시작하십시오

BlueXP ransomware protection

NetApp
September 05, 2024

목차

시작하십시오 1
BlueXP 랜섬웨어 보호에 대해 알아보십시오 1
BlueXP 랜섬웨어 방어의 사전 요구사항 6
BlueXP 랜섬웨어 보호를 위한 빠른 시작 8
BlueXP 랜섬웨어 방어 설정을 확인하십시오 9
BlueXP 랜섬웨어 방어 기능에 액세스하십시오 10
BlueXP 랜섬웨어 방어에 대한 라이센스를 설정합니다 11
BlueXP 랜섬웨어 방어에서 워크로드를 찾아보십시오 20
BlueXP 랜섬웨어 보호 설정을 구성합니다 21
BlueXP 랜섬웨어 방어에 관한 FAQ 31

시작하십시오

BlueXP 랜섬웨어 보호에 대해 알아보십시오

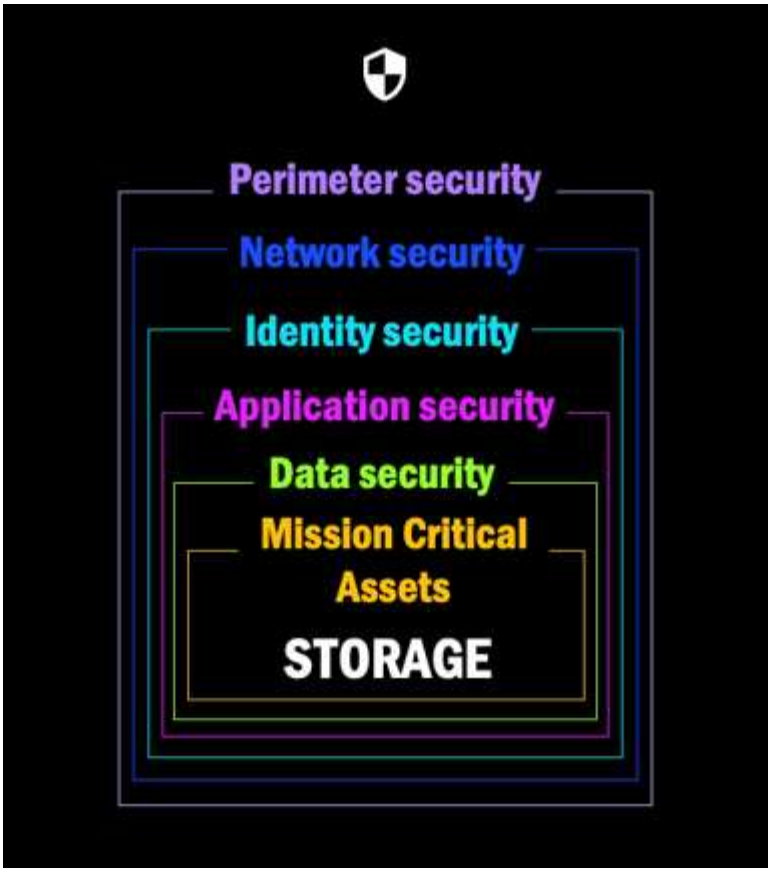
랜섬웨어 공격은 데이터에 대한 액세스를 차단할 수 있으며 공격자는 데이터 릴리즈나 암호 해독을 위한 대가로 돈을 요구할 수 있습니다. IDC에 따르면 랜섬웨어 피해자가 여러 번의 랜섬웨어 공격을 경험하는 것은 드문 일이 아닙니다. 이로 인해 1일에서 몇 주 사이에 데이터에 대한 액세스가 중단될 수 있습니다.

BlueXP 랜섬웨어 방어 서비스는 랜섬웨어로부터 데이터를 보호하는 서비스입니다. 이 서비스는 온프레미스 NAS 스토리지의 Oracle, MySQL, VM 데이터 저장소, 파일 공유(NFS 및 CIFS 프로토콜 사용)와 Amazon Web Services용 Cloud Volumes ONTAP, Cloud Volumes ONTAP for Google Cloud Platform, BlueXP 계정 전체에서 Cloud Volumes ONTAP for Microsoft Azure의 애플리케이션 기반 워크로드를 보호합니다. 이 서비스는 데이터를 Amazon Web Services, Google Cloud Platform, Microsoft Azure 클라우드 스토리지 및 NetApp StorageGRID에 백업합니다.

데이터 계층에서 랜섬웨어 방어

보안 체계는 일반적으로 다양한 사이버 위협으로부터 보호하기 위해 여러 계층의 방어 체계를 포괄합니다.

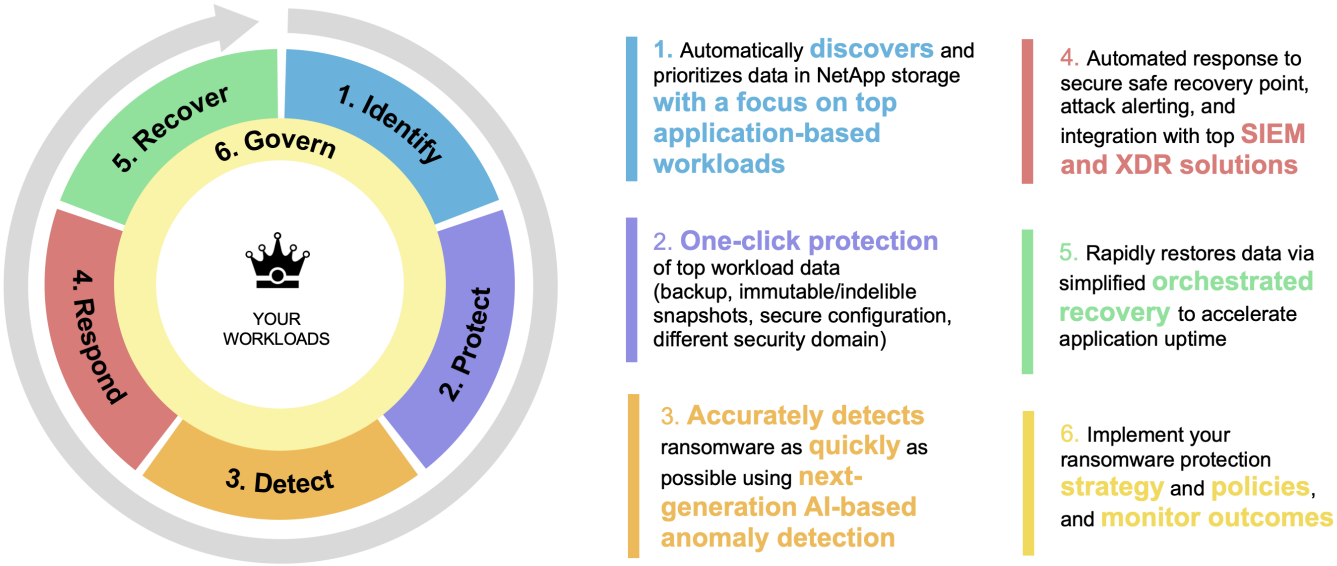
- * 가장 바깥쪽 계층 *: 방화벽, 침입 탐지 시스템 및 가상 사설망을 사용하여 네트워크 경계를 보호하는 첫 번째 방어선입니다.
- * 네트워크 보안 * : 이 계층은 네트워크 분할, 트래픽 모니터링 및 암호화를 기반으로 구축됩니다.
- **ID** 보안: 인증 방법, 액세스 제어 및 ID 관리를 사용하여 권한이 있는 사용자만 중요한 리소스에 액세스할 수 있도록 합니다.
- * 응용 프로그램 보안 *: 보안 코딩 사례, 보안 테스트 및 런타임 응용 프로그램 자체 보호를 사용하여 소프트웨어 응용 프로그램을 보호합니다.
- * 데이터 보안 * : 데이터 보호, 백업 및 복구 전략으로 데이터를 보호합니다. BlueXP 랜섬웨어 방어는 이 계층에서 작동합니다.



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.

- BlueXP의 NFS 또는 CIFS 작업 환경을 사용하여 BlueXP 계정, 작업 공간 및 BlueXP 커넥터를 통해 NetApp 온프레미스 NAS에서 모든 애플리케이션 기반, 파일 공유 또는 VMware 관리형 워크로드를 식별 * 할 수 있습니다. 그런 다음 데이터 우선순위를 범주화하고 랜섬웨어 차단 개선을 위한 권장사항을 제공합니다.
- * 데이터에 대한 백업, 스냅샷 복사본, 랜섬웨어 보호 전략을 지원하여 워크로드를 보호하십시오.
- * 랜섬웨어 공격일 수 있는 이상 징후를 감지 * 하십시오. 각주: [랜섬웨어 탐지 또는 방지 시스템은 랜섬웨어 공격으로부터 완벽하게 안전을 보장할 수 없습니다. 공격이 탐지되지 않을 수도 있지만 NetApp 기술은 중요한 추가 방어 계층으로 작용합니다.]
- * 실수로 또는 악의적으로 복사본이 삭제되지 않도록 잠겨 있는 무단 변경 방지 NetApp ONTAP 스냅샷을 자동으로 시작함으로써 잠재적 랜섬웨어 공격에 대응 * 하십시오. 백업 데이터는 변경 불가능한 상태로 유지되며 소스 및 타겟에서 랜섬웨어 공격으로부터 완벽하게 보호됩니다.
- * 여러 NetApp 기술을 조정하여 워크로드 가동 시간을 가속화하는 워크로드 복구 *. 특정 볼륨을 복구하도록 선택할 수 있습니다. 이 서비스는 최상의 옵션에 대한 권장 사항을 제공합니다.
- * 관리 *: 랜섬웨어 보호 전략을 구현하고 결과를 모니터링하십시오.



BlueXP 랜섬웨어 보호를 사용할 때의 이점

BlueXP 랜섬웨어 방어는 다음과 같은 이점을 제공합니다.

- 워크로드와 기존 스냅샷 및 백업 일정을 검색하고 상대적 중요도를 평가합니다.
- 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) 및 SnapCenter와 같은 여러 NetApp 복구 서비스를 사용하여 랜섬웨어 문제로부터 복구를 오케스트레이션합니다.
- 역할 기반 액세스 제어(RBAC)를 사용하여 서비스 내 기능 및 운영에 대한 액세스 권한을 관리함으로써 보안을 강화합니다.

비용

NetApp은 BlueXP 랜섬웨어 방어 시험판 버전을 사용하는 데 비용을 청구하지 않습니다.

BlueXP 백업 및 복구와 BlueXP 랜섬웨어 보호가 모두 있는 경우 두 제품으로 보호되는 모든 일반 데이터는 BlueXP 랜섬웨어 보호로만 청구됩니다.

라이센스 또는 PayGo 구독을 구매한 후 랜섬웨어 감지 정책(자율적 랜섬웨어 방어)을 활성화한 모든 워크로드(BlueXP 랜섬웨어 방어에서 검색하거나 설정)는 최소 하나의 스냅샷 또는 백업 정책을 의미하는 BlueXP 랜섬웨어 방어 기능은 IT를 "보호"로 분류하며, 구매한 용량 또는 PayGo 구독에 반영됩니다. 백업 또는 스냅샷 정책이 있더라도 감지 정책(ARP) 없이 워크로드가 검색되면 "위험"으로 분류되고 구매한 용량에 대해 _NOT_COUNT가 됩니다.

보호된 워크로드는 90일 평가 기간이 종료된 후 구입한 용량이나 구독에 따라 계산됩니다. BlueXP 랜섬웨어 방어는 효율성보다 보호된 워크로드와 관련된 데이터에 대해 GB 단위로 청구됩니다.

라이센싱

BlueXP 랜섬웨어 방어 기능을 사용하면 무료 평가판, 즉시 사용 가능한 용량제 구독 또는 자체 라이센스를 포함하여 다양한 라이센스 계획을 사용할 수 있습니다.

BlueXP 랜섬웨어 보호 서비스를 사용하려면 NetApp ONTAP 라이센스가 필요합니다.

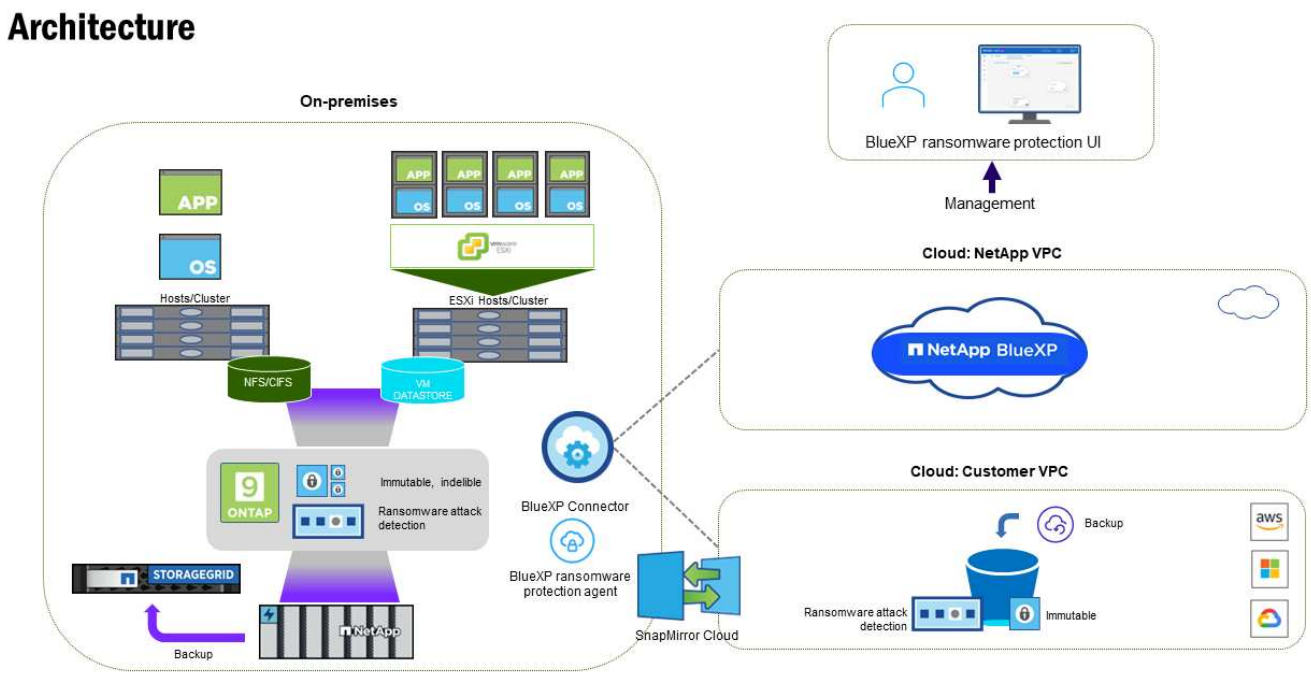
BlueXP 랜섬웨어 방지 라이센스에는 추가 NetApp 제품이 포함되지 않습니다. BlueXP 랜섬웨어 방어는 라이센스가 없는 경우에도 BlueXP 백업 및 복구를 사용할 수 있습니다.

자세한 내용은 을 참조하십시오 "라이센스를 설정합니다".

BlueXP 랜섬웨어 보호의 작동 방식

개략적으로 보면 BlueXP 랜섬웨어 방어 기능이 이와 같습니다.

BlueXP 랜섬웨어 방어는 BlueXP 백업 및 복구를 사용하여 파일 공유 워크로드에 대한 스냅샷 및 백업 정책을 검색하고 설정합니다. 또한 SnapCenter 또는 SnapCenter for VMware는 애플리케이션 및 VM 워크로드에 대한 스냅샷 및 백업 정책을 검색하고 설정합니다. 또한 BlueXP 랜섬웨어 방어 기능은 BlueXP 백업 및 복구와 SnapCenter/SnapCenter for VMware를 사용하여 파일 및 워크로드 정합성이 보장되는 복구를 수행합니다.



피처	설명
* 식별 *	• 모든 고객 사내 NAS(NFS 및 CIFS 프로토콜) 및 BlueXP에 연결된 Cloud Volumes ONTAP 데이터를 찾습니다. • ONTAP 및 SnapCenter 서비스 API에서 고객 데이터를 식별하고 이를 워크로드에 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, 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", 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. 워크로드 우선순위는 워크로드와 연결된 각 볼륨에 이미 적용된 스냅샷 주파수를 기반으로 합니다.
* 보호 *	• 워크로드를 능동적으로 모니터링하고 식별된 각 워크로드에 정책을 적용하여 BlueXP 백업 및 복구, SnapCenter, ONTAP API의 사용을 조정합니다.
* 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
* 통제 *	• 랜섬웨어 방지 전략을 할당합니다 • 결과를 모니터링할 수 있습니다.

지원되는 백업 타겟, 작업 환경 및 워크로드 데이터 소스

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

- 지원되는 백업 대상 *
- AWS(Amazon Web Services) S3
- Google 클라우드 플랫폼
- Microsoft Azure Blob
- NetApp StorageGRID를 참조하십시오
- 지원되는 작업 환경 *
- ONTAP 버전 9.11.1 이상이 설치된 온프레미스 ONTAP NAS(NFS 및 CIFS 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 9.11.1 이상(NFS 및 CIFS 프로토콜 사용)

> FlexGroup 볼륨, 9.11.1 이전 ONTAP 버전, iSCSI 볼륨, 마운트 지점 볼륨, 마운트 경로 볼륨, 오프라인 볼륨, 데이터 보호(DP) 볼륨을 지원합니다.

- 지원되는 워크로드 데이터 소스 *

이 서비스는 기본 데이터 볼륨에서 다음 애플리케이션 기반 워크로드를 보호합니다.

- NetApp 파일 공유
- VMware 데이터 저장소
- 데이터베이스(MySQL 및 Oracle)
- 곧 더 추가될 예정입니다

또한 VMware용 SnapCenter 또는 SnapCenter를 사용 중인 경우 해당 제품이 지원하는 모든 워크로드가 BlueXP 랜섬웨어 방어 전략에서도 식별됩니다. BlueXP 랜섬웨어 방어 기능은 워크로드 정합성이 보장되는 방식으로 이러한 문제를 보호하고 복구할 수 있습니다.

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 워크로드에는 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 보호를 사용하려면 다음과 같은 사전 요구사항이 필요합니다.

BlueXP 에서

- 리소스 검색을 위한 계정 관리자 Privileges가 있는 BlueXP 사용자 계정
- 온프레미스 ONTAP 클러스터에 연결하거나 AWS 또는 Azure에서 Cloud Volumes ONTAP에 연결하는 하나 이상의 활성 BlueXP Connector가 있는 BlueXP 계정
- NetApp 온프레미스 ONTAP 클러스터 또는 AWS 또는 Azure의 Cloud Volume ONTAP(NAS 또는 CIFS 프로토콜 사용)가 있는 하나 이상의 BlueXP 작업 환경
  - ONTAP OS 버전 9.11.1 이상이 설치된 ONTAP 또는 Cloud Volume ONTAP 클러스터가 지원됩니다.
  - 온프레미스 ONTAP 클러스터 또는 AWS 또는 Azure 클라우드의 Cloud Volume ONTAP가 아직 BlueXP 에 온보딩되지 않은 경우 BlueXP Connector가 필요합니다.

```
https://docs.netapp.com/us-en/bluexp-setup-admin/concept-
connectors.html["BlueXP 커넥터를 구성하는 방법에 대해 알아봅니다"]및
https://docs.netapp.com/us-en/cloud-manager-setup-admin/reference-
checklist-cm.html["표준 BlueXP 요구사항"^]을 참조하십시오.
```

> 단일 BlueXP 계정에 여러 BlueXP 커넥터가 있는 경우 BlueXP 랜섬웨어 보호 서비스가 현재 BlueXP UI에서 선택된 커넥터 이외의 모든 커넥터에서 ONTAP 리소스를 검사합니다.

ONTAP 9.11.1 이상

- 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".

> BlueXP 랜섬웨어 방어 의 일반 릴리즈에는 Preview 릴리즈와 달리 NetApp Autonomous 랜섬웨어 Protection 기술에 대한 라이센스가 포함되어 있습니다. 을 참조하십시오 "자율 랜섬웨어 보호 개요" 를 참조하십시오.

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

- 보호 구성을 적용하려면(예: 자율적 랜섬웨어 방어 활성화 등) BlueXP 랜섬웨어 차단에 ONTAP 클러스터에 대한 관리자 권한이 필요합니다. ONTAP 클러스터는 ONTAP 클러스터 관리자의 사용자 자격 증명만을 사용하여 온보딩되어야 합니다.
- ONTAP 클러스터가 관리자가 아닌 사용자 자격 증명을 사용하여 BlueXP 에 이미 온보딩된 경우, 이 페이지에 설명된 ONTAP 클러스터에 로그인하여 관리자가 아닌 사용자 권한을 필요한 권한으로 업데이트해야 합니다.

데이터 백업용입니다

- 백업 대상과 액세스 권한 집합을 위한 NetApp StorageGRID, AWS S3 또는 Azure Blob의 계정입니다.

  자세한 내용은 을 "AWS, Azure 또는 S3 사용 권한 목록" 참조하십시오.

- 작업 환경에서 BlueXP 백업 및 복구 서비스를 활성화할 필요는 없습니다.

  BlueXP 랜섬웨어 보호 서비스는 설정 옵션을 통해 백업 대상을 구성하는 데 도움이 됩니다. 을 "설정을 구성합니다

"참조하십시오.

ONTAP 작업 환경에서 관리자가 아닌 사용자 권한 업데이트

특정 작업 환경에 대해 관리자가 아닌 사용자 권한을 업데이트해야 하는 경우 다음 단계를 완료합니다.

1. BlueXP 계정에 로그인하여 ONTAP 사용자 권한을 업데이트해야 하는 작업 환경을 찾습니다.
2. 작업 환경을 두 번 클릭하여 세부 정보를 확인합니다.
3. 사용자 이름을 표시하는 * 추가 정보 보기 * 를 클릭합니다.
4. admin 사용자를 사용하여 ONTAP 클러스터 CLI에 로그인합니다.
5. 해당 사용자의 기존 역할을 표시합니다. 입력:

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

6. 사용자의 역할을 변경합니다. 입력:

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

7. BlueXP 랜섬웨어 차단 UI로 돌아가 사용하십시오.

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, Amazon Web Services 또는 Microsoft Azure를 백업 대상으로 준비합니다".
- "BlueXP에서 Connector를 구성합니다".
- "백업 대상을 구성합니다".
- "선택적으로 위협 감지를 활성화합니다".
- "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
- Microsoft Azure를 참조하십시오

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".

Azure를 백업 대상으로 삼을 준비를 합니다

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

BlueXP에서 Azure 스토리지를 관리하는 방법에 대한 자세한 내용은 을 참조하십시오 "Azure 저장소 계정을 관리합니다".

BlueXP를 설정합니다

다음 단계로 BlueXP 및 BlueXP 랜섬웨어 방어 서비스를 설정합니다.

검토 "표준 BlueXP 요구사항".

BlueXP에서 커넥터를 만듭니다

이 서비스를 사용해 보거나 사용하려면 NetApp 영업 담당자에게 문의해야 합니다. 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 랜섬웨어 방어는 RBAC(역할 기반 액세스 제어)를 사용하여 각 사용자가 특정 작업에 대한 액세스를 통제합니다. 각 역할이 수행할 수 있는 작업에 대한 자세한 내용은 을 참조하십시오"BlueXP 랜섬웨어 차단 역할 기반 액세스 제어 Privileges".

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

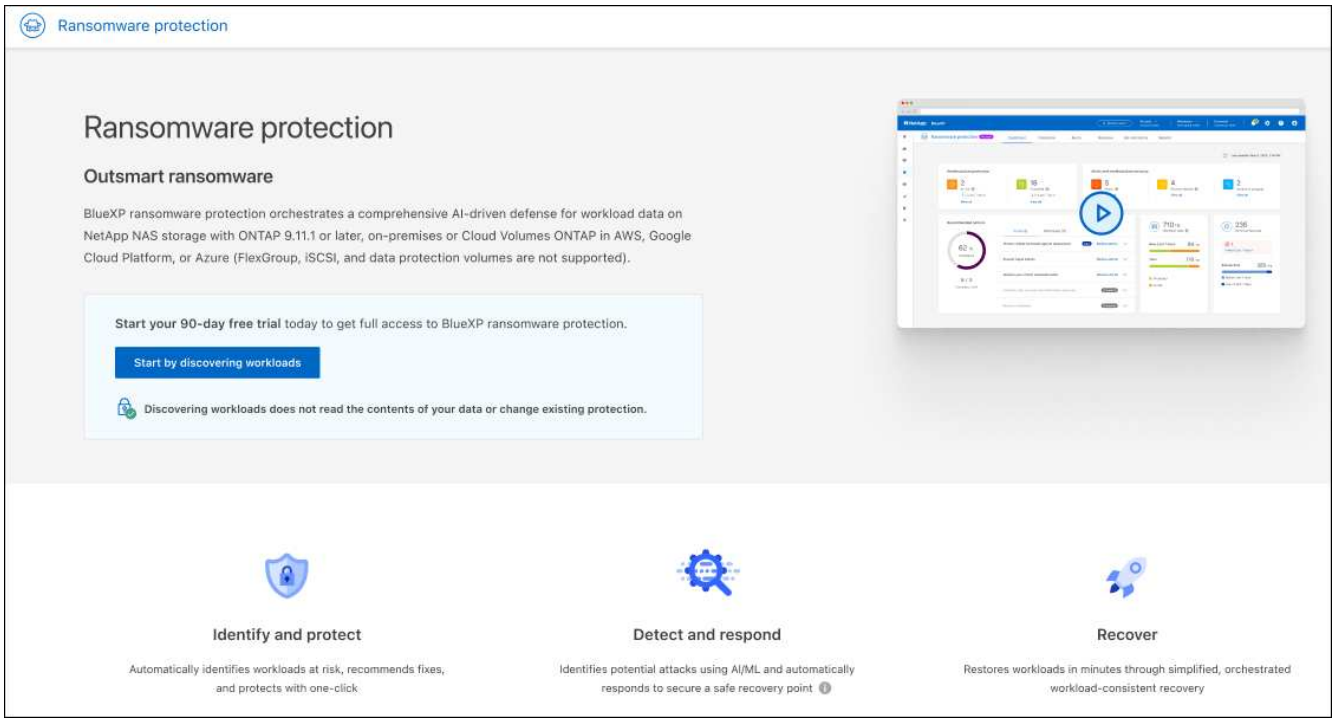
단계

1. 웹 브라우저를 열고 로 이동합니다 "BlueXP 콘솔".

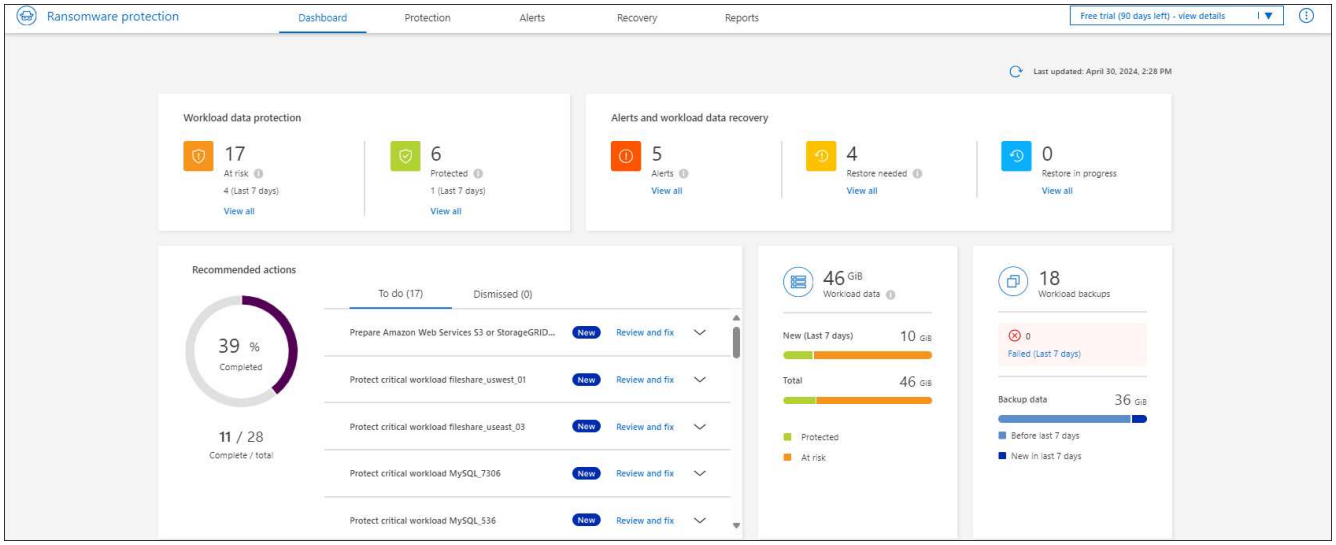
   NetApp BlueXP 로그인 페이지가 나타납니다.

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.



BlueXP 커넥터가 없거나 이 서비스의 커넥터가 아닌 경우 NetApp 지원에 문의해야 할 수 있습니다.

4. 아직 수행하지 않았다면 * 워크로드 검색 * 옵션을 선택하십시오.

   을 참조하십시오 "워크로드 검색".

BlueXP 랜섬웨어 방어에 대한 라이센스를 설정합니다

BlueXP 랜섬웨어 방어 기능을 통해 다양한 라이센스 계획을 사용할 수 있습니다.

다음과 같은 라이센스 유형을 사용할 수 있습니다.

- 90일 무료 평가판을 신청하십시오.
- AWS(Amazon Web Services) 마켓플레이스 또는 Azure 마켓플레이스(제공 예정)를 통해 용량제(PAYGO) 구독을 구매합니다.
- BYOL(Bring Your Own License) - NetApp 영업 담당자로부터 얻은 NLF(NetApp 라이센스 파일 라이센스 일련 번호를 사용하여 BlueXP 디지털 지갑에서 BYOL을 활성화할 수 있습니다.

BlueXP 랜섬웨어 방지 라이센스에는 추가 NetApp 제품이 포함되지 않습니다. BlueXP 랜섬웨어 방어는 라이센스가 없는 경우에도 BlueXP 백업 및 복구를 사용할 수 있습니다.

> BlueXP 백업 및 복구와 BlueXP 랜섬웨어 보호가 모두 있는 경우 두 제품으로 보호되는 모든 일반 데이터는 BlueXP 랜섬웨어 보호로만 청구됩니다.

BYOL을 설정하거나 PAYGO 구독을 구입하면 BlueXP 디지털 지갑 * 데이터 서비스 라이센스 * 탭에서 라이센스를 확인하거나 BlueXP 디지털 지갑 * 구독 * 탭에서 활성 구독을 확인할 수 있습니다.

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

- 워크로드 및 워크로드 상태를 확인합니다.
- 워크로드 또는 정책 등의 리소스를 삭제합니다.
- 평가판 기간 동안 또는 라이센스에 따라 생성된 모든 예약된 작업을 실행합니다.

90일 무료 평가판을 사용해 보십시오

90일 무료 평가판을 사용하여 BlueXP 랜섬웨어 보호를 체험해 볼 수 있습니다. 무료 평가판을 시작하려면 계정 관리자여야 합니다.

> 시험판 평가 중에는 용량 제한이 적용되지 않습니다.

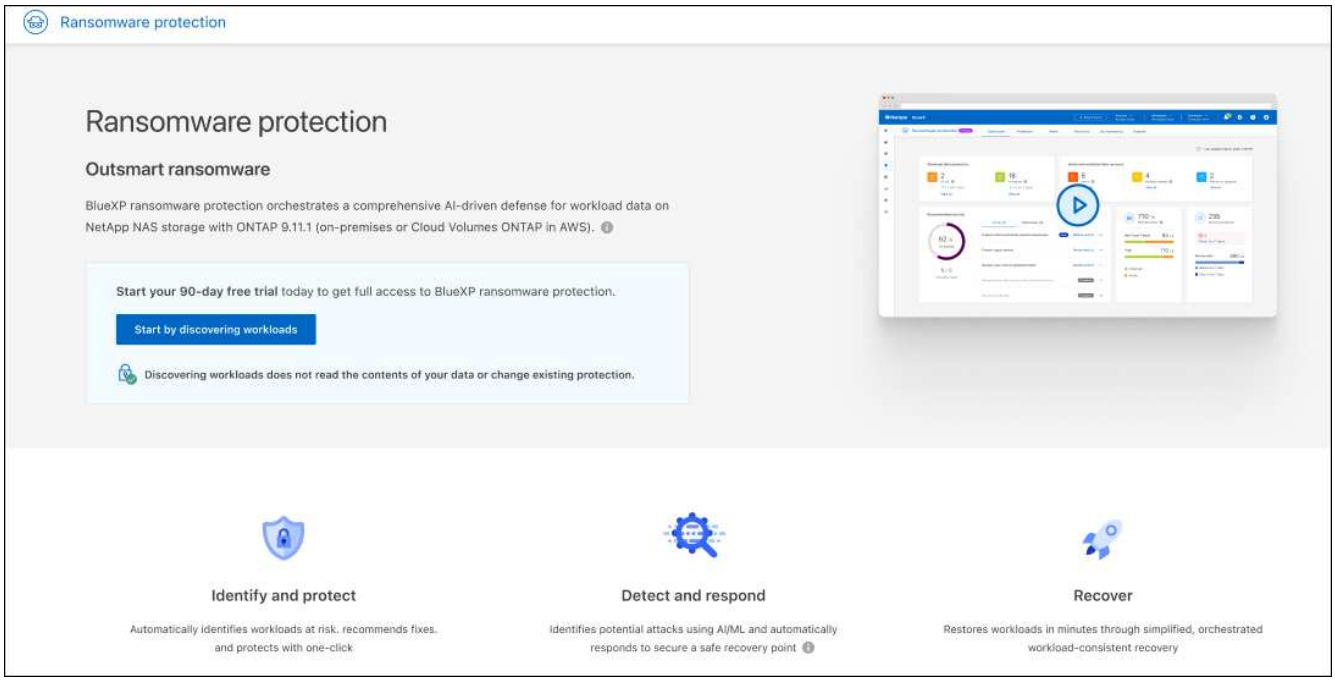
언제든지 라이선스를 받거나 가입할 수 있으며 90일 평가판이 종료될 때까지 비용이 청구되지 않습니다. 90일 평가판 사용 후 계속 진행하려면 BYOL 라이선스 또는 PAYGO 구독을 구매해야 합니다.

평가판 사용 중에는 모든 기능을 사용할 수 있습니다.

단계

1. 에 액세스합니다 "BlueXP 콘솔".
2. BlueXP에 로그인합니다.
3. BlueXP 왼쪽 탐색 창에서 * 보호 * > * 랜섬웨어 방어 * 를 선택하십시오.

   이 서비스에 처음 로그인하는 경우 랜딩 페이지가 나타납니다.



4. 다른 서비스에 대한 커넥터를 아직 추가하지 않은 경우 추가합니다.

   커넥터를 추가하려면 을 참조하십시오 "커넥터에 대해 자세히 알아보십시오".

5. 커넥터를 설정한 후 BlueXP 랜섬웨어 방어 랜딩 페이지에서 커넥터 변경 사항을 버튼을 클릭하여 워크로드 검색을 위한 버튼에 추가합니다. 워크로드 검색으로 시작 * 을 선택합니다.
6. 무료 평가판 정보를 검토하려면 오른쪽 상단의 드롭다운 옵션을 선택합니다.

평가판이 종료되면 구독 또는 라이센스를 획득하십시오

무료 평가판이 끝난 후에는 AWS Marketplace를 통해 구독하거나 NetApp에서 라이센스를 구입할 수 있습니다.

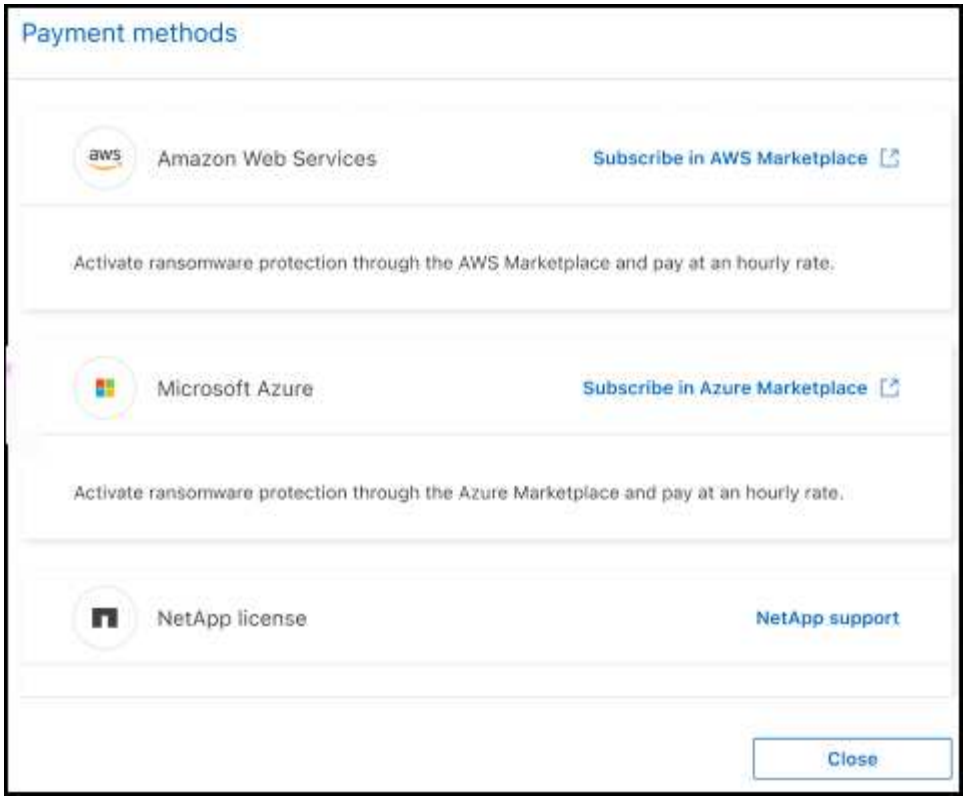
AWS Marketplace를 통해 구독 Microsoft Azure Marketplace를 통해 구독하십시오 BYOL(Bring Your Own License)

AWS Marketplace를 통해 구독

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

단계

1. BlueXP 랜섬웨어 보호에서 다음 중 하나를 수행합니다.
   - 무료 평가판이 만료된다는 메시지가 표시됩니다. 메시지에서 * 결제 방법 보기 * 를 선택합니다.
   - 오른쪽 상단의 * 무료 평가판 * 알림을 클릭하고 * 결제 방법 보기 * 를 선택합니다.

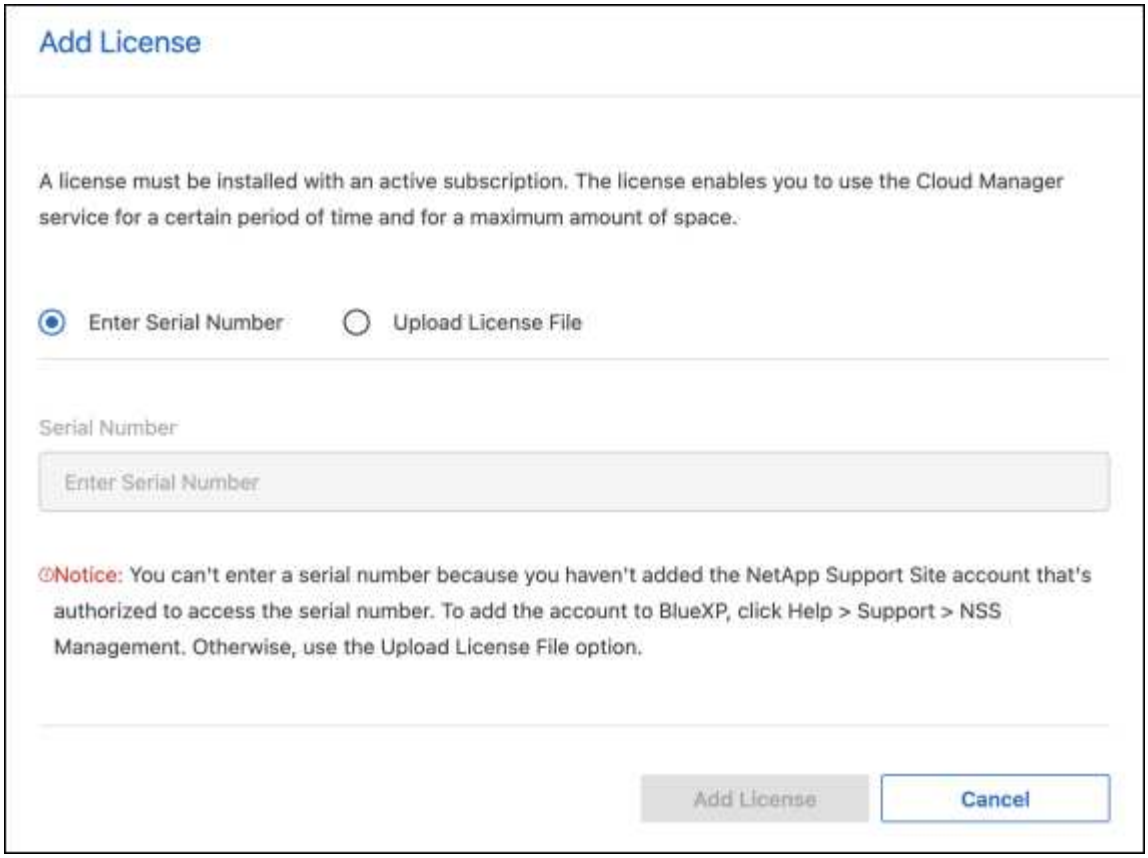


2. 지불 방법 페이지에서 * AWS Marketplace * 에서 구독 을 선택합니다.
3. AWS Marketplace에서 * 구매 옵션 보기 * 를 선택합니다.
4. AWS Marketplace를 사용하여 BlueXP 랜섬웨어 방어 체계를 구독하십시오.
5. BlueXP 랜섬웨어 방어로 돌아가면 구독 중이라는 메시지가 표시됩니다.

> BlueXP 랜섬웨어 방어 일련 번호가 포함되어 있고 AWS Marketplace에서 BlueXP 랜섬웨어 보호가 가입되어 있음을 나타내는 이메일이 발송됩니다.

6. BlueXP 랜섬웨어 방어 지불 방법 페이지로 돌아갑니다.
7. BlueXP에 라이센스 추가 * 를 선택하여 BlueXP에 라이센스를 추가합니다.

   BlueXP 디지털 지갑 서비스에 라이센스 추가 페이지가 표시됩니다.



8. BlueXP 디지털 지갑의 라이센스 추가 페이지에서 * 일련 번호 입력 * 을 선택하고 전송된 이메일에 포함된 일련 번호를 입력한 다음 * 라이센스 추가 * 를 선택합니다.
9. BlueXP 디지털 지갑에서 라이센스 세부 정보를 보려면 BlueXP 왼쪽 탐색 창에서 * Governance * > * Digital Wallet * 를 선택합니다.
   - 구독 정보를 보려면 * 구독 * 을 선택합니다.
   - BYOL 라이센스를 보려면 * Data Services Licenses * 를 선택합니다.

10. BlueXP 랜섬웨어 방어로 되돌아갑니다. BlueXP 왼쪽 탐색 창에서 * 보호 * > * 랜섬웨어 방어 * 를 선택하십시오.

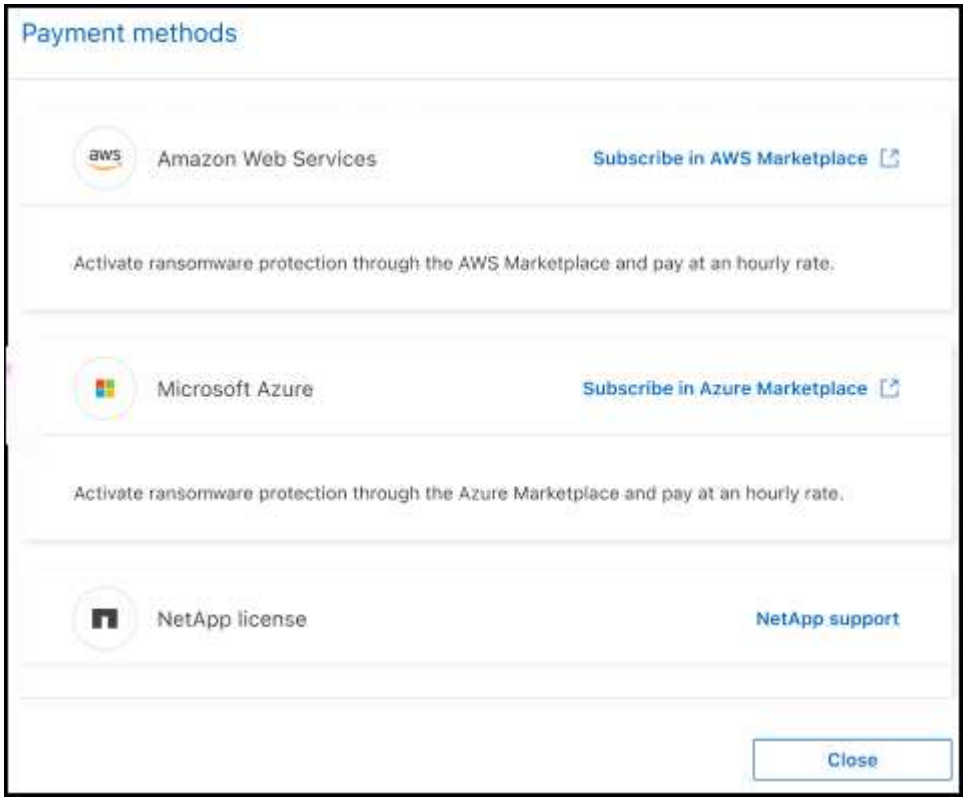
라이센스가 추가되었다는 메시지가 나타납니다.

Microsoft Azure Marketplace를 통해 구독하십시오

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

단계

1. BlueXP 랜섬웨어 보호에서 다음 중 하나를 수행합니다.
   - 무료 평가판이 만료된다는 메시지가 표시됩니다. 메시지에서 * 결제 방법 보기 * 를 선택합니다.
   - 오른쪽 상단의 * 무료 평가판 * 알림을 클릭하고 * 결제 방법 보기 * 를 선택합니다.

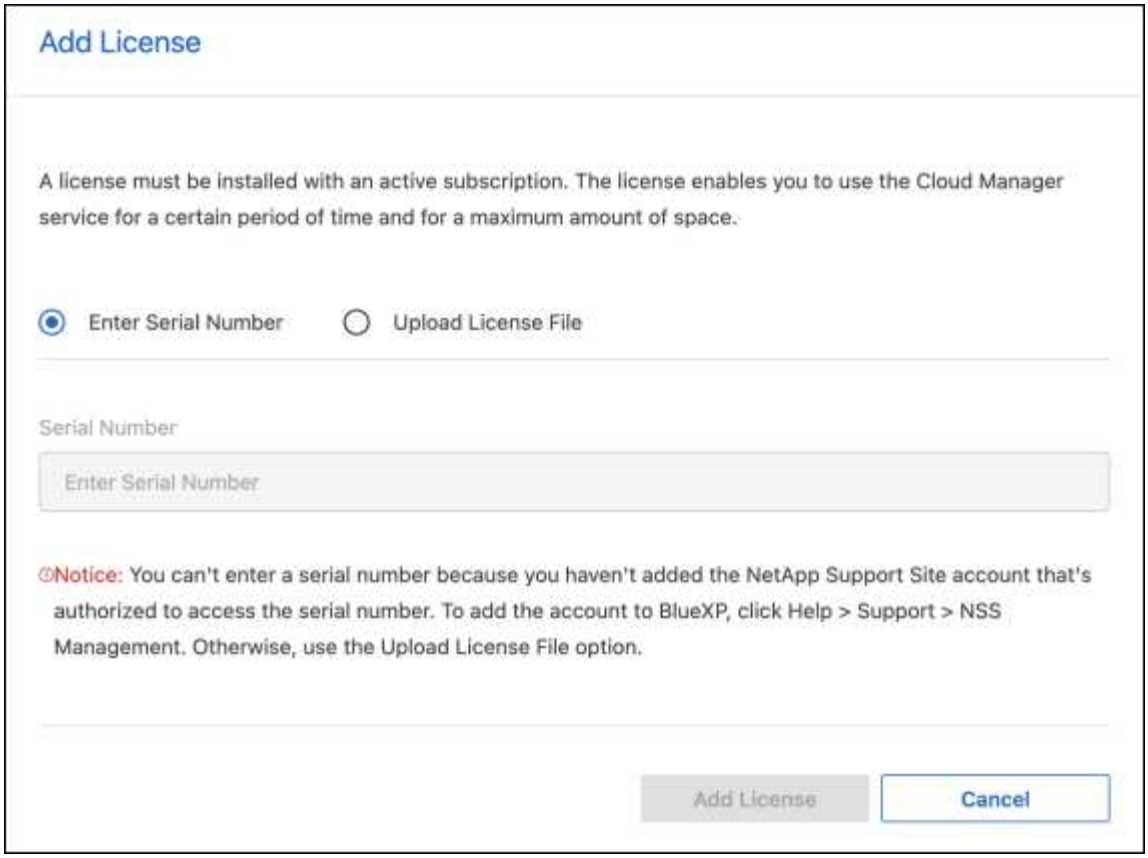


2. 결제 방법 페이지에서 * Azure Marketplace * 에서 구독 을 선택합니다.
3. Azure Marketplace에서 * 구매 옵션 보기 * 를 선택합니다.
4. Azure Marketplace를 사용하여 BlueXP 랜섬웨어 방어 서비스에 가입하십시오.
5. BlueXP 랜섬웨어 방어로 돌아가면 구독 중이라는 메시지가 표시됩니다.

   BlueXP 랜섬웨어 방어 일련 번호가 포함되어 있고 BlueXP 랜섬웨어 보호가 Azure Marketplace에서 구독되어 있음을 나타내는 이메일이 발송됩니다.

6. BlueXP 랜섬웨어 방어 지불 방법 페이지로 돌아갑니다.
7. BlueXP에 라이센스 추가 * 를 선택하여 BlueXP에 라이센스를 추가합니다.

   BlueXP 디지털 지갑 서비스에 라이센스 추가 페이지가 표시됩니다.



8. BlueXP 디지털 지갑의 라이센스 추가 페이지에서 * 일련 번호 입력 * 을 선택하고 전송된 이메일에 포함된 일련 번호를 입력한 다음 * 라이센스 추가 * 를 선택합니다.
9. BlueXP 디지털 지갑에서 라이센스 세부 정보를 보려면 BlueXP 왼쪽 탐색 창에서 * Governance * > * Digital Wallet * 를 선택합니다.
   - 구독 정보를 보려면 * 구독 * 을 선택합니다.
   - BYOL 라이센스를 보려면 * Data Services Licenses * 를 선택합니다.

10. BlueXP 랜섬웨어 방어로 되돌아갑니다. BlueXP 왼쪽 탐색 창에서 * 보호 * > * 랜섬웨어 방어 * 를 선택하십시오.

라이센스가 추가되었다는 메시지가 나타납니다.

BYOL(Bring Your Own License)

자체 라이센스(BYOL)를 사용하려면 라이센스를 구매하고 NetApp 라이센스 파일(NLF)을 받아 BlueXP 디지털 지갑에 라이센스를 추가해야 합니다.

- 라이센스 파일을 BlueXP 디지털 지갑에 추가합니다 *

NetApp 세일즈 담당자로부터 BlueXP 랜섬웨어 방어 라이센스를 구입한 후에는 BlueXP 랜섬웨어 방어 일련 번호 및 NSS(NetApp Support 사이트) 계정 정보를 입력하여 라이센스를 활성화합니다.

시작하기 전에

시작하기 전에 다음 정보가 필요합니다.

- BlueXP 랜섬웨어 방어 일련번호

  판매 주문에서 이 번호를 찾거나 계정 팀에 문의하여 이 정보를 확인하십시오.

- BlueXP 계정 ID

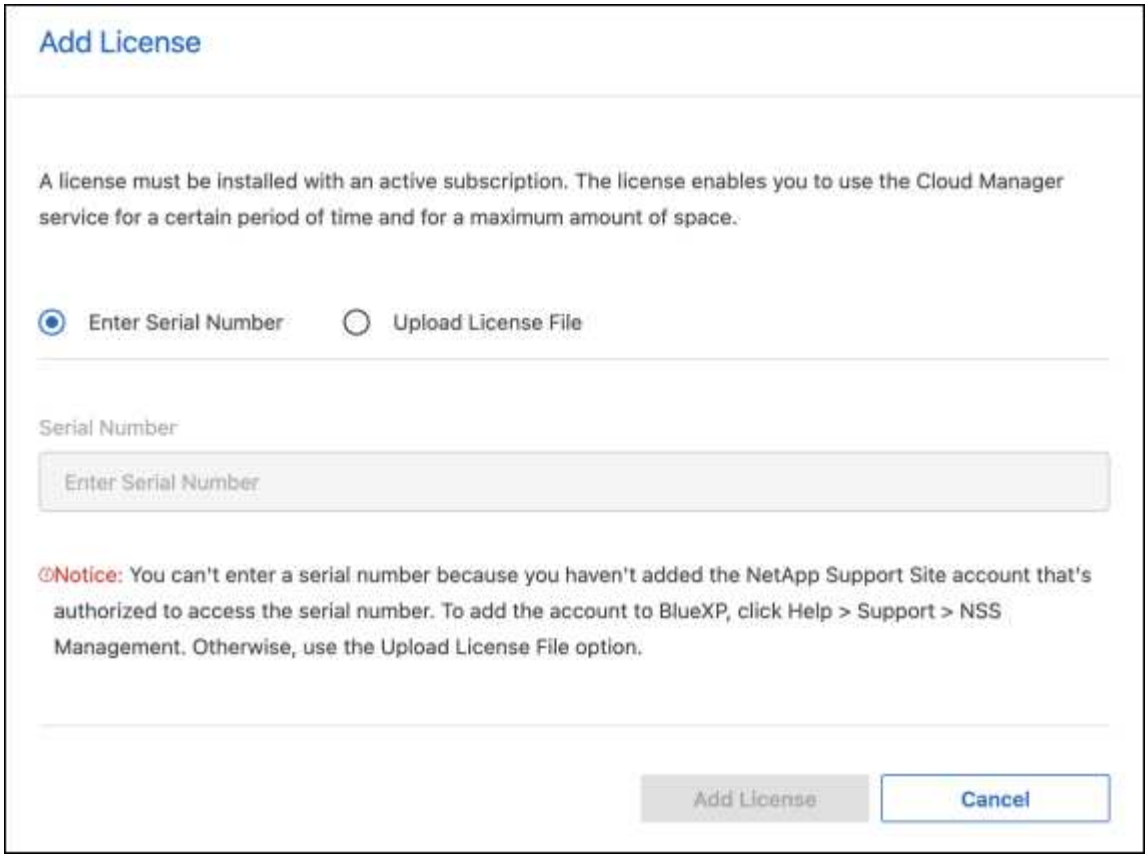
  BlueXP의 상단에서 * 계정 * 드롭다운을 선택한 다음 계정 옆의 * 계정 관리 * 를 선택하면 BlueXP 계정 ID를 찾을 수 있습니다. 계정 ID는 개요 탭에 있습니다.

단계

1. 라이센스를 가져온 후 BlueXP 랜섬웨어 방어 기능으로 돌아갑니다. 오른쪽 상단의 * 결제 방법 보기 * 옵션을 선택합니다. 또는 무료 평가판이 만료된다는 메시지에서 * 라이센스 가입 또는 구매 * 를 선택합니다.
2. BlueXP에 라이센스 추가 * 를 선택합니다.

   BlueXP 디지털 지갑으로 이동하게 됩니다.

3. BlueXP 디지털 지갑의 * Data Services Licenses * 탭에서 * Add license * 를 선택합니다.



4. 라이센스 추가 페이지에서 일련 번호와 NetApp Support 사이트 계정 정보를 입력합니다.
   - BlueXP 라이센스 일련 번호를 알고 있고 NSS 계정을 알고 있는 경우 * Enter Serial Number * 옵션을 선택하고 해당 정보를 입력합니다.

     드롭다운 목록에서 NetApp Support 사이트 계정을 사용할 수 없는 경우 "NSS 계정을 BlueXP에 추가합니다".
   - BlueXP 라이센스 파일(다크 사이트에 설치 시 필요)이 있는 경우 * Upload License File * 옵션을 선택하고 화면의 지침에 따라 파일을 첨부합니다.
5. 라이센스 추가 * 를 선택합니다.

결과

BlueXP 디지털 지갑에 라이센스로 BlueXP 랜섬웨어 보호가 표시됩니다.

BlueXP 라이센스가 만료되면 업데이트하십시오

라이센스 기간이 만료일이 가까워지거나 라이센스 용량이 한계에 도달하는 경우 BlueXP 재해 랜섬웨어 보호 UI에서 알림을 받게 됩니다. BlueXP 랜섬웨어 방어 라이센스가 만료되기 전에 업데이트하여 스캔한 데이터에 액세스하는 데 중단이 없도록 합니다.

이 메시지는 BlueXP 디지털 지갑과 에도 표시됩니다 "알림".

단계

1. BlueXP 오른쪽 하단에 있는 채팅 아이콘을 선택하여 특정 일련 번호에 대한 라이센스의 추가 용량 또는 용어의 연장을 요청합니다. 라이센스 업데이트를 요청하는 전자 메일을 보낼 수도 있습니다.

라이센스 비용을 지불하고 NetApp Support 사이트에 등록한 후 BlueXP는 BlueXP 디지털 지갑의 라이센스를 자동으로 업데이트하고 데이터 서비스 라이센스 페이지에 변경 내용이 5-10분 내에 반영됩니다.

2. BlueXP에서 라이센스를 자동으로 업데이트할 수 없는 경우(예: 어두운 사이트에 설치된 경우) 라이센스 파일을 수동으로 업로드해야 합니다.
   a. NetApp Support 사이트에서 라이센스 파일을 얻을 수 있습니다.
   b. BlueXP 디지털 지갑에 액세스합니다.
   c. 데이터 서비스 라이센스 * 탭을 선택하고 업데이트할 서비스 일련 번호에 해당하는 * 작업… * 아이콘을 선택한 다음 * 라이센스 업데이트 * 를 선택합니다.

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.

BlueXP 랜섬웨어 방어 기능은 MySQL 애플리케이션, Oracle 애플리케이션, VMware 데이터 저장소 및 파일 공유를 평가합니다.

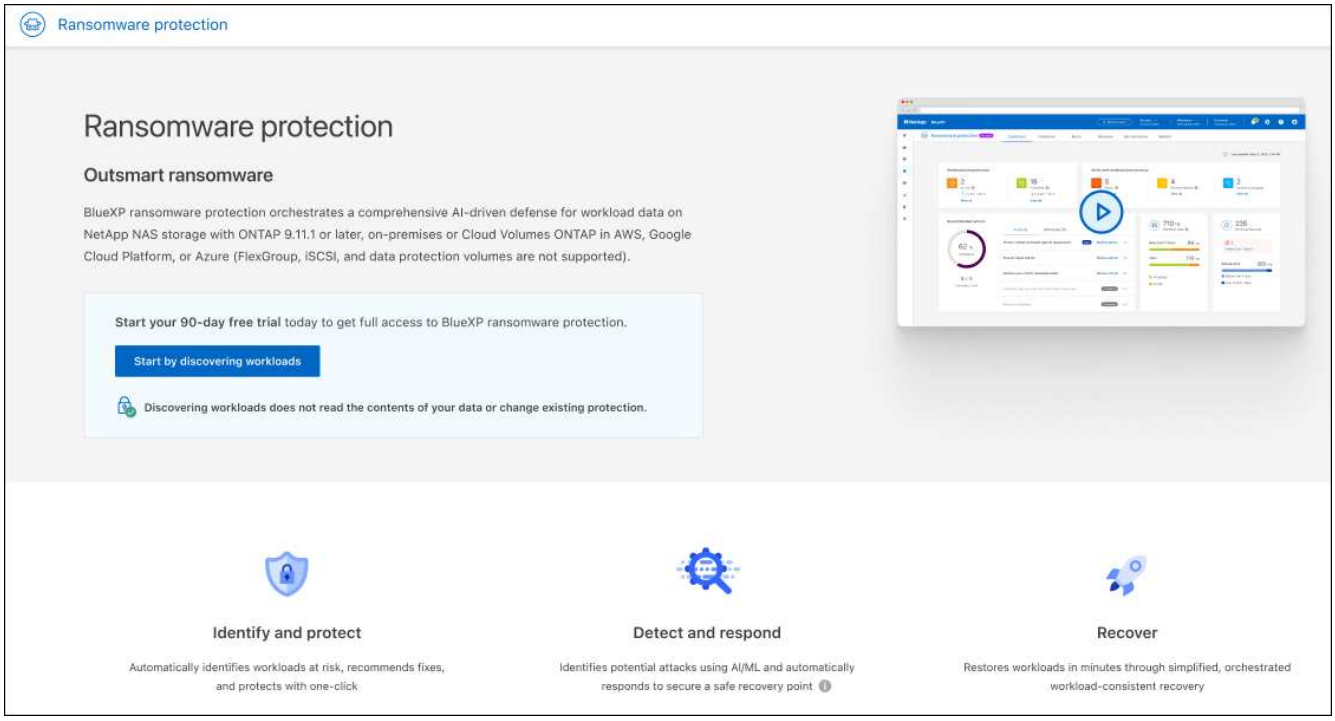
> FlexGroup 또는 iSCSI를 사용하는 볼륨이 있는 워크로드는 검색되지 않습니다.

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

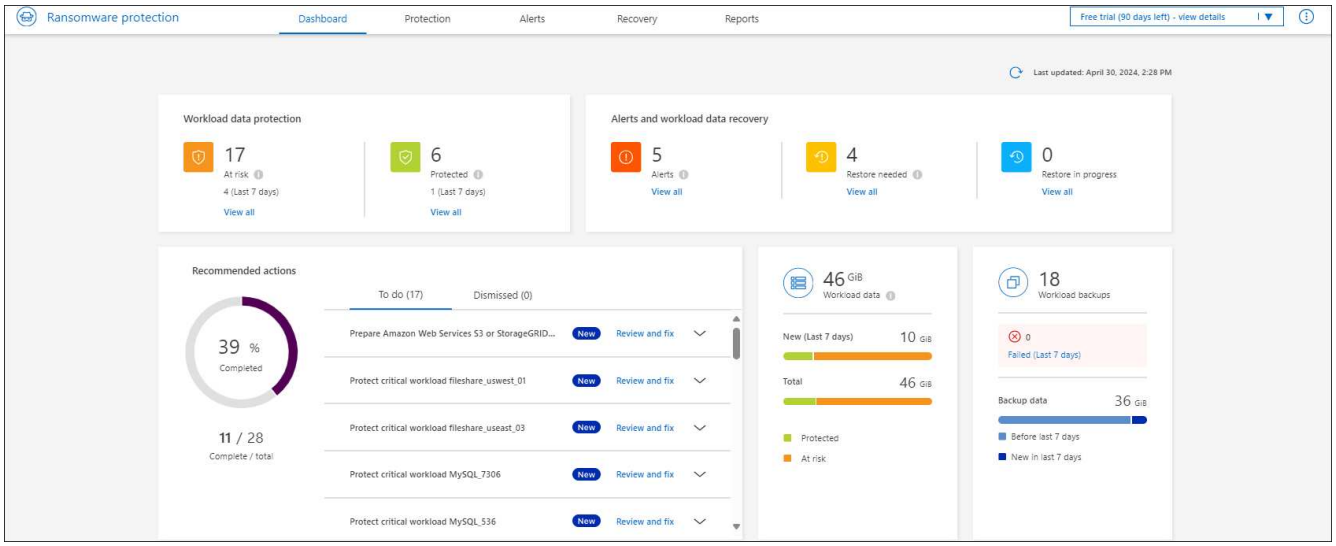
1. BlueXP 왼쪽 탐색 창에서 * 보호 * > * 랜섬웨어 방어 * 를 선택하십시오.

   이 서비스에 처음 로그인하는 경우 랜딩 페이지가 나타납니다.



2. 초기 랜딩 페이지에서 * 워크로드 검색으로 시작 * 을 선택합니다.

   이 서비스는 워크로드 데이터를 검색하고 데이터 보호 상태를 대시보드에 표시합니다.



   "대시보드에 표시되는 내용을 알아봅니다."

BlueXP 랜섬웨어 보호 설정을 구성합니다

대시보드에서 권장 사항을 검토하거나 * 설정 * 옵션에 액세스하여 백업 대상을 구성하거나 위협 감지를 활성화할 수 있습니다.

위협 감지를 활성화하면 위협 분석을 위해 데이터를 SIEM(보안 및 이벤트 관리 시스템)으로 자동으로 전송합니다.

설정 페이지에 직접 액세스합니다

상단 메뉴 근처의 동작 옵션에서 설정 페이지에 쉽게 액세스할 수 있습니다.

1. BlueXP 랜섬웨어 방어 메뉴에서 업종을 선택합니다 ⋮ 오른쪽 위에 있는 옵션.
2. 드롭다운 메뉴에서 * 설정 * 을 선택합니다.
3. 설정 페이지에서 다음을 수행할 수 있습니다.
   - 백업 대상을 추가합니다.
   - 보안 및 이벤트 관리 시스템(SIEM)을 연결하여 위협 분석 및 감지를 수행할 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)
- Google 클라우드 플랫폼
- Microsoft Azure를 참조하십시오

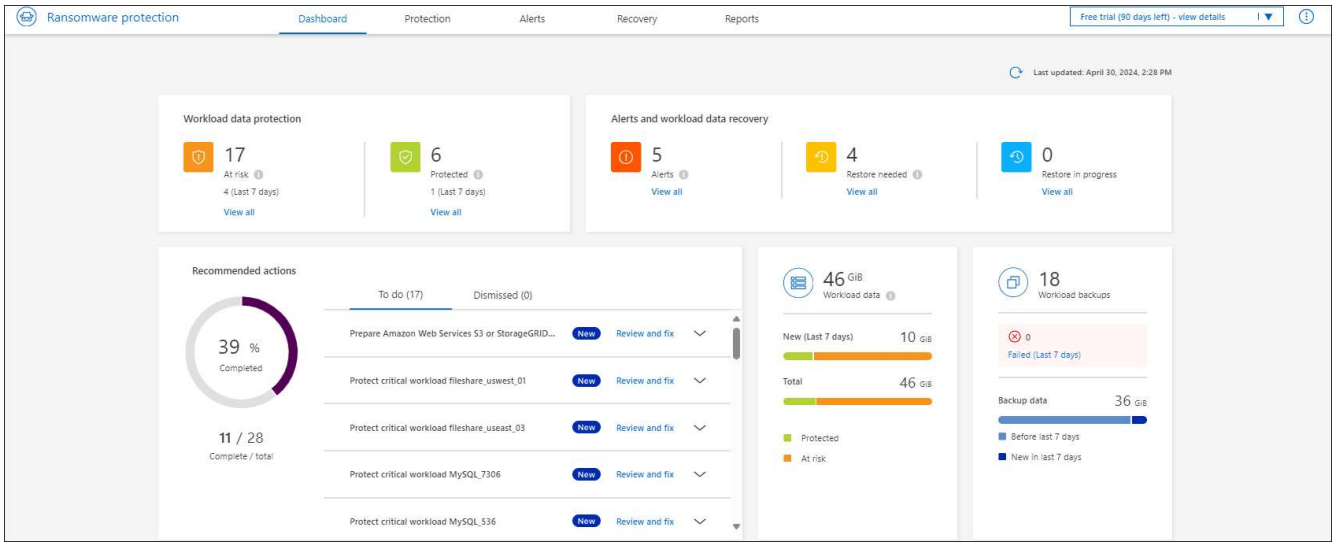
대시보드에서 권장하는 작업에 따라 백업 대상을 추가할 수 있습니다.

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 "Prepare as a backup destination(백업 대상으로 <backup provider> 준비)"의 권장 사항에 대해 * Review and fix(검토 및 수정) * 를 선택합니다.
4. 백업 공급자에 따라 지침을 계속합니다.

Actions(작업) 드롭다운 메뉴에서 **Backup Destination(백업 대상)** 옵션에 액세스합니다

상단 메뉴 근처의 동작 옵션에서 설정 페이지에 쉽게 액세스할 수 있습니다.

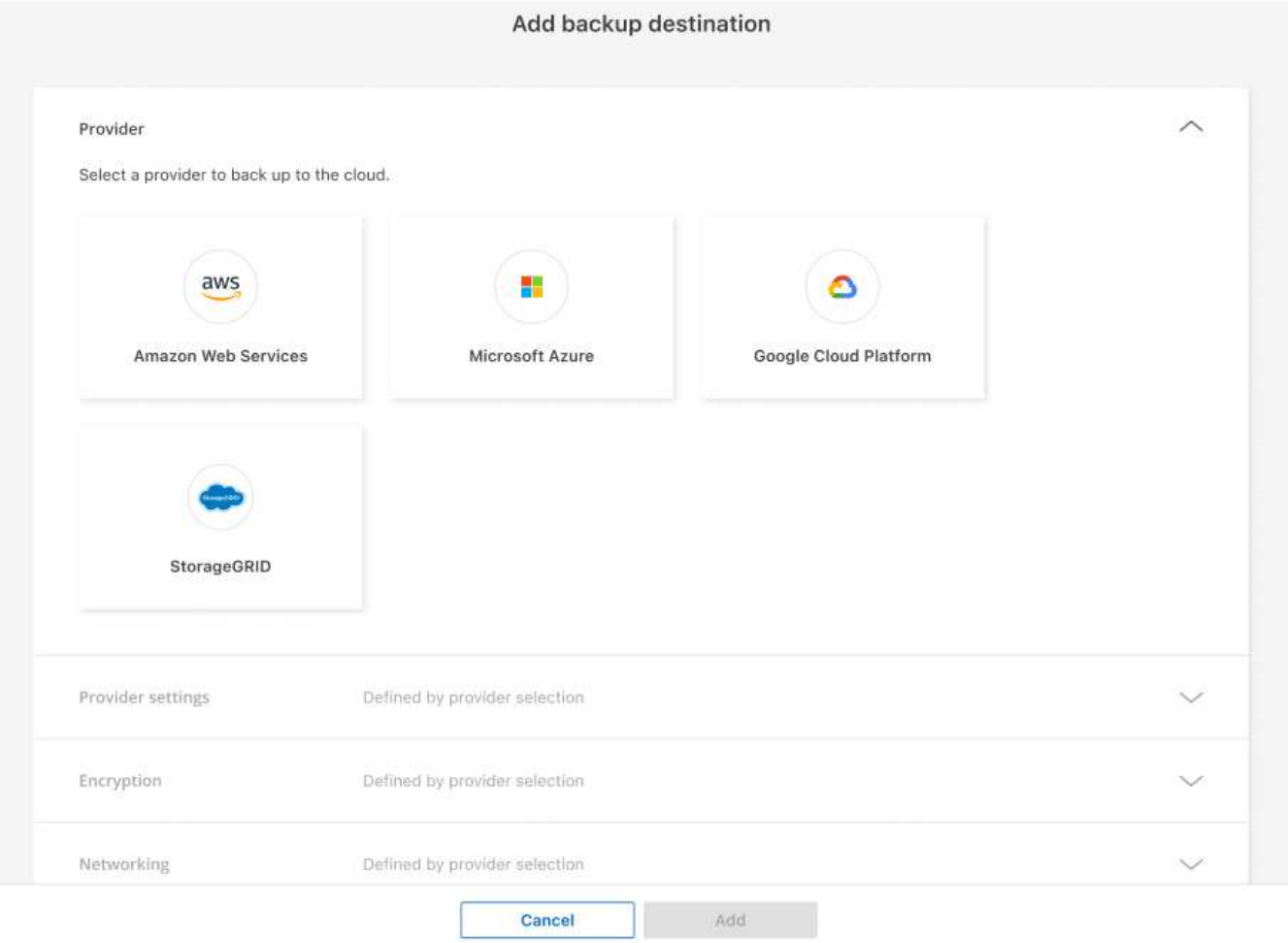
1. BlueXP 랜섬웨어 방어 메뉴에서 업종을 선택합니다 ⋮ 오른쪽 위에 있는 옵션.
2. 드롭다운 메뉴에서 * 설정 * 을 선택합니다.
3. 백업 대상을 추가하려면 * 추가 * 를 선택합니다.

StorageGRID를 백업 대상으로 추가합니다

NetApp StorageGRID를 백업 대상으로 설정하려면 다음 정보를 입력합니다.

1. 설정 > 백업 대상 * 페이지에서 * 추가 * 를 선택합니다.

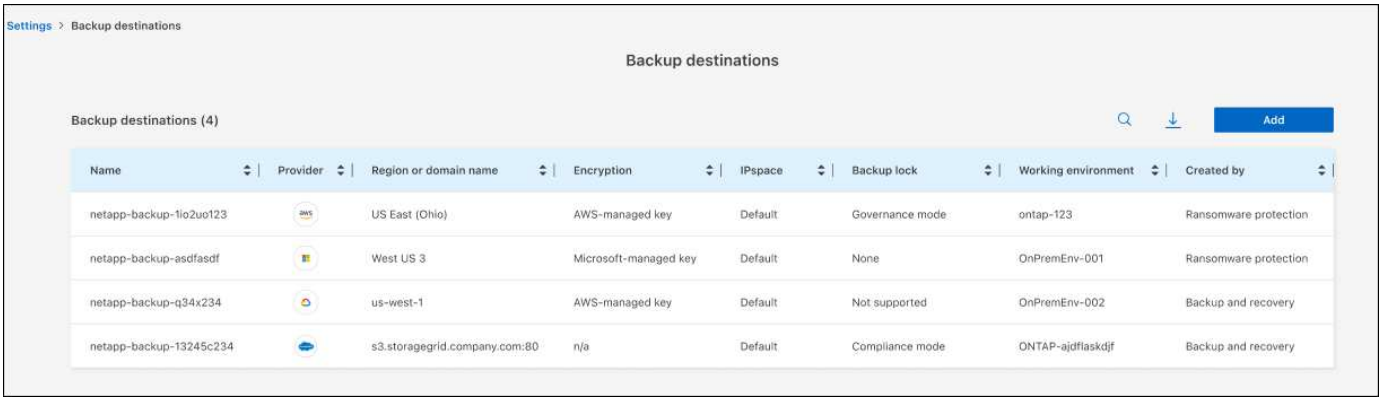
2. 백업 대상의 이름을 입력합니다.



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.
5. 추가 * 를 선택합니다.

결과

새 백업 대상이 백업 대상 목록에 추가됩니다.

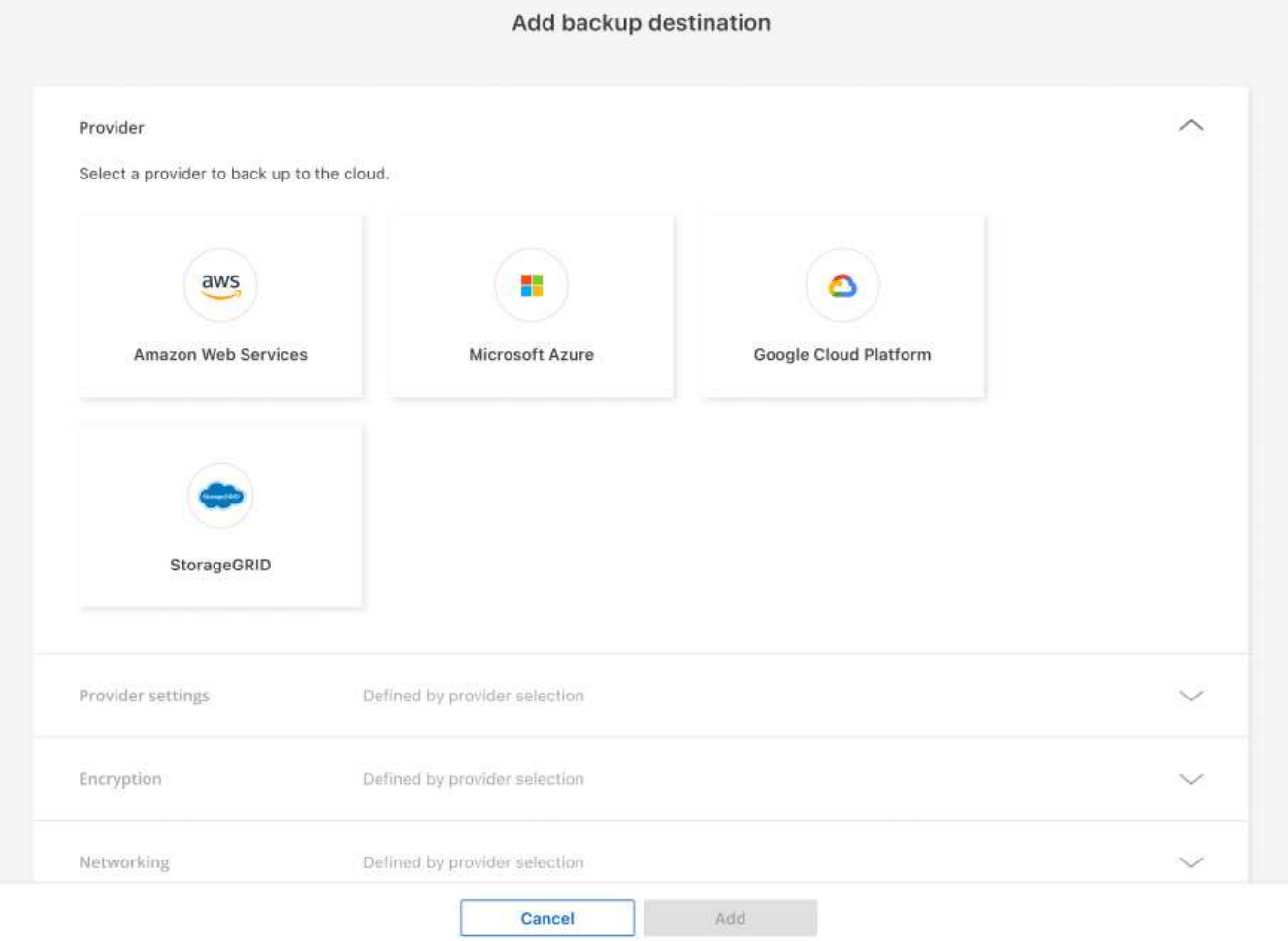


Amazon Web Services를 백업 대상으로 추가합니다

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.

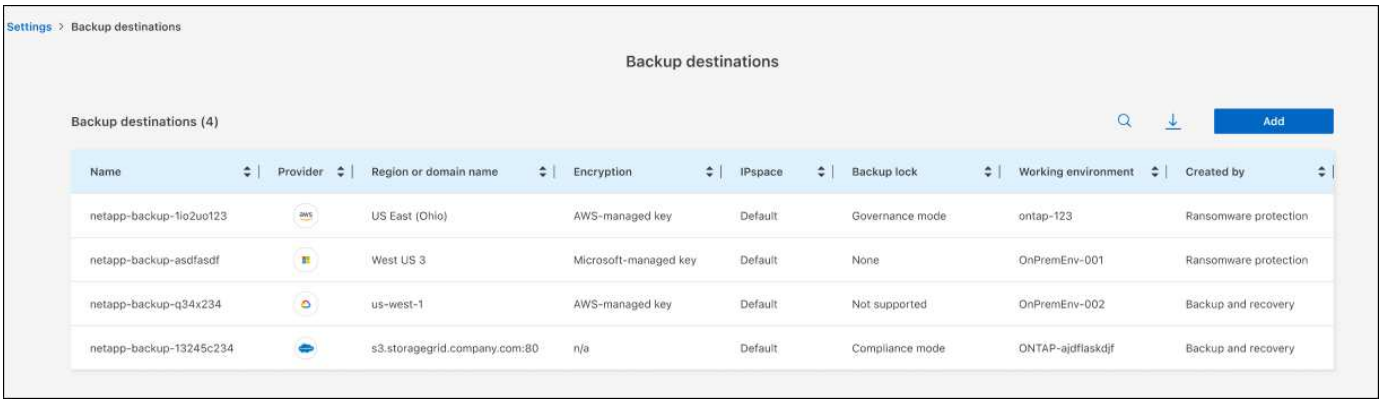
  > 지금 백업 잠금 설정을 구성하는 경우 백업 대상을 구성한 후에는 나중에 설정을 변경할 수 없습니다.

  - * 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.

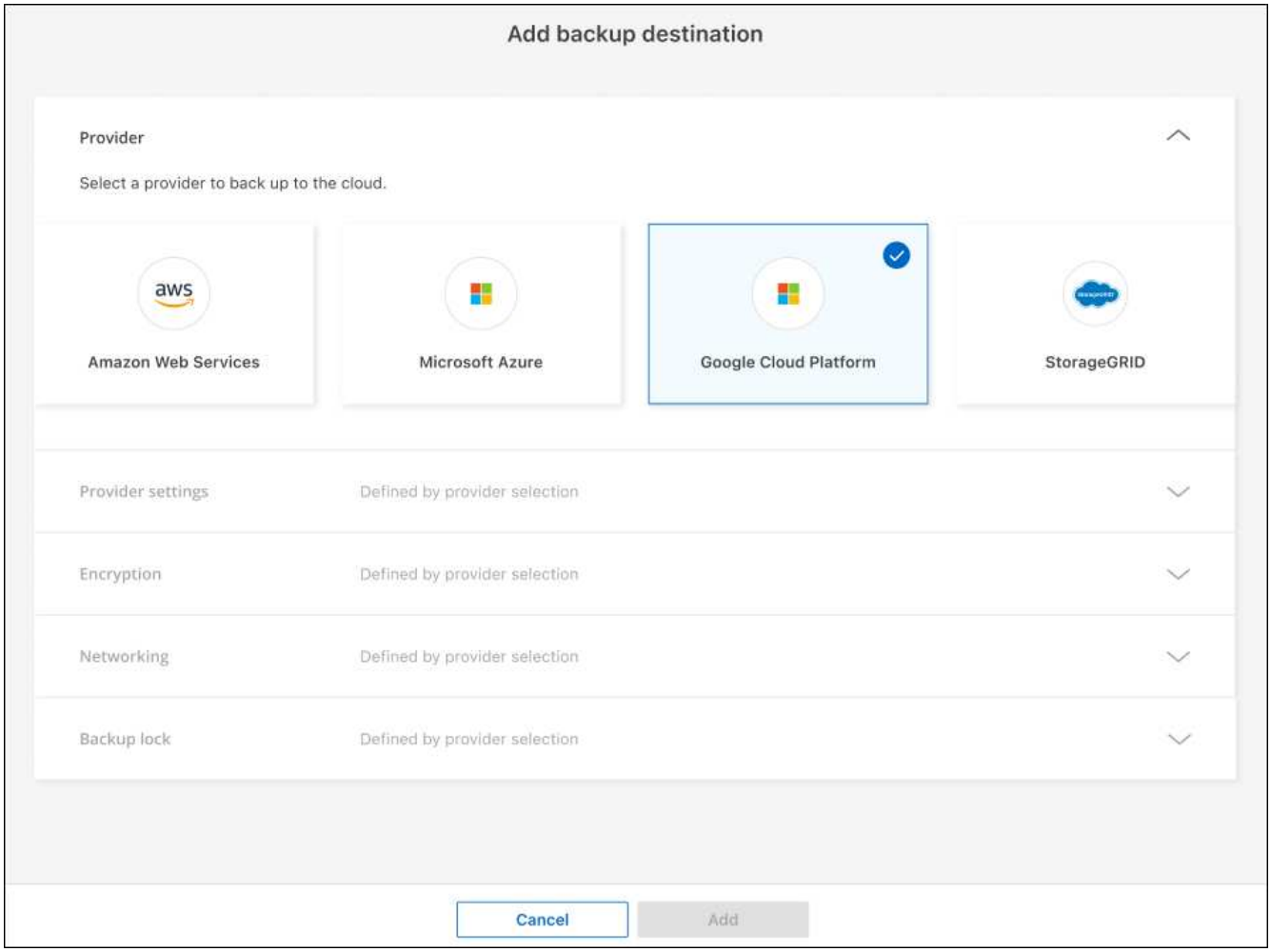


Google Cloud Platform을 백업 대상으로 추가합니다

GCP(Google Cloud Platform)를 백업 대상으로 설정하려면 다음 정보를 입력합니다.

BlueXP 에서 GCP 스토리지를 관리하는 방법에 대한 자세한 내용은 을 참조하십시오 "Google Cloud의 커넥터 설치 옵션".

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



3. Google Cloud Platform * 을 선택합니다.
4. 각 설정 옆에 있는 아래쪽 화살표를 선택하고 값을 입력하거나 선택합니다.
   - * 공급자 설정 *:
     - 새 버킷을 만듭니다. 액세스 키와 비밀 키를 입력합니다.
     - Google Cloud Platform 프로젝트 및 지역을 입력하거나 선택합니다.
   - * 암호화 * : 새 버킷을 만드는 경우 제공자로부터 받은 암호화 키 정보를 입력하십시오. 기존 버킷을 선택한 경우 암호화 정보를 이미 사용할 수 있습니다.

     버킷의 데이터는 기본적으로 Google 관리형 키로 암호화된다. Google에서 관리하는 키를 계속 사용할 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 GCP 개인 끝점(PrivateLink)을 사용할지 여부를 선택합니다.

5. 추가 * 를 선택합니다.

결과

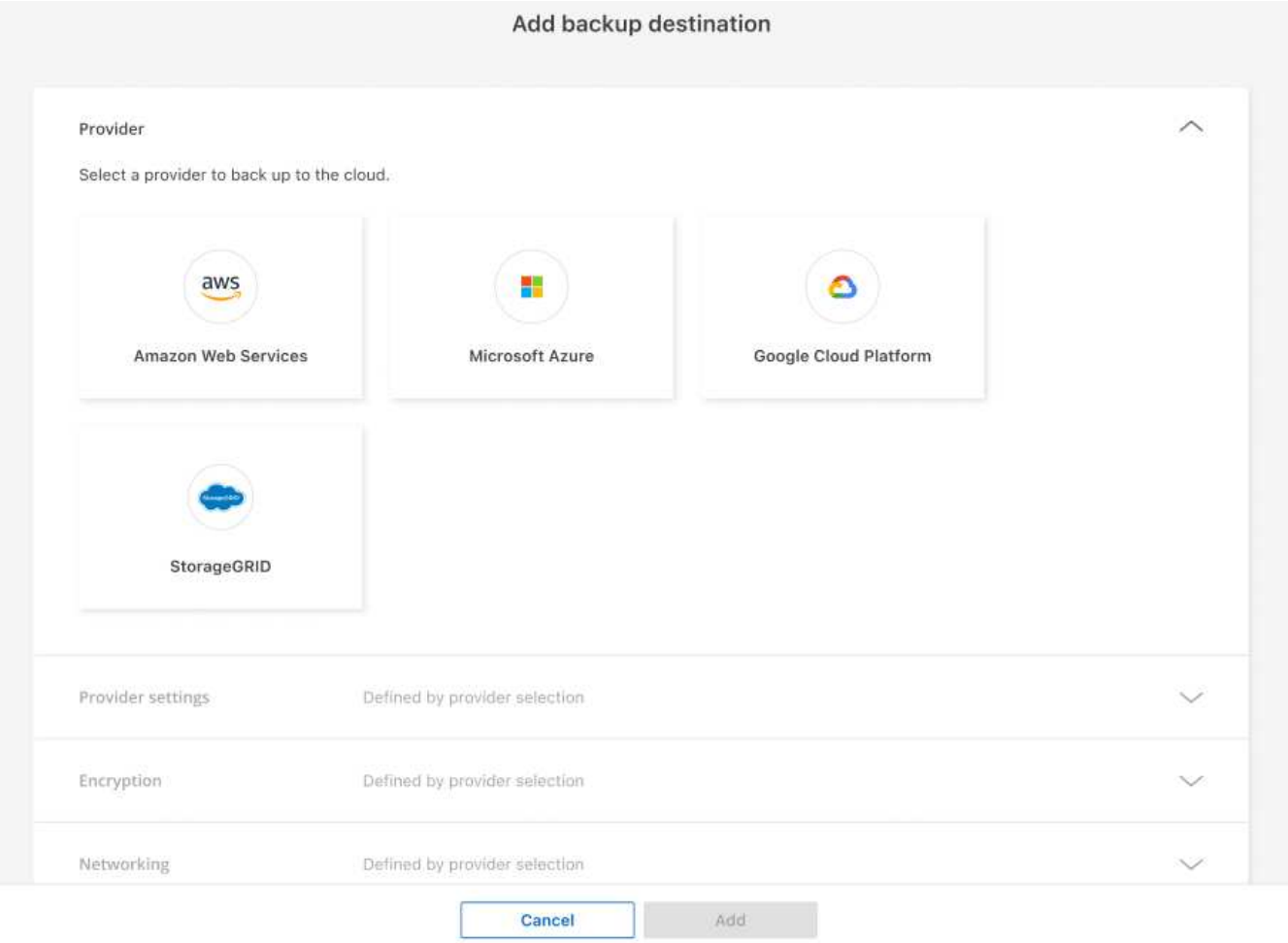
새 백업 대상이 백업 대상 목록에 추가됩니다.

Microsoft Azure를 백업 대상으로 추가합니다

Azure를 백업 대상으로 설정하려면 다음 정보를 입력합니다.

BlueXP에서 Azure 자격 증명 및 마켓플레이스 가입을 관리하는 방법에 대한 자세한 내용은 를 참조하십시오 "Azure 자격 증명 및 마켓플레이스 가입을 관리합니다".

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



3. Azure * 를 선택합니다.
4. 각 설정 옆에 있는 아래쪽 화살표를 선택하고 값을 입력하거나 선택합니다.

- * 공급자 설정 *:
  - 새 스토리지 계정을 생성하고, BlueXP에 이미 있는 기존 계정을 선택하거나, 백업을 저장할 자체 스토리지 계정을 가져옵니다.
  - Azure 자격 증명을 위한 Azure 구독, 지역 및 리소스 그룹

    "자체 스토리지 계정을 사용하려면 Azure Blob 스토리지 계정 추가 를 참조하십시오".

- * 암호화 *: 새 저장소 계정을 만드는 경우 공급자로부터 받은 암호화 키 정보를 입력합니다. 기존 계정을 선택한 경우 암호화 정보를 사용할 수 있습니다.

  계정의 데이터는 기본적으로 Microsoft에서 관리하는 키로 암호화됩니다. Microsoft에서 관리하는 키를 계속 사용하거나 사용자 고유의 키를 사용하여 데이터 암호화를 관리할 수 있습니다.

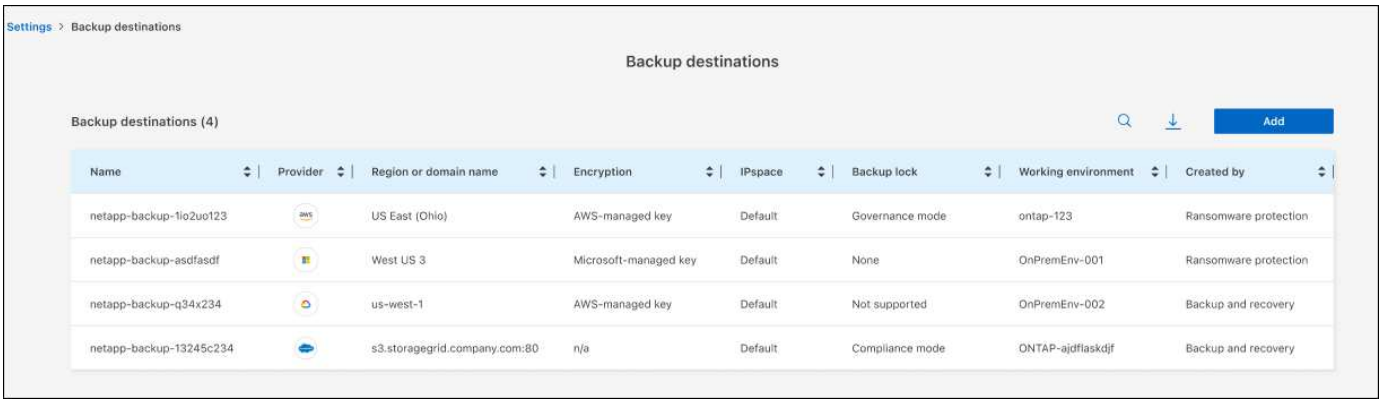
- * 네트워킹 * : IPspace를 선택하고 개인 엔드포인트를 사용할 것인지 여부를 선택하십시오.
  - IPspace는 백업하려는 볼륨이 상주하는 클러스터입니다. 이 IPspace용 인터클러스터 LIF는 아웃바운드 인터넷 액세스를 가져야 합니다.
  - 필요한 경우 이전에 구성한 Azure 개인 끝점을 사용할지 여부를 선택합니다.

    Azure PrivateLink를 사용하려면 을 참조하십시오 "Azure PrivateLink입니다".

5. 추가 * 를 선택합니다.

결과

새 백업 대상이 백업 대상 목록에 추가됩니다.



위협 감지를 활성화합니다

위협 분석 및 감지를 위해 SIEM(Security and Event Management System)으로 데이터를 자동으로 전송할 수 있습니다. AWS Security Hub 또는 Splunk Cloud를 SIEM으로 선택할 수 있습니다.

BlueXP 랜섬웨어 차단에서 SIEM을 활성화하려면 AWS 보안 허브 또는 Splunk Cloud를 구성해야 합니다.

위협 감지를 위해 **AWS Security Hub**를 구성합니다

BlueXP 랜섬웨어 차단에서 AWS 보안 허브를 활성화하기 전에 AWS 보안 허브에서 다음과 같은 개괄적인 단계를 수행해야 합니다.

- AWS Security Hub에서 사용 권한을 설정합니다.

- AWS Security Hub에서 인증 액세스 키 및 비밀 키를 설정합니다. (이 단계는 여기에 제공되지 않습니다.)

AWS Security Hub에서 사용 권한을 설정하는 단계입니다

1. AWS IAM 콘솔 * 으로 이동합니다.
2. Policies * 를 선택합니다.
3. JSON 형식으로 다음 코드를 사용하여 정책을 생성합니다.

```
{
  "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 감지를 위해 **Splunk Cloud**를 구성합니다

BlueXP 랜섬웨어 차단에서 Splunk Cloud를 사용하려면 먼저 Splunk Cloud에서 다음과 같은 개괄적인 단계를 수행해야 합니다.

- BlueXP 의 HTTP 또는 HTTPS를 통해 이벤트 데이터를 수신하도록 Splunk Cloud에서 HTTP 이벤트 수집기를 설정합니다.
- Splunk Cloud에서 이벤트 수집기 토큰을 생성합니다.

Splunk에서 **HTTP** 이벤트 수집기를 활성화하는 단계입니다

1. Splunk Cloud로 이동하십시오.
2. 설정 * > * 데이터 입력 * 을 선택합니다.
3. HTTP 이벤트 수집기 * > * 글로벌 설정 * 을 선택합니다.
4. 모든 토큰 토글에서 * 사용 * 을 선택합니다.
5. 이벤트 수집기가 HTTP가 아닌 HTTPS를 통해 수신 및 통신하도록 하려면 * SSL 활성화 * 를 선택합니다.
6. HTTP Event Collector의 HTTP Port Number * 에 포트를 입력합니다.

Splunk에서 이벤트 수집기 토큰을 생성하는 단계입니다

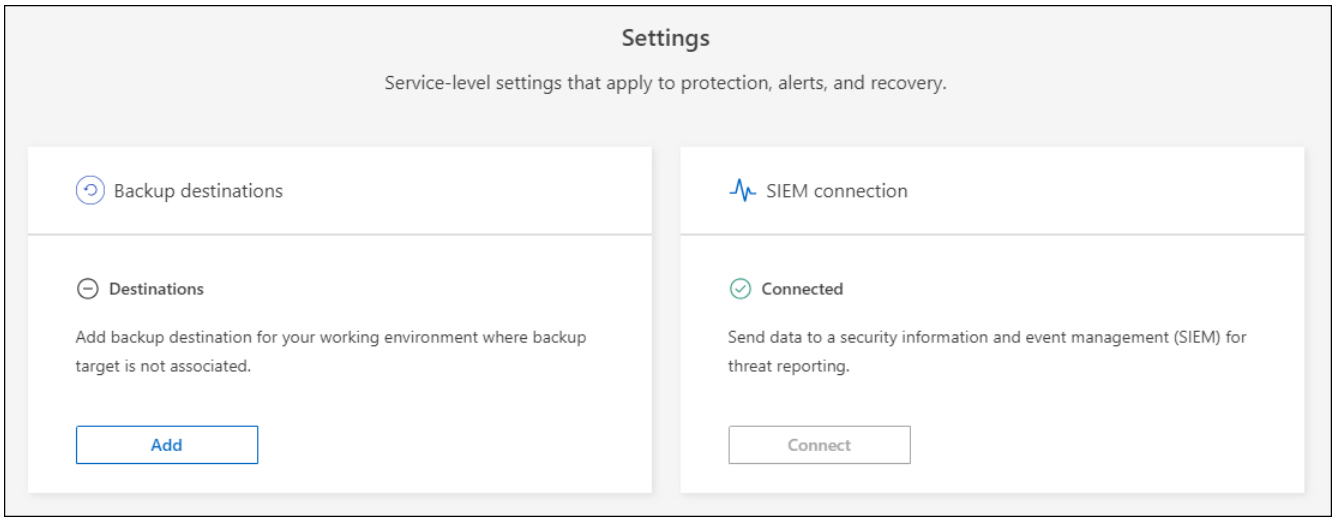
1. Splunk Cloud로 이동하십시오.
2. 설정 * > * 데이터 추가 * 를 선택합니다.
3. Monitor * > * HTTP Event Collector * 를 선택합니다.
4. 토큰의 이름을 입력하고 * Next * 를 선택합니다.
5. 이벤트가 푸시될 * 기본 색인 * 을 선택한 다음 * 검토 * 를 선택합니다.
6. 끝점에 대한 모든 설정이 올바른지 확인한 다음 * 제출 * 을 선택합니다.
7. 토큰을 복사하여 다른 문서에 붙여 넣어 인증 단계를 준비합니다.

BlueXP 랜섬웨어 방어에 **SIEM**을 연결하십시오

SIEM을 사용하면 위협 분석 및 보고를 위해 BlueXP 랜섬웨어 방어 기능에서 SIEM 서버로 데이터를 전송할 수 있습니다.

1. BlueXP 메뉴에서 * 보호 * > * 랜섬웨어 방어 * 를 선택합니다.
2. BlueXP 랜섬웨어 방어 메뉴에서 업종을 선택합니다 ⋮ 오른쪽 위에 있는 옵션.
3. 설정 * 을 선택합니다.

   설정 페이지가 나타납니다.



4. 설정 페이지의 SIEM 연결 창에서 * 연결 * 을 선택합니다.
5. AWS Security Hub 또는 Splunk Cloud에서 구성한 토큰 및 인증 세부 정보를 입력합니다.

   ℹ 입력하는 정보는 선택한 SIEM에 따라 다릅니다.

6. 활성화 * 를 선택합니다.

   설정 페이지에 "연결됨"이 표시됩니다.

SIEM 연결을 끊습니다

SIEM 연결을 해제하면 서비스가 SIEM 서버로 데이터를 전송하는 것을 중지합니다.

단계

1. BlueXP 메뉴에서 * 보호 * > * 랜섬웨어 방어 * 를 선택합니다.
2. BlueXP 랜섬웨어 방어 메뉴에서 업종을 선택합니다 오른쪽 위에 있는 옵션.
3. 설정 * 을 선택합니다.
4. SIEM 연결 창에서 * 연결 해제 * 를 선택합니다.
5. 확인 페이지에서 * 연결 해제 * 를 선택합니다.

BlueXP 랜섬웨어 방어에 관한 FAQ

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

구축

- BlueXP 랜섬웨어 보호를 사용하려면 라이센스가 필요하십니까? *

다음과 같은 라이센스 유형을 사용할 수 있습니다.

- 90일 무료 평가판을 신청하십시오.
- 곧 AWS(Amazon Web Services) Marketplace를 통해 PAYGO(용량제) 구독을 구입할 수 있습니다.
- 조만간 BYOL(Bring Your Own NetApp License File)이라는 BYOL(Bring Your Own License File)을 받을 수 있게 됩니다 NetApp 라이센스 일련 번호를 사용하여 BlueXP 디지털 지갑에서 BYOL을 활성화할 수 있습니다.
- BlueXP 랜섬웨어 보호를 어떻게 활성화하시겠습니까? *
  BlueXP 랜섬웨어 방어에 도움이 필요하지 않습니다. 랜섬웨어 방지 옵션은 BlueXP 왼쪽 탐색 창에서 자동으로 활성화됩니다.

이 서비스를 이용하려면 등록하거나 NetApp 영업 담당자에게 연락하여 이 서비스를 체험해 보십시오. BlueXP Connector를 사용하면 서비스에 적합한 기능이 여기에 포함됩니다.

BlueXP 랜섬웨어 보호를 시작하려면 초기 랜딩 페이지에서 "워크로드 발견 시작"을 클릭하십시오.

- BlueXP 랜섬웨어 방어는 표준, 제한 및 비공개 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

- BlueXP 랜섬웨어 방어 URL은 무엇입니까? *
  URL의 경우 브라우저에 다음을 입력합니다. "https://console.bluexp.netapp.com/" 를 눌러 BlueXP 콘솔에 액세스합니다.
- 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.
- BlueXP 랜섬웨어 방어는 BlueXP 백업 및 복구 및 SnapCenter와 어떻게 상호 작용합니까? *

BlueXP 랜섬웨어 방어는 다음 제품 및 서비스를 사용합니다.

- 파일 공유 워크로드에 대한 스냅샷 및 백업 정책을 검색하고 설정하는 BlueXP 백업 및 복구
- SnapCenter 또는 SnapCenter for VMware: 애플리케이션 및 VM 워크로드에 대한 스냅샷 및 백업 정책을 검색하고 설정합니다.

또한 BlueXP 랜섬웨어 방어 기능은 BlueXP 백업 및 복구와 SnapCenter/SnapCenter for VMware를 사용하여 파일 및 워크로드 정합성이 보장되는 복구를 수행합니다.

워크로드

- 워크로드를 구성하는 요소는 무엇입니까? * 워크로드는 애플리케이션, VM 또는 파일 공유입니다. 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? *
  데이터 우선 순위는 생성된 스냅샷 복사본과 예약된 백업에 의해 결정됩니다.

워크로드 우선순위(중요, 표준, 중요)는 워크로드와 관련된 각 볼륨에 이미 적용된 스냅샷 주파수에 따라 결정됩니다.

"워크로드 우선 순위 또는 중요도에 대해 알아보십시오".

- BlueXP 랜섬웨어 방어는 어떤 워크로드를 지원합니까? *

BlueXP 랜섬웨어 방어 기능은 Oracle, MySQL, 파일 공유, VM, VM 데이터 저장소와 같은 워크로드를 식별할 수 있습니다.

또한 고객이 SnapCenter 또는 SnapCenter for VMware를 사용 중인 경우 해당 제품에서 지원되는 모든 워크로드가 BlueXP 랜섬웨어 방어에서 확인되며 BlueXP 랜섬웨어 방어를 통해 워크로드를 일관적으로 보호하고 복구할 수 있습니다.

- 데이터를 워크로드와 연결하려면 어떻게 해야 합니까? *

BlueXP 랜섬웨어 방어는 다음과 같은 방식으로 데이터를 워크로드와 연결합니다.

- BlueXP 랜섬웨어 방어는 볼륨 및 파일 확장명을 검색하고 이를 적절한 워크로드에 연결합니다.
- 또한 VMware용 SnapCenter 또는 SnapCenter가 있고 BlueXP 백업 및 복구 환경에서 워크로드를 구성한 경우, BlueXP 랜섬웨어 방어는 SnapCenter 및 SnapCenter for VMware에서 관리하는 워크로드와 관련 볼륨을

검색합니다.

- "보호된" 워크로드란 무엇입니까? * BlueXP 랜섬웨어 차단에서 1차 감지 정책을 사용하도록 설정한 워크로드는 "보호됨" 상태를 표시합니다. 현재는 ARP가 워크로드와 관련된 모든 볼륨에 활성화되어 있다는 것을 의미합니다.
- "위험" 워크로드란 무엇입니까? * 워크로드에 기본 감지 정책이 활성화되어 있지 않으면 백업 및 스냅샷 정책을 활성화한 경우에도 "위험에 처해 있습니다."
- 새 볼륨이 추가되었지만 아직 나타나지 않음 * 환경에 새 볼륨을 추가한 경우 검색을 다시 시작하고 새 볼륨을 보호하기 위해 보호 정책을 적용합니다.

*대시보드에는 내 작업량이 모두 표시되지 않습니다. 무엇이 잘못되었을 수 있습니까? * 현재 NFS 및 CIFS 볼륨만 지원됩니다. iSCSI 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.

- 랜섬웨어 방지 전략에 필요한 정책은 무엇입니까? *

랜섬웨어 보호 전략에는 다음 정책이 필요합니다.

- 랜섬웨어 감지 정책
- 스냅샷 정책

BlueXP 랜섬웨어 방지 전략에서 백업 정책이 필요하지 않습니다.

- BlueXP 랜섬웨어 방어는 NetApp ONTAP의 보호 설정을 인식합니까? *

예. BlueXP 랜섬웨어 방어는 ONTAP에 설정된 스냅샷 일정과 검색된 워크로드의 모든 볼륨에서 ARP 및 FPolicy가 활성화되는지 여부를 검색합니다. 대시보드의 처음에 표시되는 정보는 다른 NetApp 솔루션 및 제품에서 집계됩니다.

- BlueXP 랜섬웨어 방어는 BlueXP 백업 및 복구와 SnapCenter에 이미 적용된 정책을 인식하고 있습니까? *

예, BlueXP 백업 및 복구 또는 SnapCenter에서 관리되는 워크로드가 있는 경우 해당 제품에서 관리되는 정책이 BlueXP 랜섬웨어 방어에 적용됩니다.

- BlueXP 백업 및 복구 및/또는 SnapCenter에서 이월된 정책을 수정할 수 있습니까? *

아니요, BlueXP 랜섬웨어 보호 내에서 BlueXP 백업 및 복구 또는 SnapCenter로 관리되는 정책을 수정할 수 없습니다. BlueXP 백업 및 복구 또는 SnapCenter에서 이러한 정책에 대한 변경 사항을 관리합니다.

- ONTAP에서 정책이 있는 경우(ARP, FPolicy 및 스냅샷과 같은 시스템 관리자에서 이미 활성화됨) BlueXP 랜섬웨어 보호에서 변경된 정책입니까? *

아니요 BlueXP 랜섬웨어 방어 기능은 ONTAP의 기존 감지 정책(ARP, FPolicy 설정)을 수정하지 않습니다.

- BlueXP 랜섬웨어 방지에 등록한 후 BlueXP 백업 및 복구 또는 SnapCenter에 새로운 정책을 추가하면 어떻게 됩니까? *

BlueXP 랜섬웨어 방어는 BlueXP 백업 및 복구 또는 SnapCenter에서 생성된 모든 새로운 정책을 인식합니다.

- ONTAP에서 정책을 변경할 수 있습니까? *

예, BlueXP 랜섬웨어 방어에서 ONTAP의 정책을 변경할 수 있습니다. BlueXP 랜섬웨어 보호에서 새로운 정책을 생성하여 워크로드에 적용할 수도 있습니다. 이 동작은 기존 ONTAP 정책을 BlueXP 랜섬웨어 보호에서 생성된 정책으로 대체합니다.

- 정책을 비활성화할 수 있습니까? *

System Manager UI, API 또는 CLI를 사용하여 감지 정책에서 ARP를 사용하지 않도록 설정할 수 있습니다.

FPolicy 및 백업 정책은 포함되지 않은 다른 정책을 적용하여 사용하지 않도록 설정할 수 있습니다.