시작하십시오
BlueXP ransomware protection

NetApp
March 22, 2024

목차

시작하십시오

BlueXP 랜섬웨어 방어 사전 공개에 관해 알아보십시오

랜섬웨어 공격은 귀사의 시스템에 대한 액세스를 차단할 수 있으며 공격자는 데이터 릴리즈나 암호 해독을 위한 대가로 돈을 요구할 수 있습니다. IDC에 따르면 랜섬웨어 피해자가 여러 번의 랜섬웨어 공격을 경험하는 것은 드문 일이 아닙니다. 이로 인해 1일에서 몇 주 사이에 데이터에 대한 액세스가 중단될 수 있습니다.

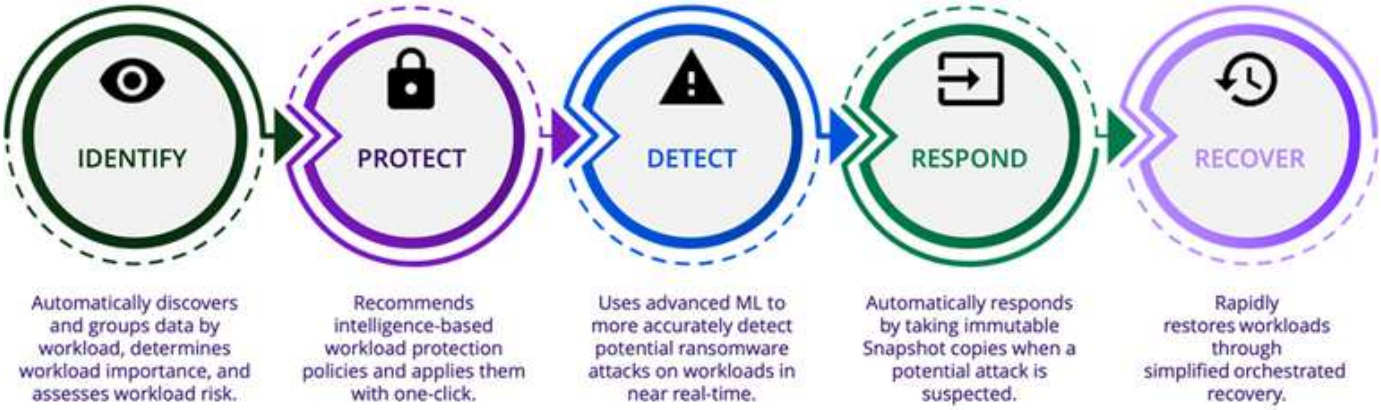
BlueXP 랜섬웨어 방어는 랜섬웨어 차단, 감지 및 복구를 위한 오케스트레이션 서비스입니다. 미리보기 버전의 경우 이 서비스는 Oracle, MySQL, VM 데이터 저장소, 온프레미스 NAS 스토리지와 Amazon Web Services의 Cloud Volumes ONTAP(NFS 프로토콜 사용) BlueXP 계정 전체에서 파일을 공유하고 Amazon Web Services 클라우드 스토리지 또는 NetApp StorageGRID에 데이터를 백업합니다.

> 이 문서는 기술 미리 보기로 제공됩니다. 이 사전 공개 오퍼링과 함께 NetApp은 일반 출시 이전에 서비스 세부 정보, 콘텐츠 및 일정을 수정할 권한을 보유합니다.

BlueXP 랜섬웨어 보호로 할 수 있는 일

BlueXP 랜섬웨어 보호 서비스는 여러 NetApp 기술을 최대한 활용하므로 스토리지 관리자, 데이터 보안 관리자 또는 보안 운영 엔지니어가 다음과 같은 목표를 달성할 수 있습니다.

- BlueXP 계정, 작업 공간 및 BlueXP 커넥터에 포함된 NFS 작업 환경을 사용하여 NetApp 온프레미스 NAS에서 모든 애플리케이션 기반, 파일 공유 또는 VMware 관리형 워크로드를 식별하십시오. 그런 다음 데이터 우선순위를 범주화하고 랜섬웨어 차단 개선을 위한 권장사항을 제공합니다.
- * 데이터에 대한 백업과 스냅샷 복사본을 사용하여 워크로드를 보호할 수 있습니다.
- * 랜섬웨어 공격일 수 있는 이상 징후를 감지합니다.
- * NetApp ONTAP 스냅샷 복사본을 자동으로 시작하여 잠재적 랜섬웨어 공격에 대응 * 합니다.
- * 여러 NetApp 기술을 조정하여 워크로드 가동 시간을 가속화하는 워크로드 복구 *. 볼륨, 폴더 또는 특정 파일을 복구하도록 선택할 수 있습니다. 이 서비스는 최상의 옵션에 대한 권장 사항을 제공합니다.



BlueXP 랜섬웨어 보호를 사용할 때의 이점

BlueXP 랜섬웨어 방어는 다음과 같은 이점을 제공합니다.

- 워크로드 및 데이터 세트를 검색하고, 사용 지수에 따라 우선 순위를 분석하고, 상대적 중요도 순위를 매깁니다.
- 랜섬웨어 보호 상태를 평가하고 이해하기 쉬운 대시보드에 표시합니다.
- 검색 및 보호 상태 분석을 기반으로 한 다음 단계에 대한 권장 사항을 제공합니다.
- 클릭 한 번으로 액세스할 수 있는 AI/ML 기반 데이터 보호 권장 사항을 적용합니다.
- MySQL, Oracle, VMware 데이터 저장소 및 파일 공유 등과 같은 주요 애플리케이션 기반 워크로드의 데이터를 보호합니다.
- AI 기술을 사용하여 운영 스토리지에서 데이터에 대한 랜섬웨어 공격을 실시간으로 감지합니다.
- 스냅샷 복사본을 생성하고 비정상적인 활동에 대한 알림을 시작하여 감지된 잠재적 공격에 대응하여 자동화된 조치를 시작합니다.
- RPO 정책을 충족하기 위해 선별된 복구를 적용합니다. BlueXP 랜섬웨어 방어 기능은 BlueXP 백업 및 복구(이전의 Cloud Backup)를 비롯한 여러 NetApp 복구 서비스를 사용하여 랜섬웨어 문제로부터 복구를 오케스트레이션합니다.

비용

NetApp은 BlueXP 랜섬웨어 방어 사전 공개 버전을 사용하는 데 비용을 청구하지 않습니다.

라이센싱

BlueXP 랜섬웨어 방어 사전 공개 자체에는 특별한 라이센스가 필요하지 않습니다. 모든 Preview 라이선스는 평가판 라이선스입니다.

> Preview 버전의 경우 NetApp는 평가판 및 필요한 모든 라이센스를 설정할 수 있도록 도와줍니다.

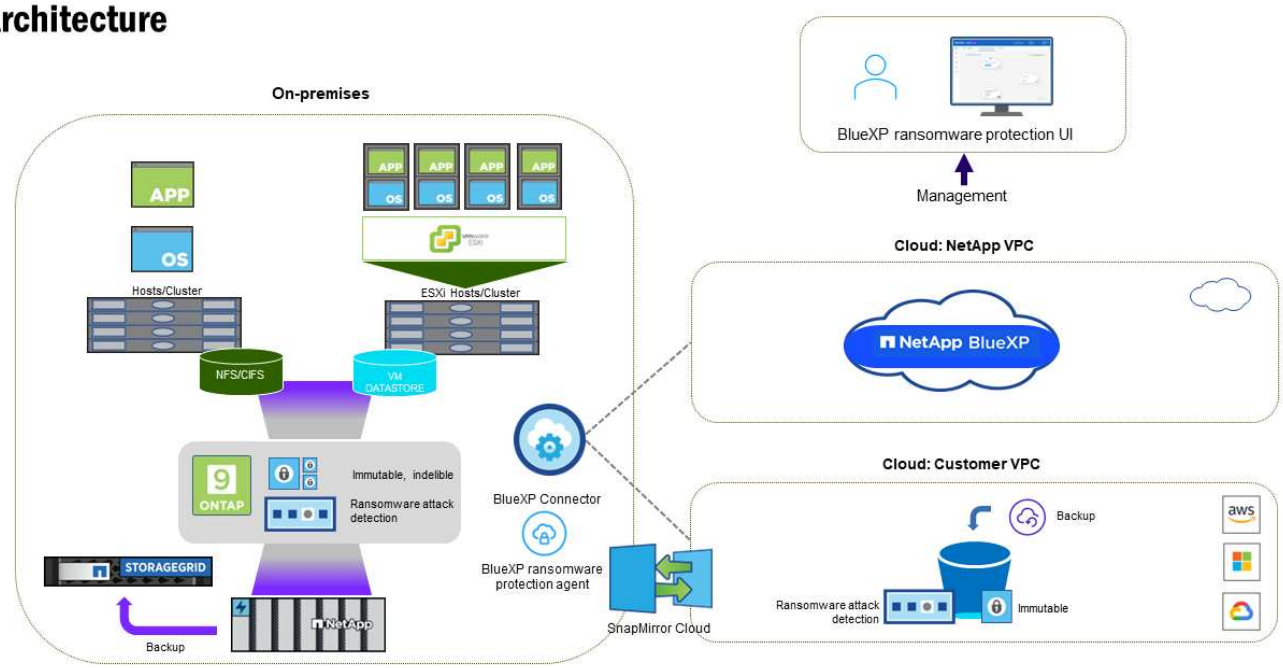
BlueXP 랜섬웨어 방어 사전 공개에는 다음 라이센스가 필요합니다.

- ONTAP
- NetApp 자율적 랜섬웨어 방어 기술. 을 참조하십시오 "자율 랜섬웨어 보호 개요" 를 참조하십시오.
- BlueXP 백업 및 복구 서비스

BlueXP 랜섬웨어 보호의 작동 방식

개략적으로 보면 BlueXP 랜섬웨어 방어 기능이 이와 같습니다.

Architecture



피처	설명
* 식별 *	• BlueXP에 연결된 모든 고객 온프레미스 NAS(NFS 마운트) 데이터를 찾습니다. • ONTAP 서비스 API에서 고객 데이터를 식별하고 워크로드와 연결합니다. 에 대해 자세히 알아보십시오 "ONTAP" 및 "SnapCenter 소프트웨어". • 각 볼륨의 현재 보호 수준 NetApp Snapshot 복사본 및 백업 정책과 모든 온박스 감지 기능을 검색합니다. 그런 다음 BlueXP 백업 및 복구, BlueXP 디지털 Advisor 및 ONTAP 서비스와 자율적 랜섬웨어 방어, FPolicy, 백업 정책 및 스냅샷 정책과 같은 NetApp 기술을 사용하여 이 보호 상태를 워크로드와 연결합니다. 에 대해 자세히 알아보십시오 "자율 랜섬웨어 보호" 및 "BlueXP 백업 및 복구", "BlueXP 디지털 자문업체", 및 "ONTAP FPolicy를 사용해 보십시오". • 자동으로 검색된 보호 수준을 기준으로 각 워크로드에 비즈니스 우선 순위를 지정하고 비즈니스 우선 순위를 기준으로 워크로드에 대한 보호 정책을 권장합니다. • 랜섬웨어 보호는 또한 정책 연계를 학습하고 유사한 워크로드에 사용자 지정 정책을 권장합니다.
* 보호 *	• 워크로드를 능동적으로 모니터링하고 식별된 각 워크로드에 정책을 적용하여 BlueXP 백업 및 복구 및 ONTAP API의 사용을 조정합니다.

피처	설명
* 감지 *	• 잠재적으로 비정상적인 암호화 및 활동을 감지하는 통합 머신 러닝(ML) 모델을 통해 잠재적 공격을 감지합니다. • 운영 스토리지에서 잠재적인 랜섬웨어 공격을 감지하고 비정상적인 활동에 대응하기 시작하는 이중 계층 감지를 제공합니다. 자동화된 Snapshot 복사본을 추가로 생성하여 가장 가까운 데이터 복원 지점을 확보할 수 있습니다. 이 서비스는 기본 워크로드의 성능에 영향을 주지 않으면서 보다 정밀하게 잠재적인 공격을 식별할 수 있는 능력을 제공합니다. • ONTAP, 자율적 랜섬웨어 방어 및 FPolicy 기술을 사용하여 공격이 관련된 의심스러운 파일을 결정하고 관련 워크로드에 매핑합니다.
* 응답 *	• 파일 활동, 사용자 활동 및 엔트로피 등의 관련 데이터를 표시하여 공격에 대한 포렌식 검토를 완료할 수 있도록 합니다. • ONTAP, 자율적 랜섬웨어 방어 및 FPolicy와 같은 NetApp 기술과 제품을 사용하여 빠른 스냅샷 복사본을 시작합니다.
* 복구 *	• BlueXP 백업 및 복구, ONTAP, 자율적 랜섬웨어 방어 및 FPolicy 기술 및 서비스를 사용하여 최상의 스냅샷 또는 백업을 결정하고 최상의 RPA(복구 지점)를 권장합니다. • 애플리케이션 정합성을 통해 VM, 파일 공유, 데이터베이스를 비롯한 워크로드의 복구를 오케스트레이션

지원되는 백업 타겟, 작업 환경 및 데이터 소스

BlueXP 랜섬웨어 방어 미리 보기를 사용하여 다음과 같은 유형의 백업 타겟, 작업 환경 및 데이터 소스에 대한 사이버 공격에 데이터가 얼마나 복원력을 갖추고 있는지 알아보십시오.

- 지원되는 백업 대상 *
- AWS(Amazon Web Services) S3
- NetApp StorageGRID를 참조하십시오
- 지원되는 작업 환경 *
- 온프레미스 ONTAP NAS(NFS 프로토콜 사용)
- ONTAP Select
- AWS의 Cloud Volumes ONTAP(NFS 프로토콜 사용)
- 데이터 소스 *

미리 보기 버전의 경우 이 서비스는 다음과 같은 애플리케이션 기반 워크로드를 보호합니다.

- NetApp 파일 공유
- VMware 데이터 저장소
- 데이터베이스(Oracle 및 MySQL의 미리보기 버전)

랜섬웨어 방어에 도움이 될 수 있는 약관을 읽어 보십시오

랜섬웨어 보호와 관련된 몇 가지 용어를 이해하면 도움이 될 수 있습니다.

- * 보호 *: BlueXP 랜섬웨어 방어의 보호는 보호 정책을 사용하여 서로 다른 보안 도메인에 대해 스냅샷과 변경 불가능한 백업을 정기적으로 발생시키도록 보장하는 것을 의미합니다.
- * 워크로드 *: BlueXP 랜섬웨어 방어 미리보기에는 MySQL 또는 Oracle 데이터베이스, VMware 데이터 저장소 또는 파일 공유가 포함될 수 있습니다.

BlueXP 랜섬웨어 방어의 사전 요구사항

운영 환경, 로그인, 네트워크 액세스 및 웹 브라우저의 준비 상태를 확인하여 BlueXP 랜섬웨어 보호를 시작하십시오.

BlueXP 랜섬웨어 방어 사전 공개 버전을 사용하려면 다음과 같은 사전 요구사항이 필요합니다.

- 백업 대상 및 액세스 권한 집합을 위한 NetApp StorageGRID 또는 AWS S3의 계정입니다

  을 참조하십시오 "AWS 권한 목록" 를 참조하십시오.

- ONTAP 9.11.1 이상
  - 클러스터 관리자 ONTAP 권한
  - BlueXP 랜섬웨어 방어에 의해 사용되는 NetApp 자율적 랜섬웨어 방어의 라이센스로, 사용 중인 ONTAP 버전에 따라 온프레미스 ONTAP 인스턴스에서 사용할 수 있습니다. 을 참조하십시오 "자율 랜섬웨어 보호 개요".

    라이센스에 대한 자세한 내용은 을 참조하십시오 "BlueXP 랜섬웨어 보호에 대해 알아보십시오".

- BlueXP의 경우:
  - 각 VPC(Virtual Private Cloud) 또는 온프레미스 영역별 BlueXP Connector를 BlueXP에서 설정해야 합니다. 을 참조하십시오 "커넥터 구성을 위한 BlueXP 설명서".

    > BlueXP 커넥터가 여러 개 있는 경우, 서비스에서는 BlueXP UI에 현재 표시된 커넥터 이외의 모든 커넥터 간에 데이터를 검사합니다.

  - 작업 환경에서 백업이 활성화된 BlueXP 백업 및 복구 서비스
  - NetApp NAS 온프레미스 스토리지를 사용하는 BlueXP 작업 환경
  - 온프레미스 ONTAP 클러스터에 연결된 활성 Connector가 하나 이상 있는 BlueXP 계정 모든 소스 및 작업 환경은 동일한 BlueXP 계정에 있어야 합니다.
  - 리소스 검색을 위한 계정 관리자 권한이 있는 BlueXP 사용자 계정
  - "표준 BlueXP 요구사항"

BlueXP 랜섬웨어 보호를 위한 빠른 시작

BlueXP 랜섬웨어 보호를 시작하는 데 필요한 단계를 간략하게 소개합니다. 각 단계의 링크를 클릭하면 자세한 내용을 제공하는 페이지로 이동합니다.

1. 사전 요구 사항을 검토합니다

"환경이 이러한 요구 사항을 충족하는지 확인합니다".

2 랜섬웨어 차단 서비스를 설정합니다

- "NetApp StorageGRID 또는 Amazon Web Services를 백업 대상으로 준비합니다".
- "BlueXP에서 Connector를 구성합니다".
- "백업 대상을 구성합니다".
- "BlueXP에서 워크로드를 찾아보십시오".

3 다음 단계

서비스를 설정한 후 수행할 수 있는 작업은 다음과 같습니다.

- "대시보드에서 워크로드 보호 상태를 확인합니다".
- "워크로드 보호".
- "잠재적인 랜섬웨어 공격 탐지에 대응".
- "공격에서 복구(인시던트가 무력화된 후)".

BlueXP 랜섬웨어 방어 설정을 확인하십시오

BlueXP 랜섬웨어 보호를 사용하려면 몇 단계를 수행하여 설정하십시오.

시작하기 전에 를 검토하십시오 "필수 구성 요소" 환경을 준비합니다.

백업 대상을 준비합니다

다음 백업 대상 중 하나를 준비합니다.

- NetApp StorageGRID를 참조하십시오
- Amazon Web Services에서 직접 지원합니다

백업 대상 자체에서 옵션을 구성한 후에는 나중에 BlueXP 랜섬웨어 방지 서비스에서 백업 대상으로 구성합니다.

백업 대상이 되도록 **StorageGRID**를 준비합니다

StorageGRID를 백업 대상으로 사용하려면 을 참조하십시오 "StorageGRID 설명서" StorageGRID에 대한 자세한 내용은

AWS를 백업 대상이 될 수 있도록 준비합니다

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

BlueXP에서 AWS 스토리지를 관리하는 방법에 대한 자세한 내용은 을 참조하십시오 "Amazon S3 버킷을 관리합니다".

BlueXP를 설정합니다

다음 단계로 BlueXP 및 BlueXP 랜섬웨어 방어 서비스를 설정합니다.

검토 "표준 BlueXP 요구사항".

BlueXP에서 커넥터를 만듭니다

이 서비스를 사용해 보려면 NetApp 영업 담당자에게 문의하십시오. BlueXP Connector를 사용하면 랜섬웨어 방지 서비스에 대한 적절한 기능이 포함됩니다.

서비스를 사용하기 전에 BlueXP에서 커넥터를 만들려면 에 설명된 BlueXP 설명서를 참조하십시오 "BlueXP Connector를 생성하는 방법".

> BlueXP 커넥터가 여러 개 있는 경우, 서비스에서는 BlueXP UI에 현재 표시된 커넥터 이외의 모든 커넥터 간에 데이터를 검사합니다. 이 서비스는 이 계정과 연결된 모든 작업 영역 및 모든 커넥터를 검색합니다.

BlueXP 랜섬웨어 방어 기능에 액세스하십시오

NetApp BlueXP를 사용하여 BlueXP 랜섬웨어 방어 서비스에 로그인할 수 있습니다. BlueXP 왼쪽 탐색 창에서 * 보호 * > * 랜섬웨어 방어 * 를 선택하십시오.

자세한 내용은 을 참조하십시오 "BlueXP 랜섬웨어 방어 기능에 액세스하십시오".

BlueXP 랜섬웨어 보호에서 백업 대상을 구성합니다

BlueXP 랜섬웨어 방어 백업 대상 옵션을 사용하여 백업 대상을 구성합니다. 자세한 내용은 을 참조하십시오 "설정 옵션을 구성합니다".

BlueXP 랜섬웨어 방어 기능에 액세스하십시오

NetApp BlueXP를 사용하여 BlueXP 랜섬웨어 방어 서비스에 로그인할 수 있습니다.

BlueXP에 로그인하려면 NetApp Support 사이트 자격 증명을 사용하거나 이메일 및 암호를 사용하여 NetApp 클라우드 로그인에 등록할 수 있습니다. "로그인에 대해 자세히 알아보십시오".

단계

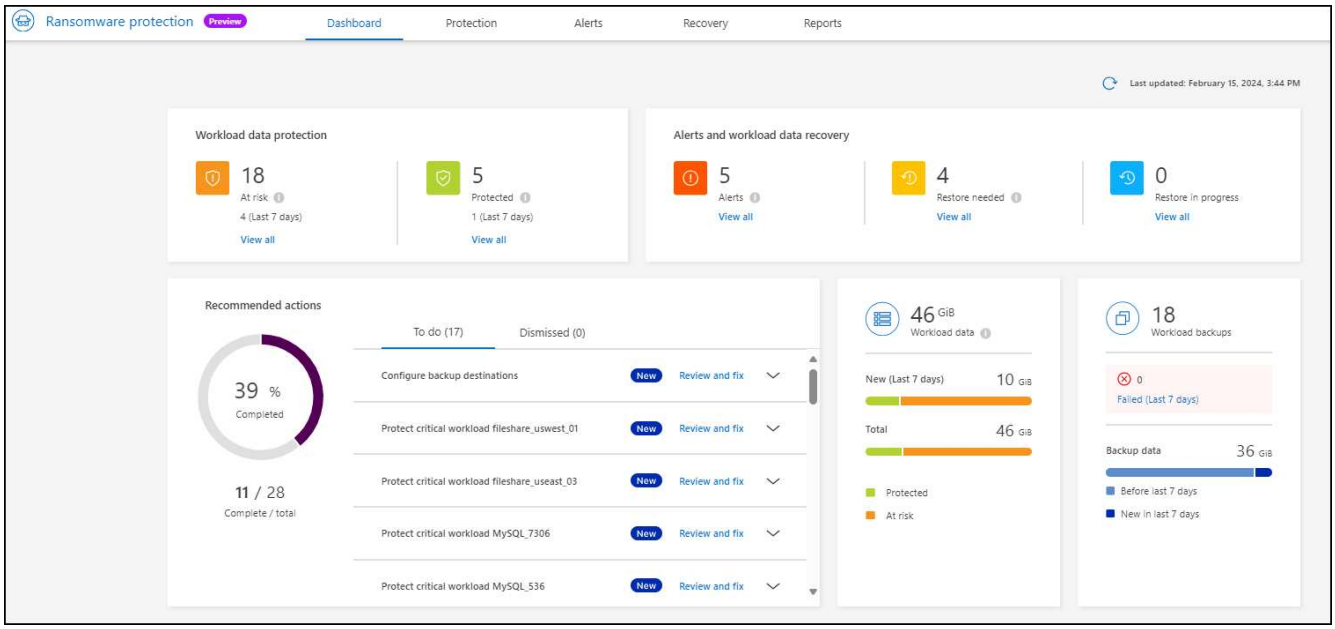
1. 웹 브라우저를 열고 로 이동합니다 "BlueXP 콘솔".

   NetApp BlueXP 로그인 페이지가 나타납니다.

2. BlueXP에 로그인합니다.
3. BlueXP 왼쪽 탐색 창에서 * 보호 * > * 랜섬웨어 방어 * 를 선택하십시오.

   이 서비스에 처음 로그인하는 경우 랜딩 페이지가 나타납니다.

   그렇지 않으면 BlueXP 랜섬웨어 보호 대시보드가 나타납니다.



4. 서비스 사용을 시작합니다.
    - BlueXP Connector가 없거나 이 사전 공개에 적합하지 않은 경우 NetApp Support에 문의하거나 메시지를 따라 이 미리 보기에 등록해야 할 수 있습니다.
    - BlueXP를 처음 접하고 Connector를 사용하지 않은 경우 " * 랜섬웨어 방지 * "를 선택하면 등록 관련 메시지가 표시됩니다. 양식을 제출하십시오. NetApp에서 귀하의 평가 요청에 대해 연락을 드릴 것입니다.
    - 기존 커넥터를 가지고 있는 BlueXP 사용자의 경우 " * 랜섬웨어 방지 * "를 선택하면 등록 메시지가 표시됩니다.
    - 미리 보기에 이미 참여하고 있는 경우 " * 랜섬웨어 방어 * "를 선택하면 서비스를 진행할 수 있습니다. 아직 수행하지 않았다면 * 워크로드 검색 * 옵션을 선택해야 합니다.

BlueXP 랜섬웨어 방어에서 워크로드를 찾아보십시오

BlueXP 랜섬웨어 보호를 사용하려면 이 서비스에서 먼저 데이터를 검색해야 합니다. BlueXP 랜섬웨어 보호는 검색 중에 고객 내의 모든 BlueXP 커넥터 및 작업 공간에 걸쳐 작업 환경의 모든 볼륨 및 파일을 분석합니다.

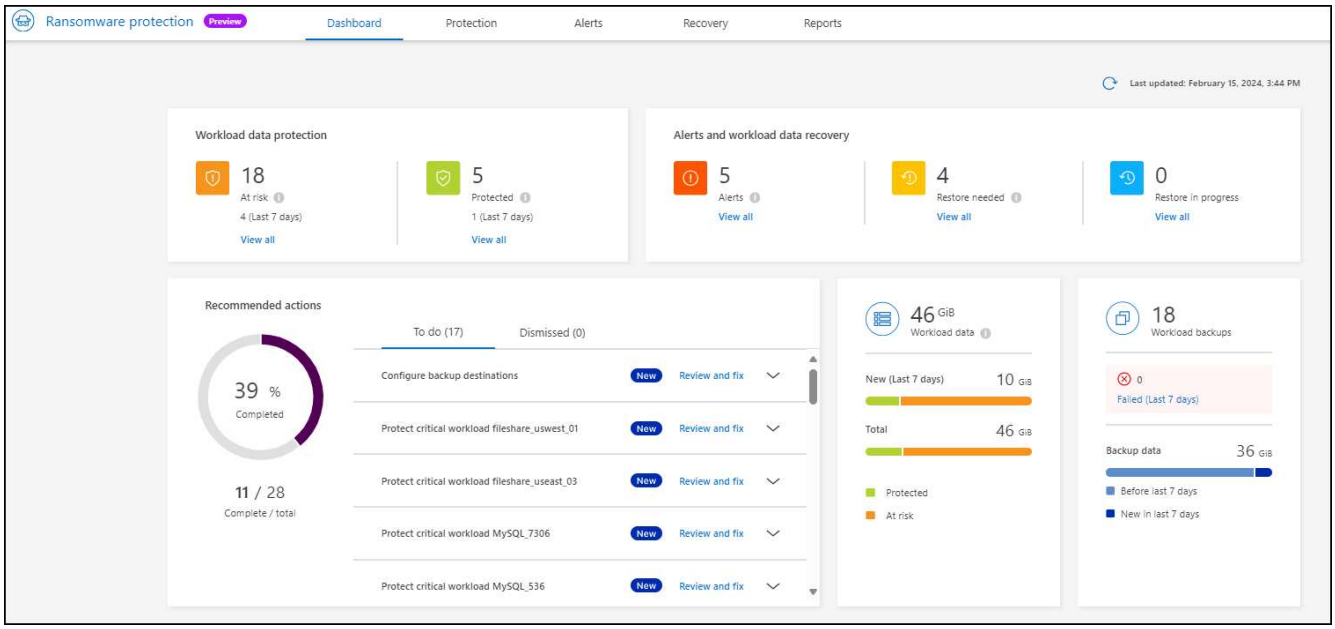
> 미리 보기 버전의 경우 BlueXP 랜섬웨어 보호를 통해 MySQL 애플리케이션, Oracle 애플리케이션, VMware 데이터 저장소 및 파일 공유를 평가합니다.

이 서비스는 현재 백업 보호, 스냅샷 복사본 및 NetApp 자율적 랜섬웨어 방어 옵션을 포함하여 기존 보호 수준을 평가합니다. 평가 결과를 기준으로 이 서비스는 랜섬웨어 보호를 개선하는 방법을 권장합니다.

단계

1. BlueXP 왼쪽 탐색 창에서 * 보호 * > * 랜섬웨어 방어 * 를 선택하십시오.
2. 초기 랜딩 페이지에서 * 워크로드 검색 * 을 선택합니다.

    이 서비스는 워크로드 데이터를 검색하고 데이터 보호 상태를 대시보드에 표시합니다.



BlueXP 랜섬웨어 보호 설정을 구성합니다

대시보드에서 권장 사항을 검토하여 백업 대상을 구성할 수 있습니다.

백업 대상을 추가합니다

BlueXP 랜섬웨어 방어 기능은 아직 백업이 없는 워크로드와 아직 백업 대상이 할당되지 않은 워크로드를 식별할 수 있습니다.

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

- NetApp StorageGRID를 참조하십시오
- AWS(Amazon Web Services)

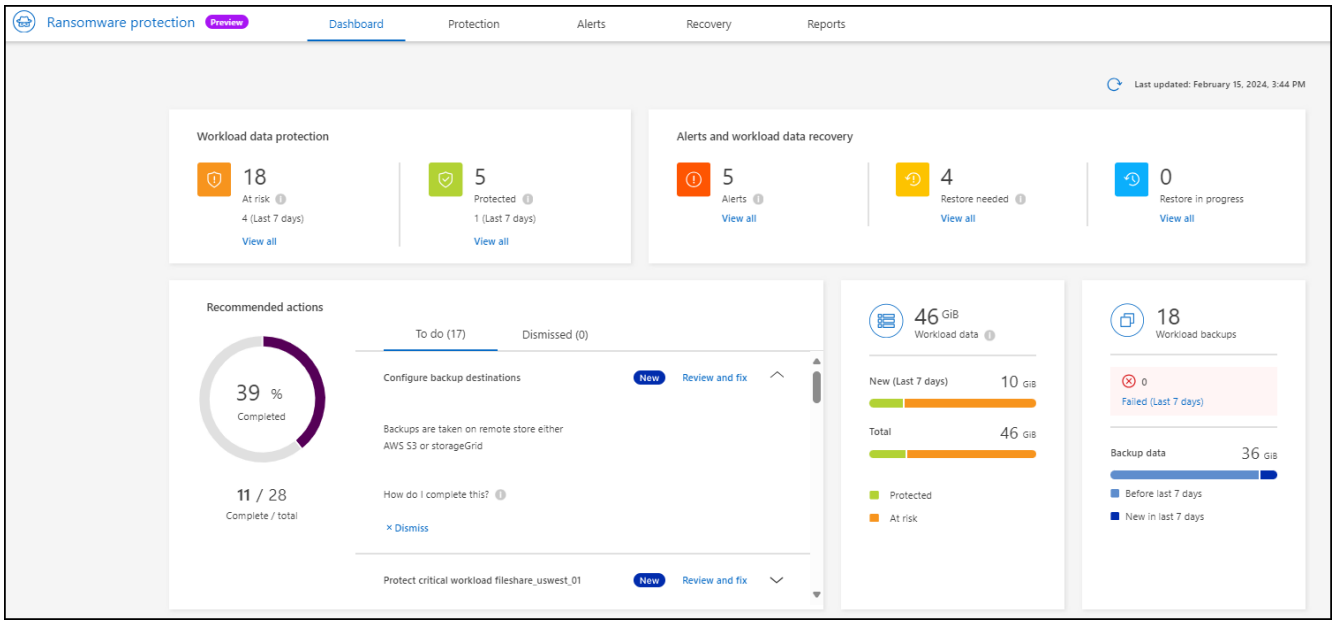
대시보드에서 권장하는 작업에 따라 백업 대상을 추가할 수 있습니다.

대시보드의 권장 작업에서 백업 대상 옵션에 액세스합니다

대시보드에는 여러 가지 권장 사항이 나와 있습니다. 한 가지 권장 사항은 백업 대상을 구성하는 것입니다.

단계

1. BlueXP 왼쪽 탐색 창에서 * 보호 * > * 랜섬웨어 방어 * 를 선택하십시오.
2. 대시보드의 권장 작업 창을 검토합니다.

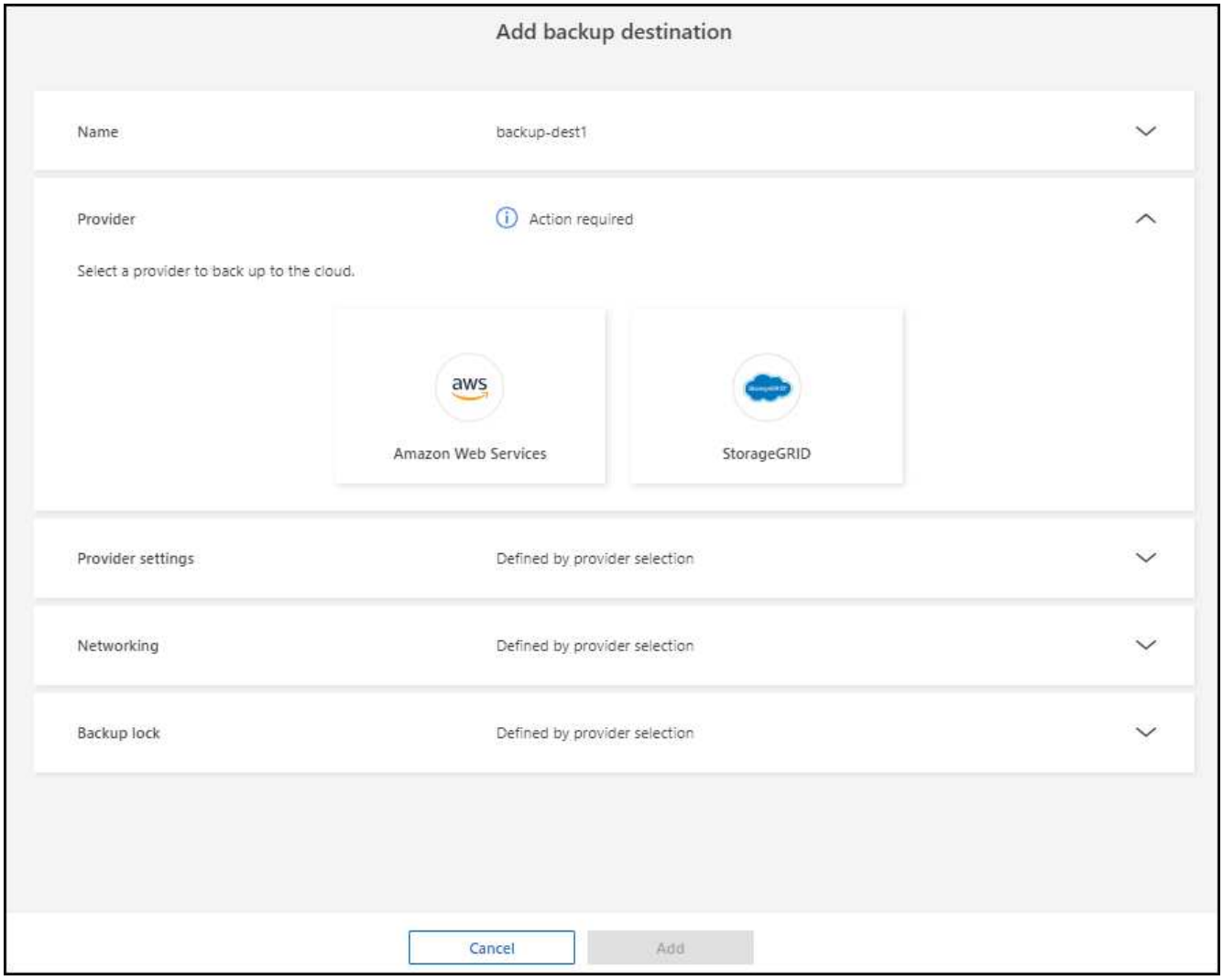


3. 대시보드에서 "백업 대상 구성"의 권장 사항에 대해 * 검토 및 수정 * 을 선택합니다.
4. 백업 공급자에 따라 지침을 계속합니다.

StorageGRID를 백업 대상으로 추가합니다

NetApp StorageGRID를 백업 대상으로 설정하려면 다음 정보를 입력합니다.

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



3. StorageGRID * 를 선택합니다.
4. 각 설정 옆에 있는 아래쪽 화살표를 선택하고 값을 입력하거나 선택합니다.
   - * 공급자 설정 *:
     - 새 버킷을 만들거나 백업을 저장할 고유 버킷을 가져오십시오.
     - StorageGRID 게이트웨이 노드 정규화된 도메인 이름, 포트, StorageGRID 액세스 키 및 비밀 키 자격 증명.
   - * 네트워킹 *: IPspace를 선택합니다.
     - IPspace는 백업하려는 볼륨이 상주하는 클러스터입니다. 이 IPspace용 인터클러스터 LIF는 아웃바운드 인터넷 액세스를 가져야 합니다.
   - * 백업 잠금 * : 서비스를 통해 백업 수정 또는 삭제로부터 백업을 보호할지 여부를 선택합니다. 이 옵션은 NetApp DataLock 기술을 사용합니다. 각 백업은 보존 기간 동안 또는 최소 30일 동안 잠기고 최대 14일의 버퍼 기간이 추가됩니다.

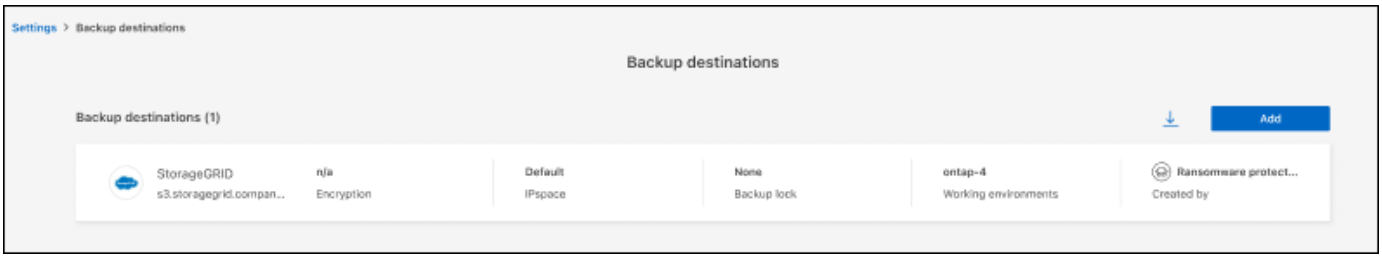
     > 지금 백업 잠금 설정을 구성하는 경우 백업 대상을 구성한 후에는 나중에 설정을 변경할 수 없습니다.

     - * 규정 준수 모드 *: 보존 기간 동안 사용자는 보호된 백업 파일을 덮어쓰거나 삭제할 수 없습니다.

5. 추가 * 를 선택합니다.

결과

새 백업 대상이 백업 대상 목록에 추가됩니다.

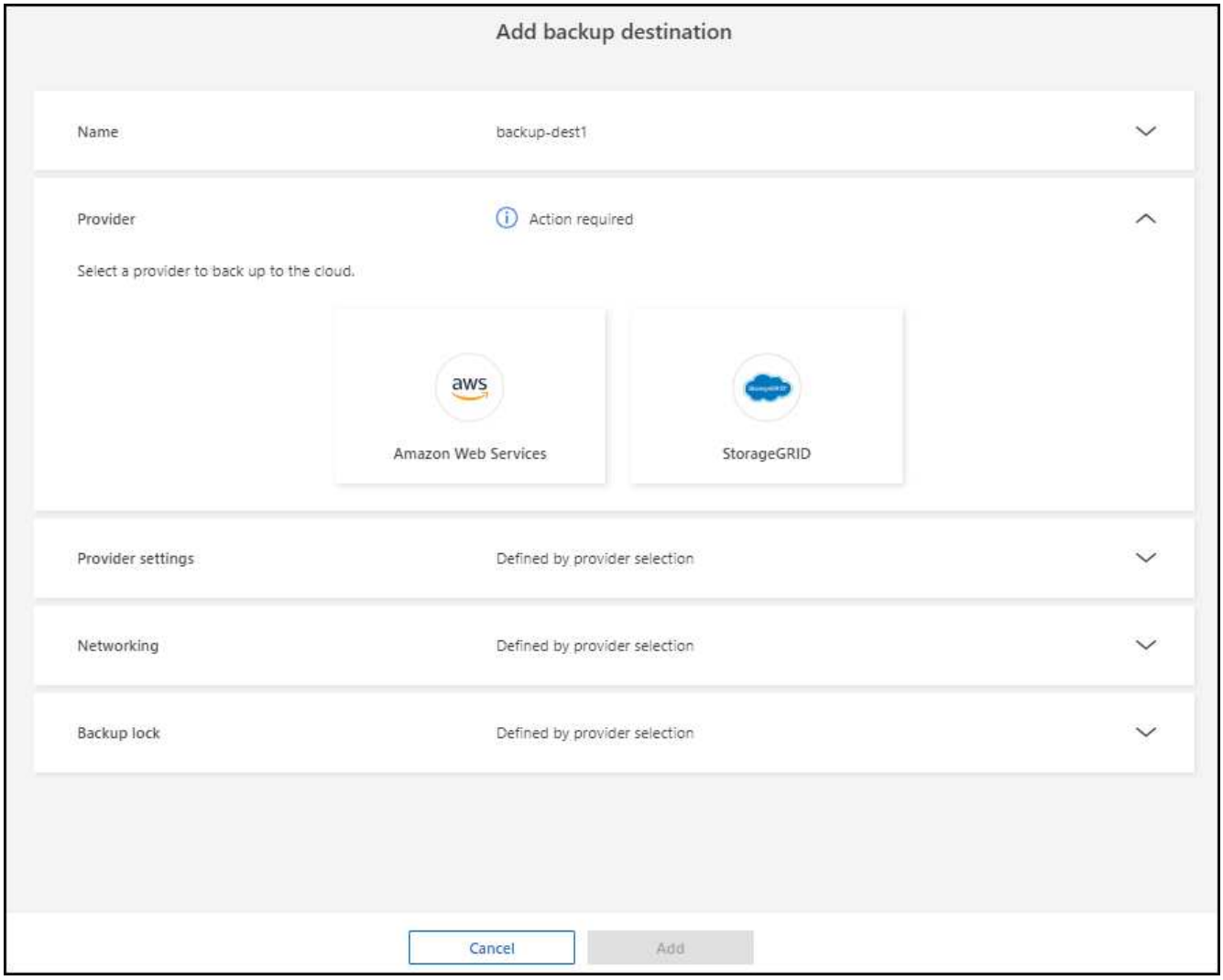


Amazon Web Services를 백업 대상으로 추가합니다

AWS를 백업 대상으로 설정하려면 다음 정보를 입력합니다.

BlueXP에서 AWS 스토리지를 관리하는 방법에 대한 자세한 내용은 을 참조하십시오 "Amazon S3 버킷을 관리합니다".

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



3. Amazon Web Services * 를 선택합니다.
4. 각 설정 옆에 있는 아래쪽 화살표를 선택하고 값을 입력하거나 선택합니다.
   - * 공급자 설정 *:
     - 새 버킷을 생성하고, BlueXP에 이미 존재하는 경우 기존 버킷을 선택하거나, 백업을 저장할 고유 버킷을 가져오십시오.
     - AWS 자격 증명을 위한 AWS 계정, 지역, 액세스 키 및 비밀 키

       "고유한 버킷을 가져오려는 경우 S3 버킷 추가 를 참조하십시오".
   - * 암호화 * : 새 S3 버킷을 만드는 경우 공급자로부터 받은 암호화 키 정보를 입력하십시오. 기존 버킷을 선택한 경우 암호화 정보를 이미 사용할 수 있습니다.

     버킷의 데이터는 기본적으로 AWS 관리형 키로 암호화됩니다. 계속해서 AWS에서 관리하는 키를 사용하거나 자체 키를 사용하여 데이터 암호화를 관리할 수 있습니다.
   - * 네트워킹 * : IPspace를 선택하고 개인 엔드포인트를 사용할 것인지 여부를 선택하십시오.
     - IPspace는 백업하려는 볼륨이 상주하는 클러스터입니다. 이 IPspace용 인터클러스터 LIF는 아웃바운드 인터넷 액세스를 가져야 합니다.
     - 필요에 따라 이전에 구성한 AWS 개인 끝점(PrivateLink)을 사용할지 여부를 선택합니다.

AWS PrivateLink를 사용하려면 을 참조하십시오 "Amazon S3를 위한 AWS PrivateLink".

- * 백업 잠금 * : 서비스를 통해 백업 수정 또는 삭제로부터 백업을 보호할지 여부를 선택합니다. 이 옵션은 NetApp DataLock 기술을 사용합니다. 각 백업은 보존 기간 동안 또는 최소 30일 동안 잠기고 최대 14일의 버퍼 기간이 추가됩니다.

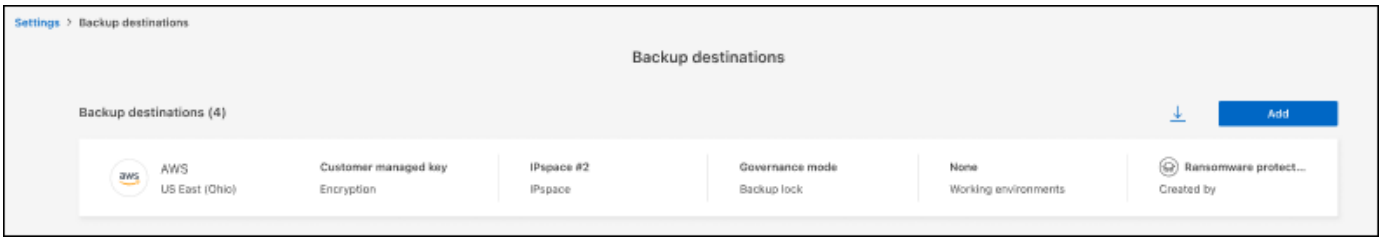
  > 지금 백업 잠금 설정을 구성하는 경우 백업 대상을 구성한 후에는 나중에 설정을 변경할 수 없습니다.

  - * Governance mode *: 특정 사용자(S3:BypassGovernanceRetention 권한이 있음)는 보존 기간 동안 보호된 파일을 덮어쓰거나 삭제할 수 있습니다.
  - * 규정 준수 모드 *: 보존 기간 동안 사용자는 보호된 백업 파일을 덮어쓰거나 삭제할 수 없습니다.

5. 추가 * 를 선택합니다.

결과

새 백업 대상이 백업 대상 목록에 추가됩니다.



BlueXP 랜섬웨어 방어에 관한 FAQ

이 FAQ는 질문에 대한 간단한 답변을 찾는 경우에 도움이 될 수 있습니다.

액세스

- BlueXP 랜섬웨어 방어 URL은 무엇입니까? *
  URL의 경우 브라우저에 다음을 입력합니다. "https://console.bluexp.netapp.com/" 를 눌러 BlueXP 콘솔에 액세스합니다.
- BlueXP 랜섬웨어 보호를 사용하려면 라이센스가 필요하십니까? *
  NetApp 라이센스 파일(NLF)은 필요하지 않습니다. BlueXP 랜섬웨어 방어 사전 공개 자체에는 특별한 라이센스가 필요하지 않습니다. 모든 Preview 라이선스는 평가판 라이선스입니다.

이 서비스의 미리 보기 버전에는 BlueXP 백업 및 복구 서비스 라이센스가 필요합니다.

> Preview 버전의 경우 NetApp는 평가판 및 필요한 모든 라이센스를 설정할 수 있도록 도와줍니다.

- BlueXP 랜섬웨어 보호를 어떻게 활성화하시겠습니까? *
  BlueXP 랜섬웨어 방어에 도움이 필요하지 않습니다. 랜섬웨어 방지 옵션은 BlueXP 왼쪽 탐색 창에서 자동으로 활성화됩니다.

Preview 버전의 경우 이 서비스를 체험하려면 등록하거나 NetApp 영업 담당자에게 연락해야 합니다. BlueXP Connector를 사용하면 서비스에 적합한 기능이 여기에 포함됩니다.

- BlueXP 랜섬웨어 보호는 표준, 제한 및 프라이빗 모드로 사용할 수 있습니까?**
  현재 BlueXP 랜섬웨어 보호는 표준 모드에서만 제공됩니다. 많은 관심 부탁드립니다.

모든 BlueXP 서비스 전체에서 이러한 모드에 대한 설명은 를 참조하십시오 "BlueXP 배포 모드".

- 액세스 권한은 어떻게 처리됩니까?**
  계정 관리자만 서비스를 시작하고 워크로드를 검색할 수 있습니다(리소스 사용을 커밋하는 작업이 포함되므로). 이후 상호 작용은 모든 역할에 의해 수행될 수 있습니다.
- 어떤 장치 해상도가 가장 좋습니까?**
  BlueXP 랜섬웨어 방어에 권장되는 장치 해상도는 1920x1080 이상입니다.
- 어떤 브라우저를 사용해야 합니까?**
  모든 최신 브라우저가 작동합니다.

다른 서비스와의 상호 작용

- BlueXP 랜섬웨어 방어는 NetApp ONTAP의 보호 설정을 인식합니까? *
  예, BlueXP 랜섬웨어 보호는 ONTAP에서 설정된 스냅샷 일정을 검색합니다.
- BlueXP 랜섬웨어 보호를 사용하여 정책을 설정한 경우 향후 이 서비스에서만 변경해야 합니까? *
  BlueXP 랜섬웨어 방어 서비스에서 정책을 변경하는 것이 좋습니다.

워크로드

업무량을 구성하는 요소는 무엇입니까**?**
워크로드에는 단일 애플리케이션 인스턴스에서 사용하는 모든 볼륨이 포함됩니다. 예를 들어, ora3.host.com 에 구축된 Oracle DB 인스턴스는 해당 데이터와 로그에 대해 각각 vol1과 vol2를 가질 수 있습니다. 이러한 볼륨은 모두 Oracle DB 인스턴스의 특정 인스턴스에 대한 워크로드를 구성합니다.

- BlueXP 랜섬웨어 방어는 워크로드 데이터의 우선순위를 어떻게 정합니까? *
  Preview 버전의 데이터 우선 순위는 생성된 스냅샷 복사본과 예약된 백업에 의해 결정됩니다.

워크로드 우선 순위는 다음과 같은 스냅샷 주파수에 의해 결정됩니다.

- * 중요 *: 시간당 1개 미만의 스냅샷 복사본 생성(매우 공격적인 보호 일정)
- * 중요 *: 매일 1회 미만으로 스냅샷 복사본을 생성합니다
- * 표준 *: 매일 1개 이상의 스냅샷 복사본이 생성됩니다
  - 새 볼륨이 추가되었지만 아직 나타나지 않습니다**
    환경에 새 볼륨을 추가한 경우 검색을 다시 시작하고 보호 정책을 적용하여 새 볼륨을 보호합니다.
  - 대시보드에 내 작업 부하가 모두 표시되지 않습니다. 무엇이 잘못되었을 수 있습니까?**
    현재 NFS 볼륨만 지원됩니다. iSCSI 볼륨, CIFS 볼륨 및 기타 지원되지 않는 구성은 필터링되어 대시보드에 표시되지 않습니다.

보호 정책

- BlueXP 랜섬웨어 정책은 다른 종류의 워크로드 정책과 공존합니까? *
  현재 BlueXP 백업 및 복구(Cloud Backup)는 볼륨당 하나의 백업 정책을 지원합니다. BlueXP 백업 및 복구와 BlueXP 랜섬웨어 방어는 백업 정책을 공유합니다.

Snapshot 복사본은 제한되지 않으며 각 서비스와 별도로 추가할 수 있습니다.