM을 이전 상태 및 마지막 트랜잭션으로 복원합니다. 애플리케이션 또는 VM 일관성 복원은 캐시나 I/O 작업에 있는 데이터 등 저장소에 들어가지 않은 모든 데이터를 볼륨의 데이터에 추가합니다.
- 애플리케이션이나 VM이 SnapCenter 에서 관리되지 않고 NetApp Backup and Recovery 또는 Ransomware Resilience에서 관리되는 경우, Ransomware Resilience는 충돌 시에도 일관된 복원을 수행합니다. 즉, 시스템이 충돌한 경우와 같이 동일한 시점에 볼륨에 있던 모든 데이터가 복원됩니다.

모든 볼륨, 특정 볼륨 또는 특정 파일을 선택하여 작업 부하를 복원할 수 있습니다.

작업 부하 복구는 실행 중인 작업 부하에 영향을 줄 수 있습니다. 적절한 이해 관계자와 함께 복구 프로세스를 조정해야 합니다.

작업 부하에는 다음 복원 상태 중 하나가 있을 수 있습니다.

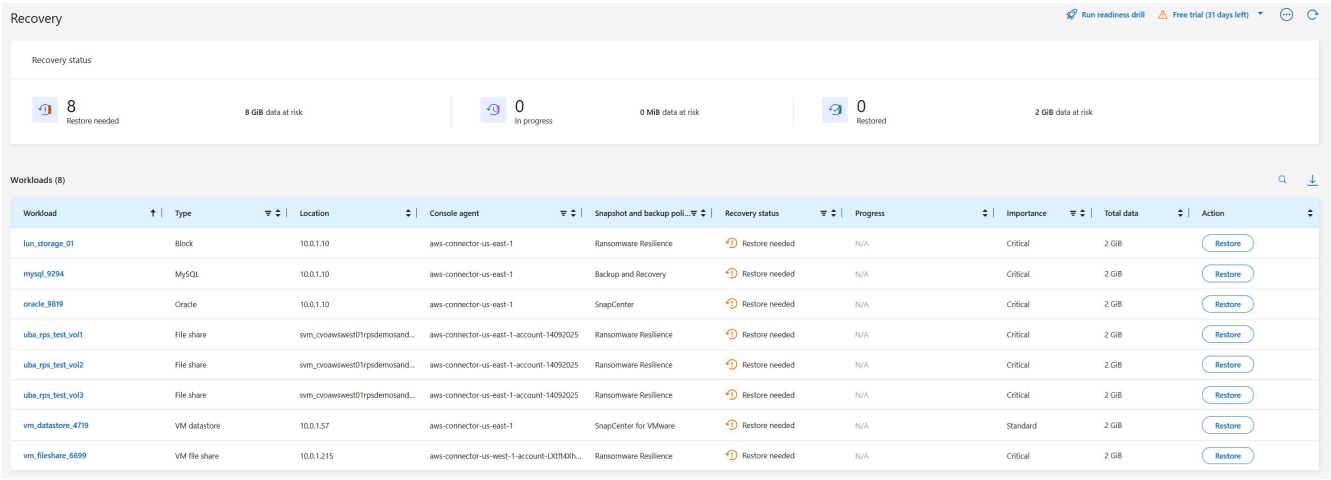
- 복구 필요: 작업 부하를 복구해야 합니다.
- 진행 중: 현재 복구 작업이 진행 중입니다.
- 복구됨: 작업 부하가 복구되었습니다.
- 실패: 작업 부하 복원 프로세스를 완료할 수 없습니다.

복구할 준비가 된 작업 부하 보기

"복원 필요" 복구 상태에 있는 워크로드를 검토합니다.

단계

1. 다음 중 하나를 수행하세요.
   - 대시보드에서 알림 창의 "복원 필요" 총계를 검토하고 *모두 보기*를 선택합니다.
   - 메뉴에서 *복구*를 선택합니다.
2. 복구 페이지에서 작업 부하 정보를 검토하세요.



SnapCenter 에서 관리하는 작업 부하 복원

랜섬웨어 복원력을 사용하면 스토리지 관리자는 권장 복원 지점이나 기본 복원 지점에서 워크로드를 복원하는 가장 좋은 방법을 결정할 수 있습니다.

복원이 필요한 경우 애플리케이션 상태가 변경됩니다. 백업에 제어 파일이 포함되어 있는 경우, 해당 제어 파일에서 애플리케이션이 이전 상태로 복원됩니다. 복원이 완료되면 애플리케이션이 읽기-쓰기 모드로 열립니다.

필수 콘솔 역할 이 작업을 수행하려면 조직 관리자, 폴더 또는 프로젝트 관리자, 랜섬웨어 복원력 관리자 역할이 필요합니다. "NetApp Console 의 랜섬웨어 복원력 역할에 대해 알아보세요" .

단계

1. 랜섬웨어 복원력에서 *복구*를 선택합니다.
2. 복구 페이지에서 작업 부하 정보를 검토하세요.
3. "복원 필요" 상태의 작업 부하를 선택하세요.
4. 복원하려면 *복원*을 선택하세요.
5. 복원 범위: 애플리케이션 일관성(또는 VM용 SnapCenter 의 경우 복원 범위는 "VM별")
6. 출처: 자세한 내용을 보려면 출처 옆에 있는 아래쪽 화살표를 선택하세요. 데이터를 복원하는 데 사용할 복원 지점을 선택하세요.

랜섬웨어 복원력은 사고 직전의 최신 백업을 최상의 복원 지점으로 식별하고 "권장" 표시를 표시합니다.

7. 목적지: 목적지 옆에 있는 아래쪽 화살표를 선택하면 자세한 내용을 볼 수 있습니다.
   a. 원래 위치나 대체 위치를 선택하세요.
   b. 시스템을 선택하세요.
   c. 저장소 VM을 선택합니다.
8. 원래 대상에 작업 부하를 복원할 충분한 공간이 없는 경우 "임시 저장소" 행이 나타납니다. 워크로드 데이터를 복원하기 위해 임시 저장소를 선택할 수 있습니다. 복구된 데이터는 임시 저장소에서 원래 위치로 복사됩니다. 임시 저장소 행에서 *아래쪽 화살표*를 클릭하고 대상 클러스터, 저장소 VM 및 로컬 계층을 설정합니다.
9. *저장*을 선택하세요.
10. *다음*을 선택하세요.
11. 선택 사항을 검토하세요.
12. *복원*을 선택하세요.
13. 상단 메뉴에서 *복구*를 선택하면 복구 페이지에서 작업 부하를 검토할 수 있습니다. 복구 페이지에서는 작업 상태가 여러 상태로 이동합니다.

SnapCenter 에서 관리하지 않는 작업 부하 복원

랜섬웨어 복원력을 사용하면 스토리지 관리자는 권장 복원 지점이나 기본 복원 지점에서 워크로드를 복원하는 가장 좋은 방법을 결정할 수 있습니다.

필수 콘솔 역할 이 작업을 수행하려면 조직 관리자, 폴더 또는 프로젝트 관리자, 랜섬웨어 복원력 관리자 역할이 필요합니다. "NetApp Console 의 랜섬웨어 복원력 역할에 대해 알아보세요" .

보안 스토리지 관리자는 다양한 수준에서 데이터를 복구할 수 있습니다.

- 모든 볼륨 복구
- 볼륨 수준이나 파일 및 폴더 수준에서 애플리케이션을 복구합니다.
- 볼륨 수준, 디렉토리 또는 파일/폴더 수준에서 파일 공유를 복구합니다.
- VM 수준에서 데이터 저장소로부터 복구합니다.

프로세스는 작업 유형에 따라 다릅니다.

단계

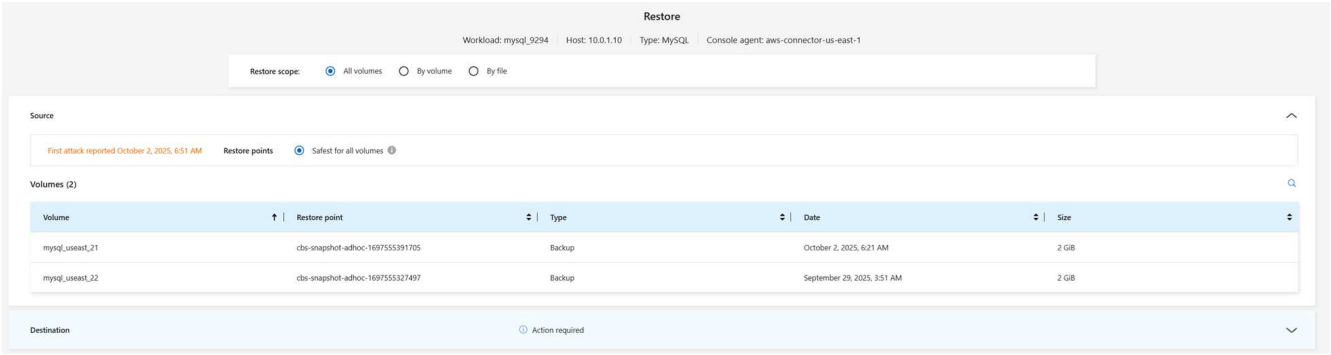
1. 랜섬웨어 복원력 메뉴에서 *복구*를 선택합니다.
2. 복구 페이지에서 작업 부하 정보를 검토하세요.
3. "복원 필요" 상태의 작업 부하를 선택하세요.
4. 복원하려면 *복원*을 선택하세요.
5. 복원 범위: 완료하려는 복원 유형을 선택하세요.
   - 모든 권
   - 볼륨별로
   - 파일별: 복원할 폴더나 단일 파일을 지정할 수 있습니다.

   SAN 워크로드의 경우 워크로드별로만 복원할 수 있습니다.

   최대 100개의 파일이나 하나의 폴더를 선택할 수 있습니다.
6. 애플리케이션, 볼륨 또는 파일 중 무엇을 선택했는지에 따라 다음 절차 중 하나를 계속 진행하세요.

모든 볼륨 복원

1. 랜섬웨어 복원력 메뉴에서 *복구*를 선택합니다.
2. "복원 필요" 상태의 작업 부하를 선택하세요.
3. 복원하려면 *복원*을 선택하세요.
4. 복원 페이지의 복원 범위에서 *모든 볼륨*을 선택합니다.



5. 출처: 자세한 내용을 보려면 출처 옆에 있는 아래쪽 화살표를 선택하세요.
   a. 데이터를 복원하는 데 사용할 복원 지점을 선택하세요.

   랜섬웨어 복원력은 사고 직전의 최신 백업을 최상의 복원 지점으로 식별하고 "모든 볼륨에 가장 안전함"이라는 표시를 보여줍니다. 즉, 첫 번째 볼륨에 대한 첫 번째 공격이 감지되기 전에 모든 볼륨이 복사본으로 복원된다는 의미입니다.
6. 목적지: 목적지 옆에 있는 아래쪽 화살표를 선택하면 자세한 내용을 볼 수 있습니다.
   a. 시스템을 선택하세요.

b. 저장소 VM을 선택합니다.

c. 집계를 선택하세요.

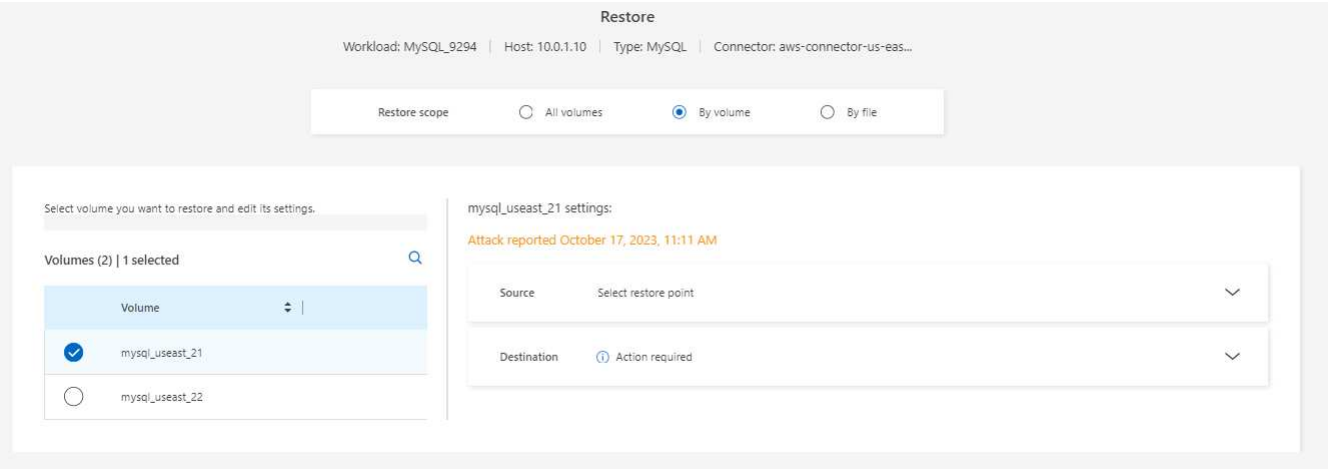
d. 모든 새 볼륨에 추가될 볼륨 접두사를 변경합니다.

새로운 볼륨 이름은 접두사 + 원래 볼륨 이름 + 백업 이름 + 백업 날짜로 표시됩니다.

7. *저장*을 선택하세요.
8. *다음*을 선택하세요.
9. 선택 사항을 검토하세요.
10. *복원*을 선택하세요.
11. 상단 메뉴에서 *복구*를 선택하면 복구 페이지에서 작업 부하를 검토할 수 있습니다. 복구 페이지에서는 작업 상태가 여러 상태로 이동합니다.

볼륨 수준에서 애플리케이션 작업 부하 복원

1. 랜섬웨어 복원력 메뉴에서 *복구*를 선택합니다.
2. "복원 필요" 상태의 애플리케이션 워크로드를 선택합니다.
3. 복원하려면 *복원*을 선택하세요.
4. 복원 페이지의 복원 범위에서 *볼륨별*을 선택합니다.



5. 볼륨 목록에서 복원하려는 볼륨을 선택합니다.
6. 출처: 자세한 내용을 보려면 출처 옆에 있는 아래쪽 화살표를 선택하세요.

a. 데이터를 복원하는 데 사용할 복원 지점을 선택하세요.

랜섬웨어 복원력은 사고 직전의 최신 백업을 최상의 복원 지점으로 식별하고 "권장" 표시를 표시합니다.

7. 목적지: 목적지 옆에 있는 아래쪽 화살표를 선택하면 자세한 내용을 볼 수 있습니다.

a. 시스템을 선택하세요.

b. 저장소 VM을 선택합니다.

c. 집계를 선택하세요.

d. 새로운 볼륨 이름을 검토합니다.

새로운 볼륨 이름은 원래 볼륨 이름 + 백업 이름 + 백업 날짜로 표시됩니다.

8. *저장*을 선택하세요.
9. *다음*을 선택하세요.
10. 선택 사항을 검토하세요.
11. *복원*을 선택하세요.
12. 상단 메뉴에서 *복구*를 선택하면 복구 페이지에서 작업 부하를 검토할 수 있습니다. 복구 페이지에서는 작업 상태가 여러 상태로 이동합니다.

파일 수준에서 애플리케이션 작업 부하 복원

파일 수준에서 애플리케이션 워크로드를 복원하기 전에 영향을 받은 파일 목록을 볼 수 있습니다. 영향을 받은 파일 목록을 다운로드하려면 알림 페이지에 접속하세요. 그런 다음 복구 페이지를 사용하여 목록을 업로드하고 복원할 파일을 선택합니다.

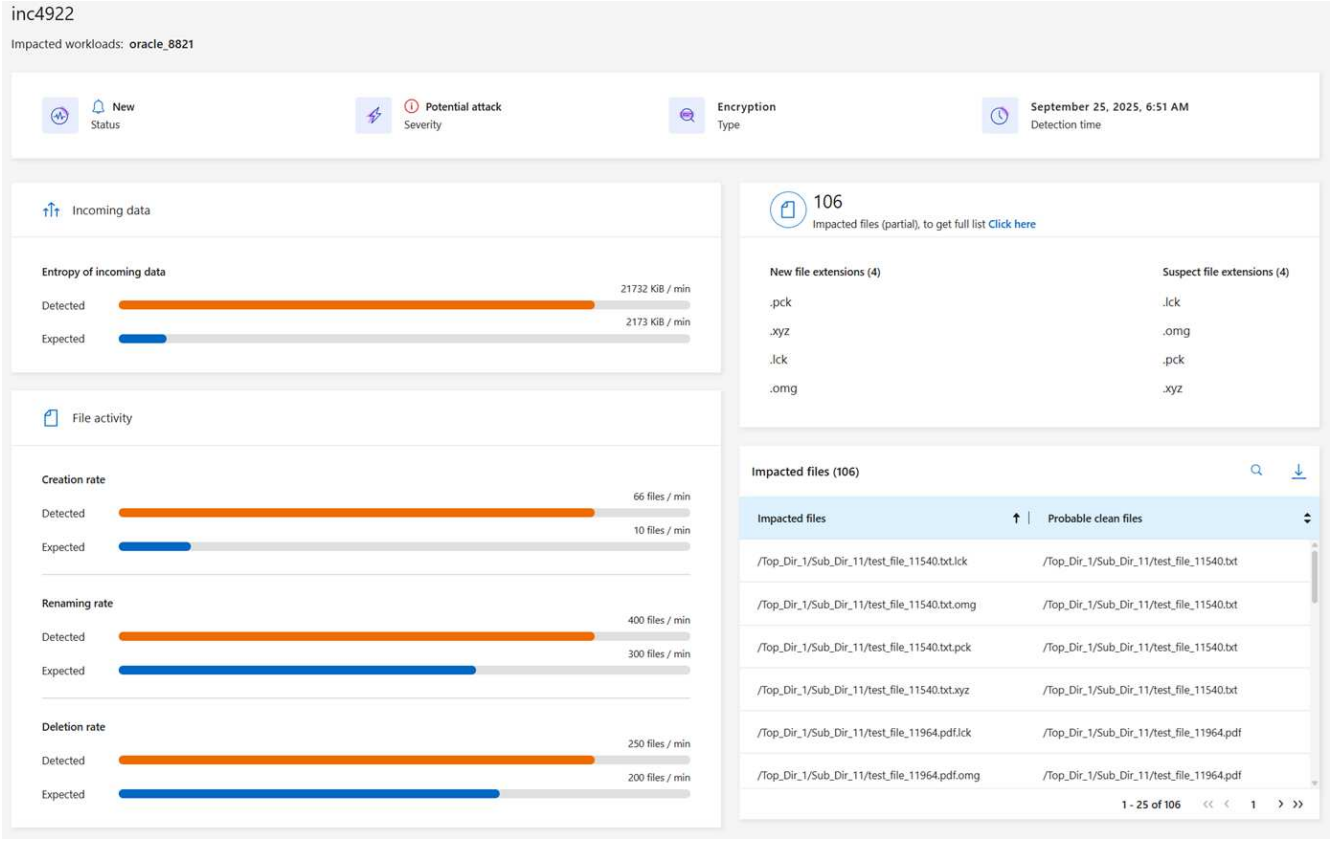
파일 수준에서 애플리케이션 작업 부하를 동일하거나 다른 시스템으로 복원할 수 있습니다.

영향을 받은 파일 목록을 얻는 단계

알림 페이지를 사용하여 영향을 받은 파일 목록을 검색하세요.

볼륨에 여러 개의 알림이 있는 경우 각 알림에 대해 영향을 받는 파일의 CSV 목록을 다운로드해야 합니다.

1. 랜섬웨어 복원력 메뉴에서 *알림*을 선택합니다.
2. 알림 페이지에서 결과를 작업 부하별로 정렬하여 복원하려는 애플리케이션 작업 부하에 대한 알림을 표시합니다.
3. 해당 작업 부하에 대한 알림 목록에서 알림을 선택합니다.
4. 해당 알림에 대해 단일 사건을 선택하세요.



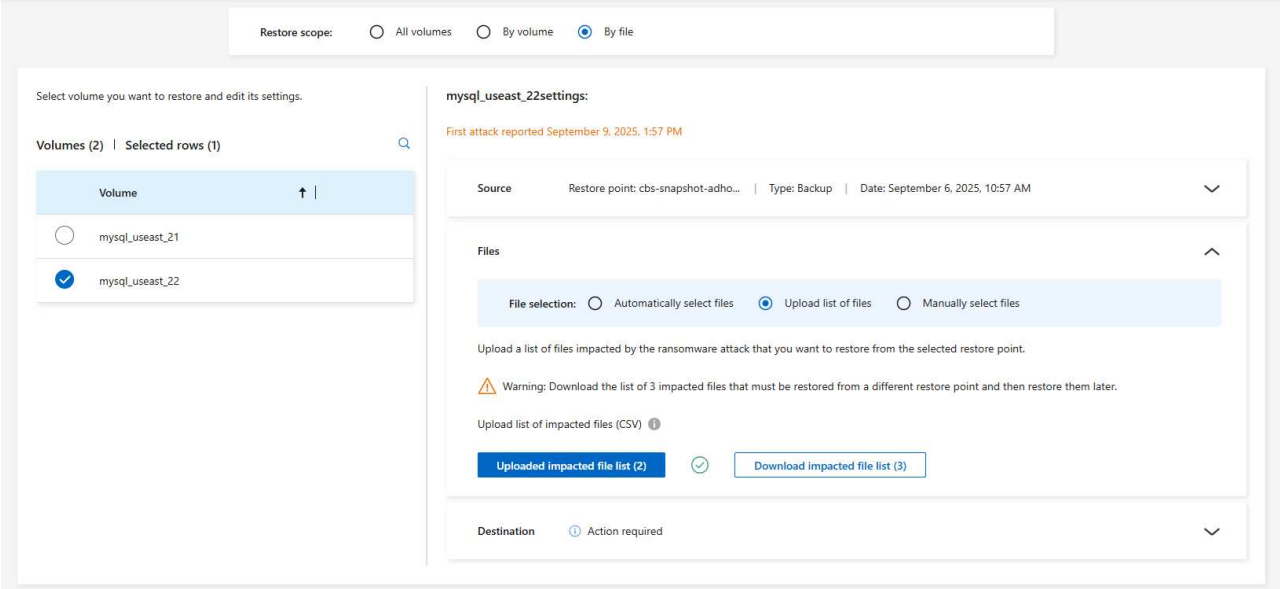
5. 전체 파일 목록을 보려면 영향을 받은 파일 창 상단에 있는 *여기를 클릭*을 선택하세요.
6. 해당 사건에 대해 다운로드 아이콘을 선택하고 영향을 받은 파일 목록을 CSV 형식으로 다운로드하세요.

해당 파일을 복원하는 단계

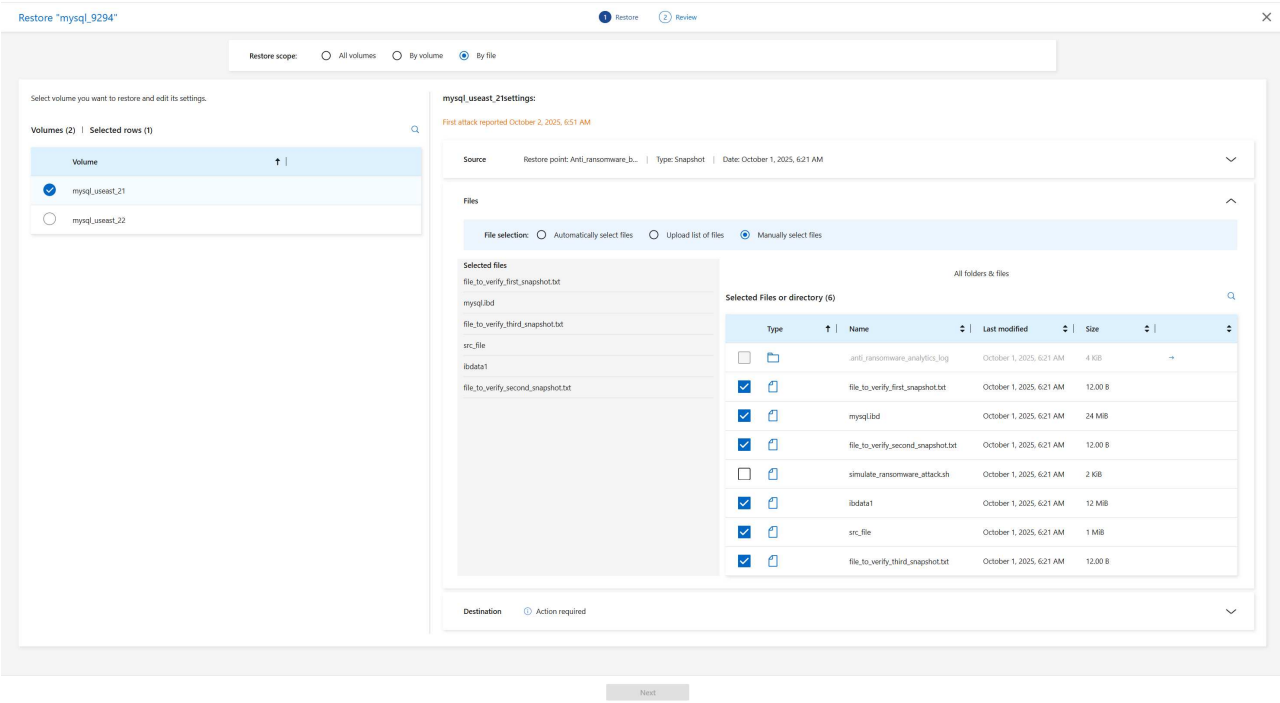
1. 랜섬웨어 복원력 메뉴에서 *복구*를 선택합니다.
2. "복원 필요" 상태의 애플리케이션 워크로드를 선택합니다.
3. 복원하려면 *복원*을 선택하세요.
4. 복원 페이지의 복원 범위에서 *파일별*을 선택합니다.
5. 볼륨 목록에서 복원하려는 파일이 들어 있는 볼륨을 선택합니다.
6. 복원 지점: 자세한 내용을 보려면 복원 지점 옆에 있는 아래쪽 화살표를 선택하세요. 데이터를 복원하는 데 사용할 복원 지점을 선택하세요.

> 복원 지점 창의 이유 열에는 스냅샷 또는 백업의 이유가 "예약됨" 또는 "랜섬웨어 사고에 대한 자동 대응"으로 표시됩니다.

7. 파일:
   - 자동으로 파일 선택: Ransomware Resilience가 복구할 파일을 선택하도록 합니다.
   - 파일 목록 업로드: 알림 페이지에서 받았거나 본인이 가지고 있는 영향을 받은 파일 목록이 포함된 CSV 파일을 업로드하세요. 한 번에 최대 10,000개의 파일을 복원할 수 있습니다.



◦ 수동으로 파일 선택: 최대 10,000개의 파일이나 단일 폴더를 선택하여 복원합니다.



선택한 복원 지점을 사용하여 복원할 수 없는 파일이 있는 경우 복원할 수 없는 파일 수를 나타내는 메시지가 나타나고 *영향을 받은 파일 목록 다운로드*를 선택하여 해당 파일 목록을 다운로드할 수 있습니다.

8. 목적지: 목적지 옆에 있는 아래쪽 화살표를 선택하면 자세한 내용을 볼 수 있습니다.
   a. 데이터를 복원할 위치를 선택합니다. 원래 위치 또는 사용자가 지정할 수 있는 대체 위치입니다.

원본 파일이나 디렉토리는 복원된 데이터로 덮어쓰여지지만, 새 이름을 지정하지 않는 한 원본 파일과 폴더 이름은 동일하게 유지됩니다.

b. 시스템을 선택하세요.

c. 저장소 VM을 선택합니다.

d. 선택적으로 경로를 입력하세요.

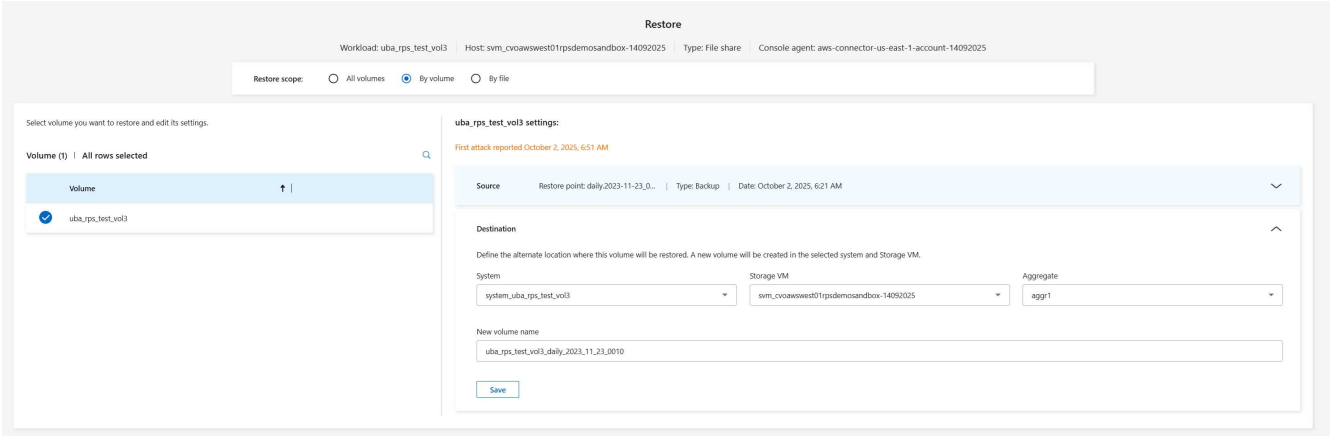
> 복원 경로를 지정하지 않으면 파일은 최상위 디렉토리의 새 볼륨에 복원됩니다.

e. 복원된 파일이나 디렉토리의 이름을 현재 위치와 같은 이름으로 할지, 아니면 다른 이름으로 할지 선택합니다.

9. *다음*을 선택하세요.
10. 선택 사항을 검토하세요.
11. *복원*을 선택하세요.
12. 상단 메뉴에서 *복구*를 선택하면 복구 페이지에서 작업 부하를 검토할 수 있습니다. 복구 페이지에서는 작업 상태가 여러 상태로 이동합니다.

파일 공유 또는 데이터 저장소 복원

1. 복원할 파일 공유 또는 데이터 저장소를 선택한 후 복원 페이지의 복원 범위에서 *볼륨별*을 선택합니다.



2. 볼륨 목록에서 복원하려는 볼륨을 선택합니다.
3. 출처: 자세한 내용을 보려면 출처 옆에 있는 아래쪽 화살표를 선택하세요.

a. 데이터를 복원하는 데 사용할 복원 지점을 선택하세요.

> 랜섬웨어 복원력은 사고 직전의 최신 백업을 최상의 복원 지점으로 식별하고 "권장" 표시를 표시합니다.

4. 목적지: 목적지 옆에 있는 아래쪽 화살표를 선택하면 자세한 내용을 볼 수 있습니다.

a. 데이터를 복원할 위치를 선택합니다. 원래 위치 또는 사용자가 지정할 수 있는 대체 위치입니다.

> 원본 파일이나 디렉토리는 복원된 데이터로 덮어쓰여지지만, 새 이름을 지정하지 않는 한 원본 파일과 폴더 이름은 동일하게 유지됩니다.

b. 시스템을 선택하세요.

c. 저장소 VM을 선택합니다.

d. 선택적으로 경로를 입력하세요.

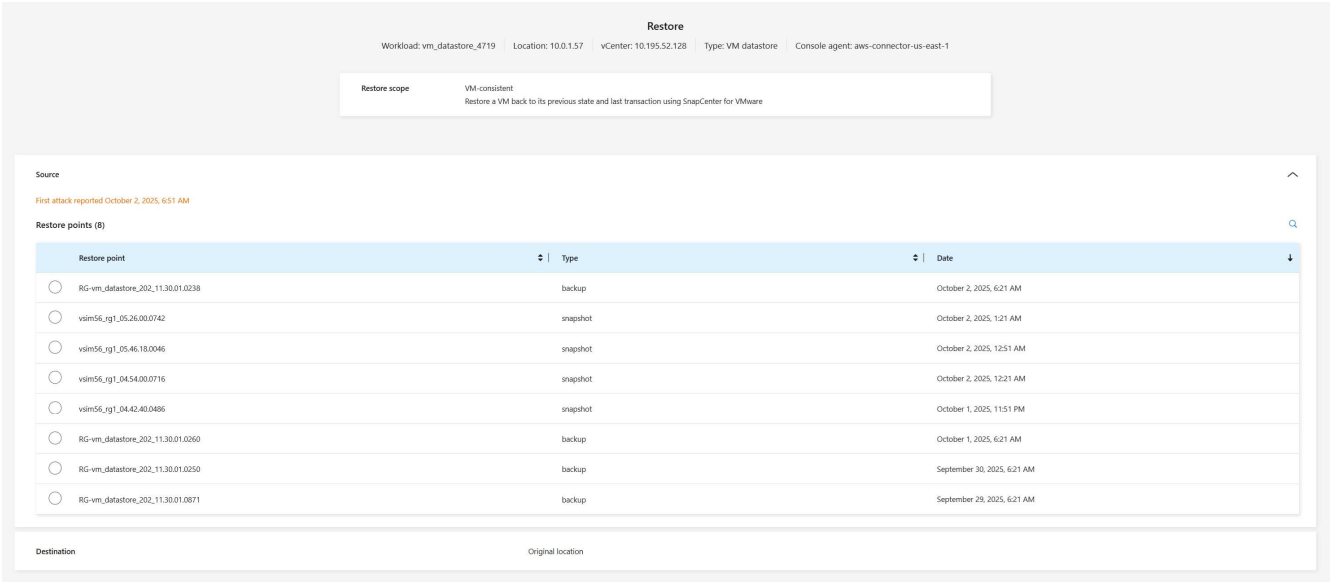
복원 경로를 지정하지 않으면 파일은 최상위 디렉토리의 새 볼륨에 복원됩니다.

5. *저장*을 선택하세요.
6. 선택 사항을 검토하세요.
7. *복원*을 선택하세요.
8. 메뉴에서 *복구*를 선택하면 복구 페이지에서 작업 부하를 검토할 수 있습니다. 복구 페이지에서는 작업 상태가 여러 상태로 이동합니다.

VM 수준에서 **VM** 파일 공유 복원

복원할 VM을 선택한 후 복구 페이지에서 다음 단계를 계속 진행합니다.

1. 출처: 자세한 내용을 보려면 출처 옆에 있는 아래쪽 화살표를 선택하세요.



2. 데이터를 복원하는 데 사용할 복원 지점을 선택하세요.
3. 목적지: 원래 위치로.
4. *다음*을 선택하세요.
5. 선택 사항을 검토하세요.
6. *복원*을 선택하세요.
7. 메뉴에서 *복구*를 선택하면 복구 페이지에서 작업 부하를 검토할 수 있습니다. 복구 페이지에서는 작업 상태가 여러 상태로 이동합니다.

NetApp Ransomware Resilience 보고서 다운로드

보호 데이터를 내보내고 공격 준비 훈련, 보호, 알림 및 복구에 대한 세부 정보를 보여주는 CSV 또는 JSON 파일을 다운로드할 수 있습니다.

파일을 다운로드하기 전에 데이터를 새로 고쳐야 합니다. 그러면 파일에 표시되는 데이터도 새로 고쳐집니다.

필수 콘솔 역할 이 작업을 수행하려면 조직 관리자, 폴더 또는 프로젝트 관리자, 랜섬웨어 복원력 관리자 또는 랜섬웨어 복원력 뷰어 역할이 필요합니다. "NetApp Console 의 랜섬웨어 복원력 역할에 대해 알아보세요" .

어떤 데이터를 다운로드할 수 있나요**?** 다음 메인 메뉴 옵션에서 파일을 다운로드할 수 있습니다.

- 보호: 보호되는 총 작업 수와 위험에 처한 총 작업 수를 포함하여 모든 작업의 상태와 세부 정보가 포함됩니다.
- 알림: 모든 알림의 상태와 세부 정보, 총 알림 수 및 자동 스냅샷이 포함됩니다.
- 복구: 복원이 필요한 모든 작업 부하의 상태와 세부 정보가 포함됩니다. 여기에는 "복원 필요", "진행 중", "복원 실패" 및 "복원 성공"으로 표시된 작업 부하의 총 수가 포함됩니다.
- 보고서: 모든 페이지에서 데이터를 내보내고 파일을 다운로드할 수 있습니다.

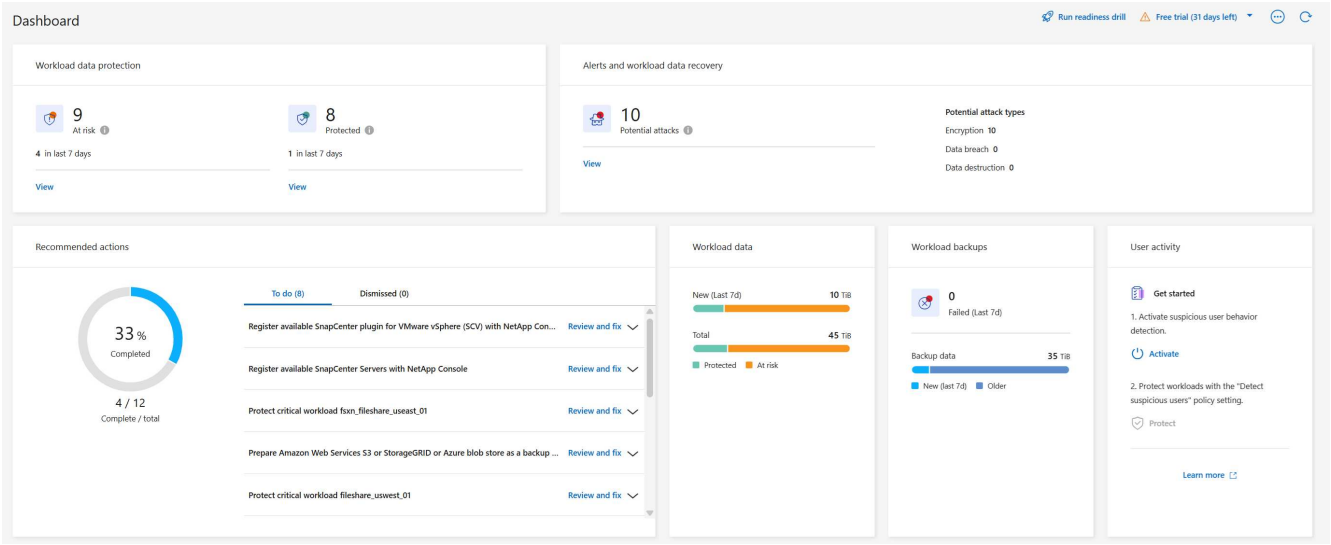
  준비 훈련 보고서는 보고서 페이지에서만 다운로드할 수 있습니다.

보호, 알림 또는 복구 페이지에서 CSV 또는 JSON 파일을 다운로드하는 경우 해당 페이지의 데이터만 표시됩니다.

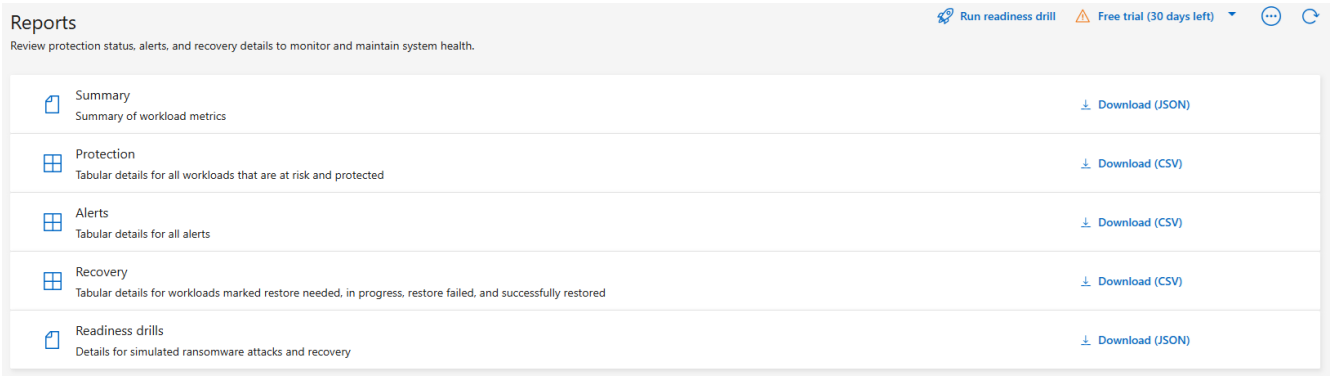
CSV 또는 JSON 파일에는 모든 콘솔 시스템의 모든 워크로드에 대한 데이터가 포함되어 있습니다.

단계

1. 콘솔 왼쪽 탐색에서 보호 > *랜섬웨어 복원력*을 선택합니다.



2. 대시보드 또는 다른 페이지에서 *새로 고침*을 선택하세요. 보고서에 표시될 데이터를 새로 고치려면 오른쪽 상단의 옵션을 선택하세요.
3. 다음 중 하나를 수행하세요.
   - 해당 페이지에서 *다운로드*를 선택하세요 옵션.
   - NetApp Ransomware Resilience 메뉴에서 *보고서*를 선택합니다.
4. 보고서 옵션을 선택한 경우 미리 구성된 파일 이름 중 하나를 선택하고 *다운로드*를 선택합니다.


Reports
Review protection status, alerts, and recovery details to monitor and maintain system health.
Run readiness drill
Free trial (30 days left)
Summary
Summary of workload metrics
Download (JSON)
Protection
Tabular details for all workloads that are at risk and protected
Download (CSV)
Alerts
Tabular details for all alerts
Download (CSV)
Recovery
Tabular details for workloads marked restore needed, in progress, restore failed, and successfully restored
Download (CSV)
Readiness drills
Details for simulated ransomware attacks and recovery
Download (JSON)

지식과 지원

지원 등록

BlueXP 와 해당 스토리지 솔루션 및 서비스에 대한 기술 지원을 받으려면 지원 등록이 필요합니다. Cloud Volumes ONTAP 시스템의 주요 워크플로를 활성화하려면 지원 등록도 필요합니다.

지원에 등록해도 클라우드 공급자 파일 서비스에 대한 NetApp 지원은 제공되지 않습니다. 클라우드 공급자 파일 서비스, 해당 인프라 또는 서비스를 사용하는 솔루션과 관련된 기술 지원에 대해서는 해당 제품의 BlueXP 설명서에서 "도움말 받기"를 참조하세요.

- "ONTAP 용 Amazon FSx"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

지원 등록 개요

지원 자격을 활성화하기 위한 등록 방법은 두 가지가 있습니다.

- BlueXP 계정 일련 번호를 등록합니다(BlueXP 의 지원 리소스 페이지에 있는 20자리 960xxxxxxxxx 일련 번호).

  이는 BlueXP 내의 모든 서비스에 대한 단일 지원 구독 ID 역할을 합니다. 각 BlueXP 계정 수준 지원 구독을 등록해야 합니다.

- 클라우드 공급업체의 마켓플레이스에서 구독과 관련된 Cloud Volumes ONTAP 일련 번호를 등록합니다(20자리 909201xxxxxxxx 일련 번호).

  이러한 일련 번호는 일반적으로 _PAYGO 일련 번호_라고 하며 Cloud Volumes ONTAP 배포 시 BlueXP 에서 생성됩니다.

두 가지 유형의 일련 번호를 모두 등록하면 지원 티켓 개설 및 자동 사례 생성과 같은 기능을 사용할 수 있습니다. 아래 설명된 대로 BlueXP 에 NetApp 지원 사이트(NSS) 계정을 추가하여 등록을 완료합니다.

NetApp 지원을 위해 **BlueXP** 등록

지원을 등록하고 지원 자격을 활성화하려면 BlueXP 조직(또는 계정)의 한 사용자가 NetApp 지원 사이트 계정을 BlueXP 로그인과 연결해야 합니다. NetApp 지원에 등록하는 방법은 NetApp 지원 사이트(NSS) 계정이 있는지 여부에 따라 달라집니다.

NSS 계정이 있는 기존 고객

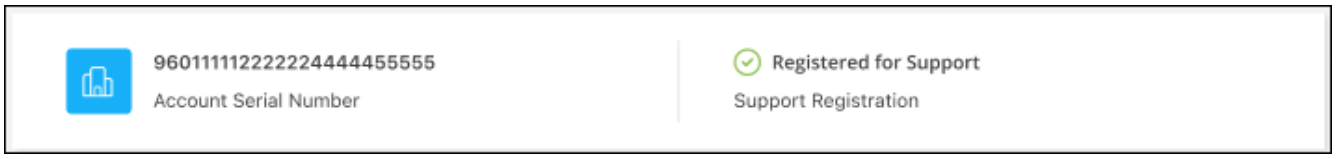
NSS 계정이 있는 NetApp 고객이라면 BlueXP 통해 지원을 받기 위해 등록하기만 하면 됩니다.

단계

1. BlueXP 콘솔의 오른쪽 상단에서 설정 아이콘을 선택하고 *자격 증명*을 선택합니다.
2. *사용자 자격 증명*을 선택하세요.

3. *NSS 자격 증명 추가*를 선택하고 NetApp 지원 사이트(NSS) 인증 프롬프트를 따릅니다.
4. 등록 과정이 성공적으로 완료되었는지 확인하려면 도움말 아이콘을 선택하고 *지원*을 선택하세요.

   리소스 페이지에는 귀하의 BlueXP 조직이 지원을 위해 등록되어 있다는 것이 표시되어야 합니다.



   다른 BlueXP 사용자는 NetApp 지원 사이트 계정을 BlueXP 로그인과 연결하지 않은 경우 이와 동일한 지원 등록 상태를 볼 수 없습니다. 하지만 그렇다고 해서 BlueXP 조직이 지원에 등록되지 않았다는 의미는 아닙니다. 조직 내 한 명의 사용자가 이러한 단계를 따랐다면 귀하의 조직은 등록된 것입니다.

기존 고객이지만 **NSS** 계정이 없습니다**.**

기존 라이선스와 일련 번호는 있지만 NSS 계정이 없는 기존 NetApp 고객인 경우 NSS 계정을 만들고 BlueXP 로그인과 연결해야 합니다.

단계

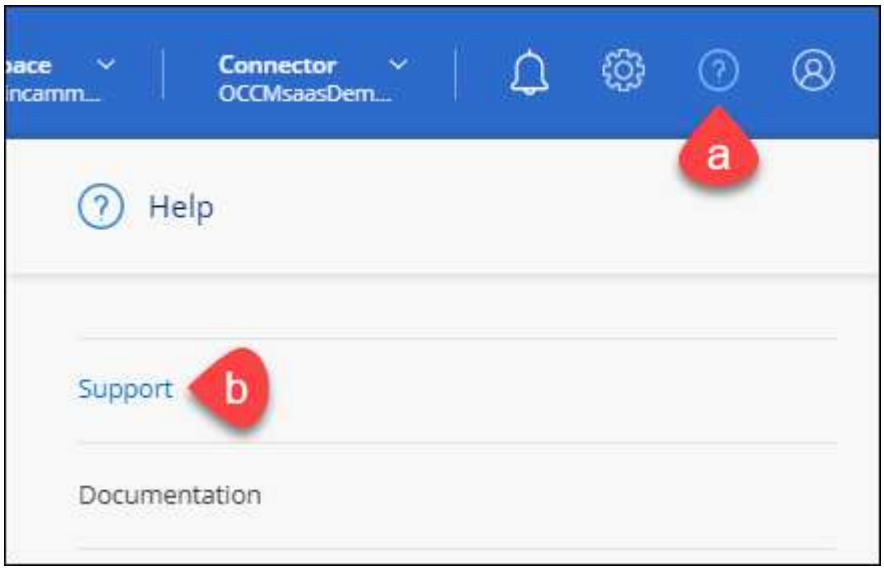
1. 다음을 완료하여 NetApp 지원 사이트 계정을 만드십시오. "NetApp 지원 사이트 사용자 등록 양식"
   a. 일반적으로 * NetApp 고객/최종 사용자*인 적절한 사용자 수준을 선택하세요.
   b. 위에 사용된 BlueXP 계정 일련번호(960xxxx)를 일련번호 필드에 꼭 복사해 두세요. 이렇게 하면 계정 처리가 빨라집니다.
2. 다음 단계를 완료하여 새 NSS 계정을 BlueXP 로그인과 연결하세요.NSS 계정이 있는 기존 고객 .

NetApp 의 새로운 기능

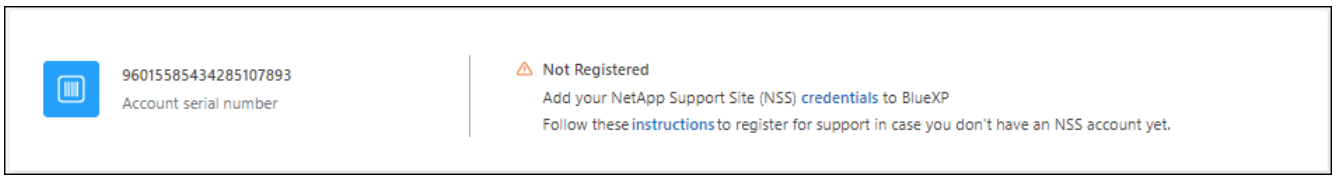
NetApp 처음 사용하시고 NSS 계정이 없으신 경우 아래의 각 단계를 따르세요.

단계

1. BlueXP 콘솔의 오른쪽 상단에서 도움말 아이콘을 선택하고 *지원*을 선택하세요.



2. 지원 등록 페이지에서 계정 ID 일련 번호를 찾으세요.



3. 로 이동 "NetApp 지원 등록 사이트" *저는 등록된 NetApp 고객이 아닙니다*를 선택하세요.
4. 필수 입력란(빨간색 별표가 있는 항목)을 작성해 주세요.
5. 제품군 필드에서 *클라우드 관리자*를 선택한 다음 해당 청구 제공자를 선택하세요.
6. 위의 2단계에서 계정 일련번호를 복사하고 보안 검사를 완료한 다음 NetApp의 글로벌 데이터 개인정보 보호정책을 읽었는지 확인하세요.

   이 안전한 거래를 마무리하기 위해 제공된 사서함으로 이메일이 즉시 전송됩니다. 몇 분 안에 인증 이메일이 도착하지 않으면 스팸 폴더를 확인하세요.

7. 이메일 내에서 작업을 확인하세요.

   확인을 클릭하면 귀하의 요청이 NetApp 에 제출되고 NetApp 지원 사이트 계정을 만드는 것이 좋습니다.

8. 다음을 완료하여 NetApp 지원 사이트 계정을 만드십시오. "NetApp 지원 사이트 사용자 등록 양식"
   a. 일반적으로 * NetApp 고객/최종 사용자*인 적절한 사용자 수준을 선택하세요.
   b. 위에 사용된 계정 일련번호(960xxxx)를 일련번호 필드에 꼭 복사해 두세요. 이렇게 하면 처리 속도가 빨라집니다.

당신이 완료한 후

이 과정에서 NetApp 귀하에게 연락을 드릴 것입니다. 이는 신규 사용자를 대상으로 한 일회성 온보딩 과정입니다.

NetApp 지원 사이트 계정이 있으면 아래 단계를 완료하여 계정을 BlueXP 로그인과 연결하세요.NSS 계정이 있는 기존 고객 .

Cloud Volumes ONTAP 지원을 위한 NSS 자격 증명 연결

Cloud Volumes ONTAP 에 대한 다음과 같은 주요 워크플로를 활성화하려면 NetApp 지원 사이트 자격 증명을 BlueXP 조직과 연결해야 합니다.

- 지원을 위해 Pay-as-you-go Cloud Volumes ONTAP 시스템 등록

  시스템 지원을 활성화하고 NetApp 기술 지원 리소스에 액세스하려면 NSS 계정을 제공해야 합니다.

- BYOL(Bring Your Own License)을 사용할 때 Cloud Volumes ONTAP 배포

  BlueXP 귀하의 라이선스 키를 업로드하고 귀하가 구매한 기간 동안 구독을 활성화하려면 귀하의 NSS 계정을 제공하는 것이 필요합니다. 여기에는 기간 갱신을 위한 자동 업데이트가 포함됩니다.

- Cloud Volumes ONTAP 소프트웨어를 최신 릴리스로 업그레이드

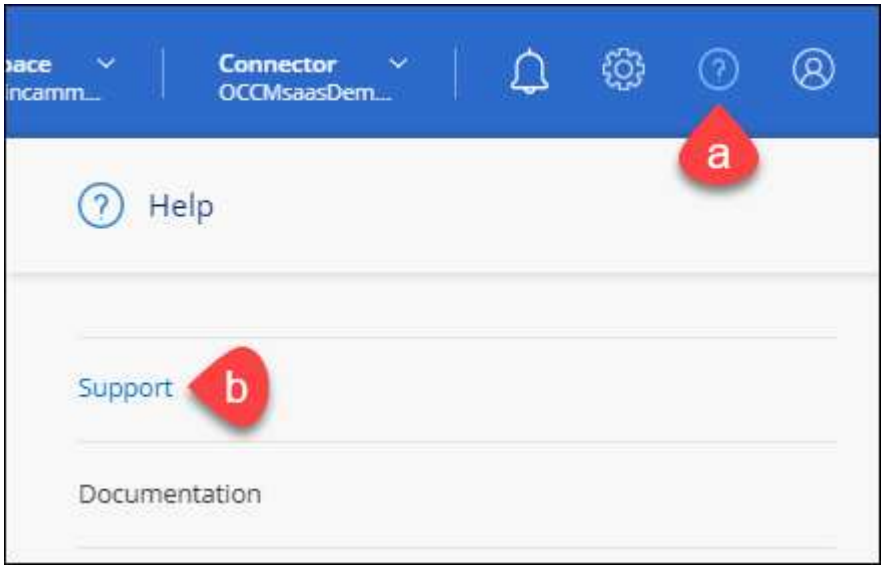
NSS 자격 증명을 BlueXP 조직에 연결하는 것은 BlueXP 사용자 로그인에 연결된 NSS 계정과 다릅니다.

이러한 NSS 자격 증명은 특정 BlueXP 조직 ID와 연결됩니다. BlueXP 조직에 속한 사용자는 *지원 > NSS 관리*에서 이러한 자격 증명에 액세스할 수 있습니다.

- 고객 수준 계정이 있는 경우 하나 이상의 NSS 계정을 추가할 수 있습니다.
- 파트너 또는 리셀러 계정이 있는 경우 하나 이상의 NSS 계정을 추가할 수 있지만 고객 수준 계정과 함께 추가할 수는 없습니다.

단계

1. BlueXP 콘솔의 오른쪽 상단에서 도움말 아이콘을 선택하고 *지원*을 선택하세요.



2. *NSS 관리 > NSS 계정 추가*를 선택하세요.
3. 메시지가 표시되면 *계속*을 선택하여 Microsoft 로그인 페이지로 이동합니다.

   NetApp 지원 및 라이선싱에 특화된 인증 서비스를 위한 ID 공급자로 Microsoft Entra ID를 사용합니다.

4. 로그인 페이지에서 NetApp 지원 사이트에 등록된 이메일 주소와 비밀번호를 입력하여 인증 과정을 진행합니다.

   이러한 작업을 통해 BlueXP 라이선스 다운로드, 소프트웨어 업그레이드 확인, 향후 지원 등록과 같은 작업에 NSS 계정을 사용할 수 있습니다.

   다음 사항에 유의하세요.

   - NSS 계정은 고객 수준 계정이어야 합니다(게스트나 임시 계정이어서는 안 됩니다). 여러 개의 고객 수준 NSS 계정을 가질 수 있습니다.
   - 해당 계정이 파트너 수준 계정인 경우 NSS 계정은 하나만 있을 수 있습니다. 고객 수준 NSS 계정을 추가하려고 하는데 파트너 수준 계정이 이미 있는 경우 다음과 같은 오류 메시지가 표시됩니다.

     "이 계정에는 다른 유형의 NSS 사용자가 이미 있으므로 NSS 고객 유형이 허용되지 않습니다."

   기존 고객 수준 NSS 계정이 있고 파트너 수준 계정을 추가하려는 경우에도 마찬가지입니다.

   - 로그인에 성공하면 NetApp NSS 사용자 이름을 저장합니다.

     이는 귀하의 이메일에 매핑되는 시스템 생성 ID입니다. **NSS** 관리 페이지에서 이메일을 표시할 수 있습니다. •••

메뉴.

- 로그인 자격 증명 토큰을 새로 고쳐야 하는 경우 자격 증명 업데이트 옵션도 있습니다. ••• 메뉴.

  이 옵션을 사용하면 다시 로그인하라는 메시지가 표시됩니다. 이 계정의 토큰은 90일 후에 만료됩니다. 이에 대한 알림이 게시됩니다.

도움을 받으세요

NetApp BlueXP 와 클라우드 서비스에 대한 다양한 지원을 제공합니다. 지식 베이스(KB) 문서 및 커뮤니티 포럼 등 다양한 무료 셀프 지원 옵션을 연중무휴 24시간 이용하실 수 있습니다. 지원 등록 시 웹 티켓팅을 통한 원격 기술 지원이 제공됩니다.

클라우드 공급자 파일 서비스에 대한 지원을 받으세요

클라우드 공급자 파일 서비스, 해당 인프라 또는 서비스를 사용하는 솔루션과 관련된 기술 지원에 대해서는 해당 제품의 BlueXP 설명서에서 "도움말 받기"를 참조하세요.

- "ONTAP 용 Amazon FSx"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

BlueXP 와 해당 스토리지 솔루션 및 서비스에 대한 구체적인 기술 지원을 받으려면 아래에 설명된 지원 옵션을 이용하세요.

셀프 지원 옵션 사용

다음 옵션은 주 7일, 하루 24시간 무료로 이용 가능합니다.

- 설명서

  현재 보고 있는 BlueXP 문서입니다.

- "지식 기반"

  BlueXP 지식 기반을 검색하여 문제 해결에 도움이 되는 문서를 찾아보세요.

- "커뮤니티"

  현재 진행 중인 토론을 팔로우하거나 새로운 토론을 만들려면 BlueXP 커뮤니티에 가입하세요.

NetApp 지원을 통해 사례 만들기

위에 나열된 셀프 지원 옵션 외에도, 지원을 활성화한 후 NetApp 지원 전문가와 협력하여 문제를 해결할 수 있습니다.

시작하기 전에

- 사례 만들기 기능을 사용하려면 먼저 NetApp 지원 사이트 자격 증명을 BlueXP 로그인과 연결해야 합니다. "BlueXP 로그인과 관련된 자격 증명을 관리하는 방법을 알아보세요." .

- 일련 번호가 있는 ONTAP 시스템에 대한 사례를 개설하는 경우 NSS 계정은 해당 시스템의 일련 번호와 연결되어야 합니다.

단계

1. BlueXP 에서 *도움말 > 지원*을 선택하세요.
2. 리소스 페이지에서 기술 지원 아래에 있는 사용 가능한 옵션 중 하나를 선택하세요.

   a. 전화로 상담원과 통화하고 싶으시면 *전화하기*를 선택하세요. netapp.com에서 전화할 수 있는 전화번호가 나열된 페이지로 이동하게 됩니다.

   b. NetApp 지원 전문가에게 티켓을 열려면 *사례 만들기*를 선택하세요.

      - 서비스: 문제와 관련된 서비스를 선택하세요. 예를 들어, BlueXP 서비스 내의 워크플로나 기능에 대한 기술 지원 문제에 특화되어 있습니다.
      - 작업 환경: 스토리지에 해당되는 경우 * Cloud Volumes ONTAP* 또는 *온프레미스*를 선택한 다음 연관된 작업 환경을 선택합니다.

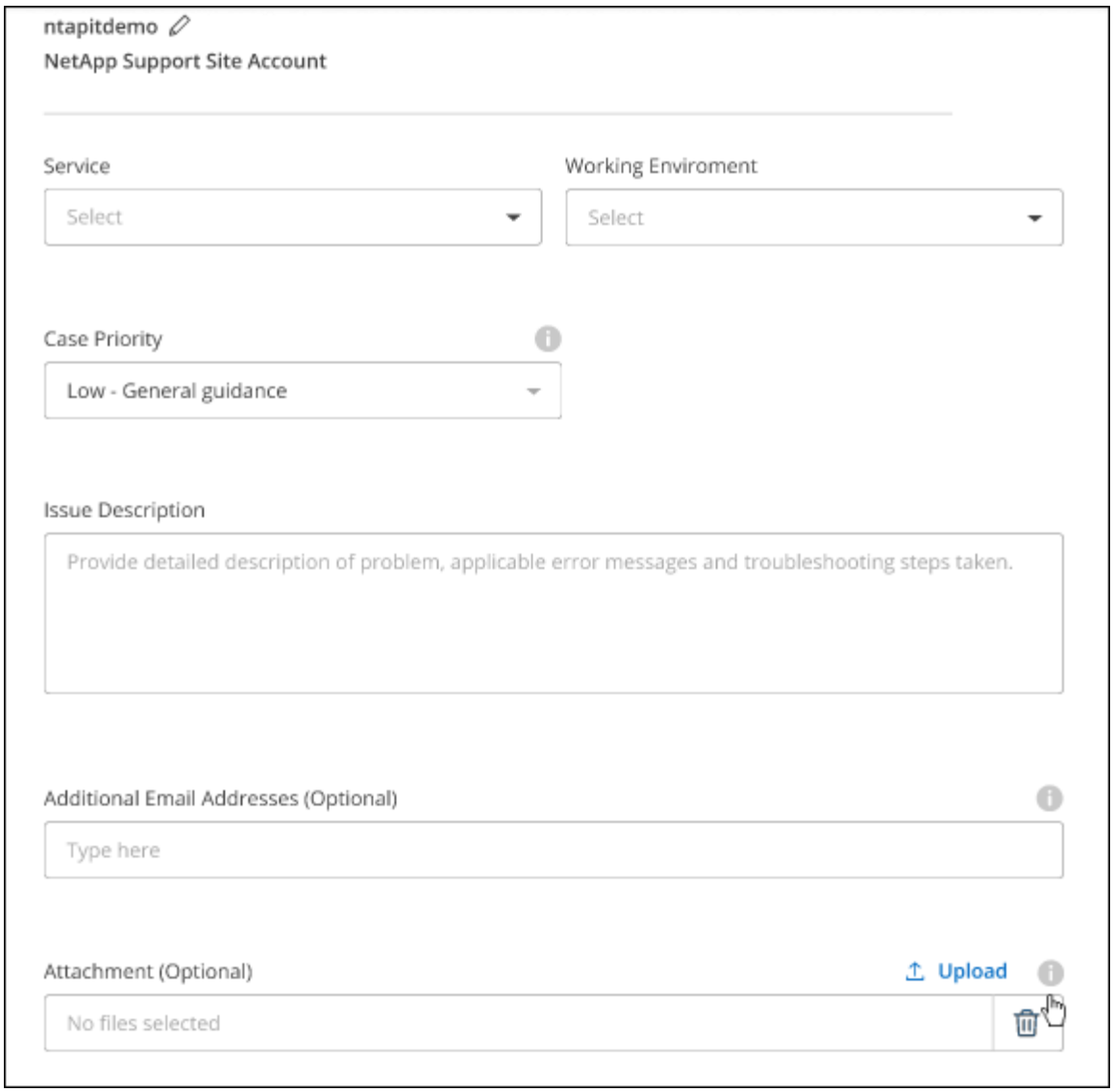
        작업 환경 목록은 서비스의 상단 배너에서 선택한 BlueXP 조직(또는 계정), 프로젝트(또는 작업 공간) 및 커넥터의 범위 내에 있습니다.

      - 사례 우선순위: 낮음, 보통, 높음 또는 중요로 사례의 우선순위를 선택합니다.

        이러한 우선순위에 대한 자세한 내용을 알아보려면 필드 이름 옆에 있는 정보 아이콘 위에 마우스를 올려놓으세요.

      - 문제 설명: 해당 오류 메시지나 수행한 문제 해결 단계를 포함하여 문제에 대한 자세한 설명을 제공하세요.
      - 추가 이메일 주소: 이 문제를 다른 사람에게 알리려면 추가 이메일 주소를 입력하세요.
      - 첨부파일(선택사항): 최대 5개의 첨부파일을 한 번에 하나씩 업로드하세요.

        첨부파일은 파일당 25MB로 제한됩니다. 다음 파일 확장자가 지원됩니다: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx, csv.



당신이 완료한 후

지원 사례 번호가 포함된 팝업이 나타납니다. NetApp 지원 전문가가 귀하의 사례를 검토하고 곧 연락드릴 것입니다.

지원 사례 기록을 보려면 *설정 > 타임라인*을 선택하고 "지원 사례 만들기"라는 이름의 작업을 찾으세요. 가장 오른쪽에 있는 버튼을 누르면 동작을 확장하여 자세한 내용을 볼 수 있습니다.

사례를 생성하려고 할 때 다음과 같은 오류 메시지가 나타날 수 있습니다.

"선택한 서비스에 대해 사례를 생성할 권한이 없습니다."

이 오류는 NSS 계정과 해당 계정과 연결된 기록상 회사가 BlueXP 계정 일련 번호에 대한 기록상 회사와 동일하지 않다는 것을 의미할 수 있습니다(예: 960xxxx) 또는 작업 환경 일련 번호. 다음 옵션 중 하나를 사용하여 도움을 요청할 수 있습니다.

- 제품 내 채팅을 사용하세요
- 비기술적 사례를 제출하세요 https://mysupport.netapp.com/site/help

지원 사례 관리(미리 보기)

BlueXP 에서 직접 활성화된 지원 사례와 해결된 지원 사례를 보고 관리할 수 있습니다. 귀하의 NSS 계정 및 회사와 관련된 사례를 관리할 수 있습니다.

사례 관리 기능은 미리 보기로 제공됩니다. 우리는 이 경험을 더욱 개선하고 향후 릴리스에서 향상된 기능을 추가할 계획입니다. 제품 내 채팅을 이용해 피드백을 보내주세요.

다음 사항에 유의하세요.

- 페이지 상단의 사례 관리 대시보드는 두 가지 보기를 제공합니다.
  - 왼쪽 보기는 귀하가 제공한 NSS 계정 사용자에 의해 지난 3개월 동안 열린 총 사례를 보여줍니다.
  - 오른쪽 보기는 사용자 NSS 계정을 기준으로 지난 3개월 동안 회사 수준에서 열린 총 사례를 보여줍니다.

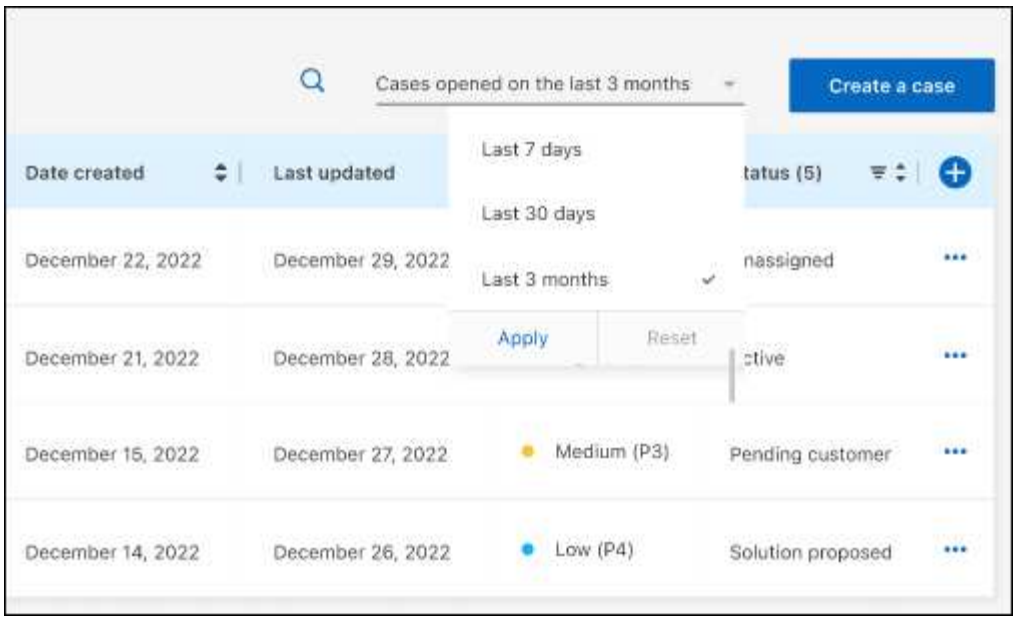
  표의 결과는 귀하가 선택한 보기와 관련된 사례를 반영합니다.
- 관심 있는 열을 추가하거나 제거할 수 있으며, 우선순위 및 상태와 같은 열의 내용을 필터링할 수 있습니다. 다른 열은 정렬 기능만 제공합니다.

  자세한 내용은 아래 단계를 참조하세요.
- 사례별로 사례 메모를 업데이트하거나 아직 닫힘 또는 닫힘 보류 상태가 아닌 사례를 닫는 기능을 제공합니다.

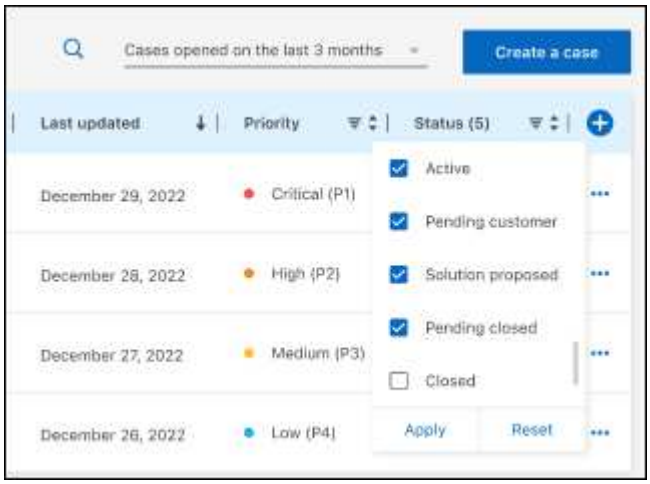
단계

1. BlueXP 에서 *도움말 > 지원*을 선택하세요.
2. *사례 관리*를 선택하고 메시지가 표시되면 BlueXP 에 NSS 계정을 추가합니다.

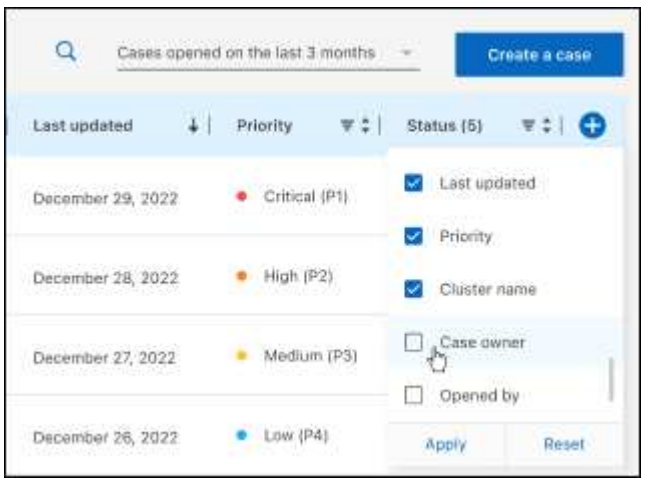
   사례 관리 페이지는 BlueXP 사용자 계정과 연결된 NSS 계정과 관련된 미해결 사례를 보여줍니다. 이는 **NSS** 관리 페이지 상단에 표시되는 NSS 계정과 동일합니다.
3. 필요에 따라 표에 표시되는 정보를 수정합니다.
   - *조직 사례*에서 *보기*를 선택하면 회사와 관련된 모든 사례를 볼 수 있습니다.
   - 정확한 날짜 범위를 선택하거나 다른 기간을 선택하여 날짜 범위를 수정하세요.



◦ 열의 내용을 필터링합니다.



◦ 표에 나타나는 열을 변경하려면 다음을 선택하세요. 그런 다음 표시하려는 열을 선택합니다.

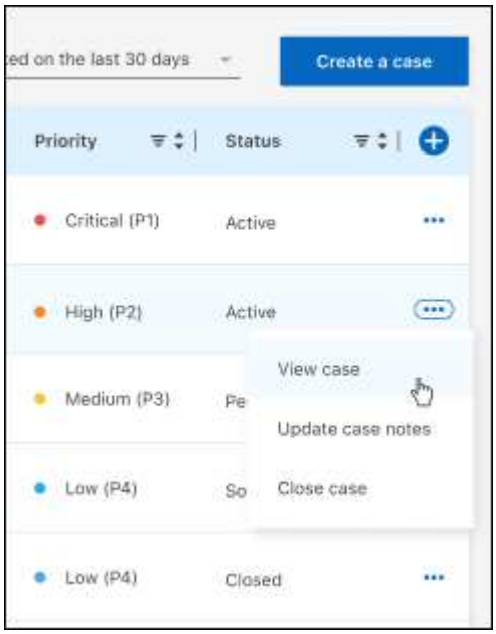


4. 기존 사례를 선택하여 관리하세요. 그리고 사용 가능한 옵션 중 하나를 선택하세요:

- 사례 보기: 특정 사례에 대한 전체 세부 정보를 확인하세요.
- 사례 메모 업데이트: 문제에 대한 추가 세부 정보를 제공하거나 *파일 업로드*를 선택하여 최대 5개의 파일을 첨부하세요.

  첨부파일은 파일당 25MB로 제한됩니다. 다음 파일 확장자가 지원됩니다: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx, csv.

- 사건 종결: 사건을 종결하는 이유를 자세히 입력하고 *사건 종결*을 선택하세요.



NetApp Ransomware Resilience 에 대한 자주 묻는 질문

NetApp Ransomware Resilience 에 대한 질문에 대한 빠른 답변을 찾고 있다면 이 FAQ가 도움이 될 수 있습니다.

전개

랜섬웨어 복원력을 사용하려면 라이선스가 필요합니까?

다음 라이선스 유형을 사용할 수 있습니다.

- 30일 무료 체험판에 등록하세요.
- Amazon Web Services(AWS) Marketplace, Google Cloud Marketplace, Microsoft Azure Marketplace에서 NetApp Intelligent Services 및 Ransomware Resilience에 대한 종량제(PAYGO) 구독을 구매하세요.
- BYOL(Bring Your Own License)은 NetApp 영업 담당자로부터 받는 NetApp 라이선스 파일(NLF)입니다. 콘솔의 Licenses and subscriptions 섹션에서 라이선스 일련 번호를 사용하여 BYOL을 활성화할 수 있습니다.

랜섬웨어 복원력을 어떻게 활성화하나요?

NetApp Console 에서 랜섬웨어 복원력에 액세스할 수 있습니다. 당신이 가지고 있는지 확인하십시오 "액세스 역할" 그리고 "전제 조건". 콘솔 에이전트를 성공적으로 구성했다면 다음을 수행할 수 있습니다. "워크로드 검색".

자세한 내용은 다음을 참조하세요."랜섬웨어 복원력에 액세스" 그리고"랜섬웨어 복원력 빠른 시작 가이드" .

랜섬웨어 복원력을 표준, 제한, 비공개 모드로 사용할 수 있나요?

랜섬웨어 복원력은 현재 표준 모드에서만 사용할 수 있습니다.

모든 NetApp 데이터 서비스에서 이러한 모드에 대한 설명은 다음을 참조하세요. "NetApp Console 배포 모드" .

입장

랜섬웨어 복구 **URL**은 무엇인가요?

브라우저에서 다음을 입력하세요. "https://console.netapp.com/ransomware-resilience" 콘솔에 접속하려면.

접근 권한은 어떻게 처리되나요?

"모든 서비스에 대한 콘솔 액세스 역할에 대해 알아보세요.". 랜섬웨어 복원력도 있습니다 "전담 액세스 역할".

어떤 기기의 해상도가 가장 좋은가요?

랜섬웨어 복원력에 권장되는 장치 해상도는 1920x1080 이상입니다.

어떤 브라우저를 사용해야 하나요?

모든 최신 웹 브라우저를 사용하여 NetApp Console 에 액세스할 수 있습니다.

상호 운용성

랜섬웨어 복원력은 **NetApp ONTAP** 에서 설정된 보호 설정을 인식합니까?

네, 랜섬웨어 복원력은 ONTAP 에 설정된 스냅샷 일정을 검색합니다.

랜섬웨어 복원력은 **NetApp Backup and Recovery** 와 **SnapCenter** 와 어떻게 상호 작용합니까**?**

랜섬웨어 복원력은 백업 및 복구와 함께 작동하여 파일 공유 작업 부하에 대한 스냅샷 및 백업 정책을 검색하고 설정합니다.

랜섬웨어 복원력은 SnapCenter 또는 SnapCenter for VMware와 함께 작동하여 애플리케이션 및 VM 워크로드에 대한 스냅샷 및 백업 정책을 검색하고 설정합니다.

Ransomware Resilience는 백업 및 복구와 SnapCenter (VMware용 SnapCenter 포함)와도 연동하여 파일과 워크로드에 일관된 복구를 수행합니다.

작업 부하

랜섬웨어 복원력의 맥락에서 워크로드란 무엇입니까**?**

워크로드는 애플리케이션, VM 또는 파일 공유입니다. 작업 부하에는 단일 애플리케이션 인스턴스에서 사용되는 모든 볼륨이 포함됩니다.

예를 들어 ora3.host.com에 배포된 Oracle 데이터베이스를 고려해 보세요. `vol1` 데이터를 포함하고 `vol2` 로그를 포함하고 있습니다. 두 볼륨은 해당 Oracle Database 인스턴스의 작업 부하를 구성합니다.

랜섬웨어 복원력은 어떻게 워크로드 데이터의 우선 순위를 정합니까**?**

워크로드 우선순위(중요, 표준, 중요)는 워크로드와 예약된 백업에 연결된 각 볼륨에 이미 적용된 스냅샷 빈도에 따라 결정됩니다.

"작업 우선순위 또는 중요도에 대해 알아보세요" .

Ransomware Resilience는 어떤 작업 부하를 지원합니까**?**

랜섬웨어 복원력은 다음과 같은 작업 부하를 식별할 수 있습니다: Oracle, MySQL, 파일 공유, 블록 스토리지, VM 및 VM 데이터 저장소.

SnapCenter 또는 SnapCenter for VMware를 사용하는 경우 이러한 제품에서 지원하는 모든 워크로드는 랜섬웨어 복원력에서도 식별됩니다. 랜섬웨어 복원력은 SnapCenter 및 SnapCenter 워크로드를 워크로드에 맞춰 일관되게 보호하고 복구할 수 있습니다.

데이터를 작업 부하와 어떻게 연관시키나요**?**

랜섬웨어 복원력은 볼륨과 파일 확장자를 검색하여 적절한 작업 부하와 연결합니다.

SnapCenter 또는 SnapCenter for VMware가 있고 백업 및 복구에서 워크로드를 구성한 경우 Ransomware Resilience는 SnapCenter 및 SnapCenter for VMware와 관련 볼륨에서 관리하는 워크로드를 검색합니다.

보호된 작업 부하란 무엇입니까**?**

랜섬웨어 복원력에서 작업 부하가 기본 탐지 정책이 활성화된 경우 보호됨 상태를 표시합니다. "자율 랜섬웨어 보호(ARP)" 작업 부하와 관련된 모든 볼륨에서 활성화됩니다.

"위험에 처한**"** 작업 부하란 무엇입니까**?**

워크로드에 기본 감지 정책이 활성화되어 있지 않으면 백업 및 스냅샷 정책이 활성화되어 있어도 "위험"으로 표시됩니다. 랜섬웨어 보호를 위해서는 다음을 활성화해야 합니다. "탐지 정책".

새로운 볼륨을 추가했지만 아직 나타나지 않았습니다**.** 어떻게 해야 하나요**?**

환경에 새 볼륨을 추가한 경우 워크로드 검색을 다시 시작합니다. 볼륨이 발견된 후, "새 볼륨을 보호하기 위해 보호 정책을 적용합니다.".

보호 정책

랜섬웨어 복원력 랜섬웨어 정책은 다른 종류의 워크로드 정책과 공존할 수 있나요?

현재 백업 및 복구(클라우드 백업)는 볼륨당 하나의 백업 정책을 지원합니다. 백업 및 복구를 사용하여 백업 보호를 구성하는 경우 랜섬웨어 복원력과 백업 정책을 공유합니다.

스냅샷 사본은 제한이 없으며 각 서비스에서 별도로 추가할 수 있습니다.

랜섬웨어 보호 전략에는 어떤 정책이 필요합니까?

에이 "랜섬웨어 보호 전략" 필요사항:

- 랜섬웨어 탐지 정책 및
- 스냅샷 정책

랜섬웨어 복원력 전략에는 백업 정책이 필요하지 않습니다.

랜섬웨어 복원력은 **NetApp ONTAP** 에서 설정된 보호 설정을 인식합니까?

네, 랜섬웨어 복원력은 ONTAP 에 설정된 스냅샷 일정을 검색합니다. 또한 검색된 작업 부하의 모든 볼륨에서 ARP와 FPolicy가 활성화되어 있는지도 알아냅니다. 랜섬웨어 복원력 대시보드에 표시되는 정보는 다른 NetApp 솔루션 및 제품에서 집계된 것입니다.

Ransomware Resilience는 백업 및 복구와 **SnapCenter** 에서 이미 만들어진 정책을 알고 있습니까?

네, 백업 및 복구 또는 SnapCenter 에서 관리되는 워크로드가 있는 경우 해당 제품에서 관리하는 정책이 Ransomware Resilience로 적용됩니다.

NetApp Backup and Recovery 및/또는 **SnapCenter** 에서 가져온 정책을 수정할 수 있나요?

아니요, Ransomware Resilience의 Backup and Recovery 또는 SnapCenter 에서 관리하는 정책은 수정할 수 없습니다. 해당 정책에 대한 변경 사항은 백업 및 복구 또는 SnapCenter 에서 관리합니다.

ONTAP 의 정책(예**: ARP, FPolicy,** 스냅샷)이 있는 경우 랜섬웨어 복원력에서 해당 정책이 변경됩니까?

아니요. 랜섬웨어 복원력은 ONTAP 의 기존 탐지 정책(ARP, FPolicy 설정)을 수정하지 않습니다.

랜섬웨어 복원력에 가입한 후 백업 및 복구 또는 **SnapCenter** 에 새로운 정책을 추가하면 어떻게 되나요?

랜섬웨어 복원력은 백업 및 복구 또는 SnapCenter 에서 새로 생성된 정책과 정책 변경 사항을 인식합니다.

ONTAP 에서 정책을 변경할 수 있나요?

네, ONTAP 에서 Ransomware Resilience 정책을 변경할 수 있습니다. 랜섬웨어 복원력에서 새로운 정책을 만들어 워크로드에 적용할 수도 있습니다. 이 작업은 기존 ONTAP 정책을 Ransomware Resilience에서 생성된 정책으로 대체합니다.

ONTAP 에서 정책을 비활성화할 수 있나요?

ONTAP 의 시스템 관리자 UI, API 또는 CLI를 사용하여 탐지 정책에서 ARP를 비활성화할 수 있습니다.

FPolicy 및 백업 정책을 비활성화하려면 해당 정책을 포함하지 않는 다른 정책을 적용하면 됩니다.

법적 고지 사항

법적 고지사항은 저작권 표시, 상표, 특허 등에 대한 정보를 제공합니다.

저작권

"https://www.netapp.com/company/legal/copyright/"

상표

NETAPP, NETAPP 로고 및 NetApp 상표 페이지에 나열된 마크는 NetApp, Inc.의 상표입니다. 다른 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.

"https://www.netapp.com/company/legal/trademarks/"

특허

NetApp 이 소유한 현재 특허 목록은 다음에서 확인할 수 있습니다.

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

개인정보 보호정책

"https://www.netapp.com/company/legal/privacy-policy/"

오픈소스

공지 파일은 NetApp 소프트웨어에서 사용되는 타사 저작권 및 라이선스에 대한 정보를 제공합니다.

- "NetApp Console 에 대한 알림"

저작권 정보

상표 정보