Cyber Protect Cloud

24.03

파트너 관리자 가이드

수정 버전: 2024-04-10

목차

이 문서의 정보

이 문서는 Cyber Protect Cloud를 사용하여 고객에게 서비스를 제공하려는 파트너 관리자를 위해 작성되었습니다.

이 문서는 관리 포털을 사용하여 Cyber Protect Cloud에서 사용 가능한 서비스를 설정하고 관리하는 방법에 대해 설명합니다.

Cyber Protect 정보

Cyber Protect는 서비스 제공업체, 리셀러, 유통업체에서 파트너 및 고객에게 데이터 보호 서비스를 제공할 수 있도록 해주는 클라우드 플랫폼입니다.

서비스는 파트너 수준에서부터 고객 회사 수준과 최종 사용자 수준까지 제공됩니다.

서비스 관리는 **서비스 콘솔**이라고 부르는 웹 애플리케이션을 통해 가능합니다. 테넌트 및 사용자 계정 관리는 **관리 포털**이라고 부르는 웹 애플리케이션을 통해 가능합니다.

관리 포털을 통해 관리자는 다음을 할 수 있습니다.

- 서비스 사용 및 서비스 콘솔에 대한 액세스 모니터링
- 테넌트 관리
- 사용자 계정 관리
- 테넌트에 대한 서비스 및 할당량 구성
- 스토리지 관리
- 브랜딩 관리
- 서비스 사용에 대한 보고서 생성

Cyber Protect 서비스

이 섹션에서는 새로운 요금 청구 모델과 함께 2021년 3월에 도입된 기능 세트에 대해 설명합니다. 새 요금 청구 모델의 이점에 대한 자세한 내용은 Cyber Protect 데이터시트에서 확인할 수 있습니다.

Cyber Protect Cloud에서 사용할 수 있는 서비스와 기능은 다음과 같습니다.

- **Cyber Protect**
  - **보호** - 기본 제품에 포함되어 있는 모든 사이버 보호와 보안 및 관리 기능이 제공됩니다. 또한 재해 복구, 백업 및 복구, 자동화, 이메일 보안은 종량과금제 기능으로 제공됩니다. Advanced Protection 팩(추가 요금이 부과됨)을 구매하면 이 기능을 확장할 수 있습니다.
    Advanced Protection 팩은 Advanced Backup, Advanced Security + EDR 등과 같은 특정 기능 영역에서 더 정교한 시나리오를 처리하는 고유한 기능의 세트입니다. Advanced 팩은 표준 Cyber Protect 서비스에서 사용할 수 있는 기능을 확장합니다.
    Advanced Protection 팩에 대한 자세한 내용은 "Advanced Protection 팩"(119페이지) 항목을 참조하십시오.
  - **File Sync & Share** - 모든 장치에서 언제 어디서나 회사 컨텐츠를 안전하게 공유하는 데 사용할 수 있는 솔루션입니다.
  - **실제 데이터 전달** - 데이터를 하드 드라이브에 저장하여 클라우드 데이터 센터로 발송하는 방식을 통해 시간과 네트워크 트래픽을 절약할 수 있는 솔루션입니다.
  - **공증** - 공유 컨텐츠의 신뢰성을 보장하는 블록체인 기반 솔루션입니다.
- **Cyber Infrastructure SPLA**

관리 포털에서 테넌트에게 제공할 서비스 및 기능 세트를 선택할 수 있습니다. 테넌트 생성에서 설명하는 것처럼 테넌트를 프로비저닝하거나 편집할 때 테넌트별로 구성을 수행합니다.

Cyber Protect의 청구 모드

요금 청구 모드는 서비스 및 해당 기능 사용 시에 적용되는 회계 및 요금 청구 체계입니다. 요금 청구 모드에 따라 가격 계산 기준으로 사용할 단위가 결정됩니다. 파트너가 고객 수준에서 요금 청구 모드를 설정할 수 있습니다.

라이센싱 엔진은 보호 계획에서 요청하는 기능에 따라 제공 항목을 자동으로 가져옵니다. 사용자는 보호 계획을 사용자 정의하여 비용 및 보호 수준을 최적화할 수 있습니다.

참고
요금 청구 모드는 고객 테넌트당 하나만 사용할 수 있습니다.

보호 컴퍼넌트의 요금 청구 모드

보호에서는 두 가지 요금 청구 모드를 사용할 수 있습니다.

- 워크로드당
- 기가바이트당

두 요금 청구 모드의 기능 세트는 동일합니다.

두 요금 청구 모드에서 보호 서비스에는 대다수 사이버 보안 위협에 적용되는 표준 보호 기능이 포함됩니다. 사용자는 이러한 기능을 추가 비용 없이 사용할 수 있습니다. 포함된 기능 사용 시 사용량은 계산되지만 요금은 청구되지 않습니다. 포함된 제공 항목 및 요금 청구 대상 제공 항목의 전체 목록은 "Cyber Protect 서비스"(7페이지)의 내용을 참조하십시오.

고객을 대상으로 Advanced 팩을 활성화하더라도 고객이 보호 계획에서 해당 팩의 기능 사용을 시작한 후부터 요금 청구가 시작됩니다. 보호 계획에서 고급 기능을 적용하면 라이선스 엔진이 필요한 라이선스를 보호된 워크로드에 자동 할당합니다.

고급 기능을 더 이상 사용하지 않는 경우에는 라이선스가 철회되며 요금 청구가 중지됩니다. 라이센싱 엔진은 기능 실제 사용량이 반영된 라이센스를 자동 할당합니다.

표준 Cyber Protect 서비스 기능에만 라이센스를 할당할 수 있습니다. 고급 기능의 요금은 사용량을 기준으로 청구되며, 이러한 기능의 라이센스는 수동으로 수정할 수 없습니다. 이러한 라이센스는 라이센싱 엔진이 자동으로 할당하고 할당을 해제합니다. 워크로드의 라이센스 유형을 수동으로 변경할 수는 있지만, 사용자가 해당 워크로드용 보호 계획을 수정하면 라이센스 유형이 재할당됩니다.

참고
고급 보호 기능 요금 청구는 해당 기능을 활성화할 때 시작되지 않습니다. 즉, 고객이 보호 계획에서 고급 기능 사용을 시작해야 요금 청구가 시작됩니다. 활성화된 기능 세트의 사용량이 계산되며 계산 결과가 사용 보고서에 포함되기는 하지만, 기능을 사용하지 않으면 요금은 청구되지 않습니다.

File Sync & Share의 요금 청구 모드

File Sync & Share에서는 다음과 같은 요금 청구 모드가 사용됩니다.

- 사용자당
- 기가바이트당

레거시 File Sync & Share 버전의 요금 청구 규칙을 적용할 수도 있습니다.

참고
Advanced File Sync & Share 요금 청구는 해당 기능을 활성화할 때 시작되지 않습니다. 즉, 고객이 고급 기능 사용을 시작해야 요금 청구가 시작됩니다. 활성화된 고급 기능 세트의 사용량이 계산되며 계산 결과가 사용 보고서에 포함되기는 하지만, 기능을 사용하지 않으면 요금은 청구되지 않습니다.

실제 데이터 전달의 요금 청구

실제 데이터 전달의 요금은 종량과금제 모델로 청구됩니다.

공증 요금 청구

공증 요금은 종량과금제 모델로 청구됩니다.

레거시 버전에서 요금 청구 모드 사용

최신 요금 청구 모델로 아직 마이그레이션하지 않은 경우 레거시 버전 대신 요금 청구 모드 중 하나에 따라 제공 항목을 사용하십시오. 라이센싱 엔진은 청구 금액을 최소화하기 위해 고객에게 할당되는 라이센스를 자동으로 자동화합니다.

참고
버전과 요금 청구 모드를 함께 사용할 수는 없습니다.

레거시 버전에서 최신 라이선스 모델로 전환

테넌트의 프로필을 편집하여 테넌트용으로 제공 항목을 선택하면 테넌트의 제공 항목을 수동으로 전환할 수 있습니다. 전환 프로세스에 대한 자세한 내용은 "버전과 요금 청구 모드 간 전환"(9페이지)의 내용을 참조하십시오.

여러 고객을 대상으로 버전을 청구 모드로 전환하려는 경우 여러 고객의 버전 대량 전환(67942)을 참조하십시오.

버전과 요금 청구 모드 간 전환

관리 포털에서 테넌트 계정을 수정하여 제공 항목의 청구 모드(워크로드당/기가바이트당)를 전환할 수 있으며 레거시 버전과 청구 모드 간을 전환할 수도 있습니다.

테넌트 대량 전환 관련 정보는 여러 고객의 버전 대량 전환(67942)을 참조하십시오.

전환 프로세스에서는 다음 단계를 수행합니다.

1. 원래 제공 항목에서 제공되었던 기능과 일치하도록 고객 테넌트에 새 제공 항목을 프로비저닝(제공 항목 활성화 및 할당량 설정)합니다.

2. 사용하지 않은 제공 항목을 할당 해제하고, 보호 계획에서 사용되는 기능에 따라 워크로드에 제공 항목을 할당(사용량 조정)합니다.

아래 표에 양방향 전환 프로세스에 대한 설명이 나와 있습니다.

	전환 방향	
	버전 > 요금 청구 모드	**요금 청구 모드 > 요금 청구 모드**
제공 항목 전환	소스 버전에서 제공되었던 기능이 그대로 제공되도록 제공 항목을 활성화합니다.	동일한 제공 항목 세트가 활성화됩니다.
할당량 전환	소스 제공 항목에서 대상 제공 항목으로 할당량이 복제됩니다. 소스 표준 → 대상 표준 제품. 소스 표준 → 대상 팩. **참고** 버전에서 하위 버전(예: "Cyber Protect(워크로드당)")으로 전환하는 경우에는 할당량 요약 정보가 제공됩니다.	소스 제공 항목에서 대상 제공 항목으로 할당량이 복제됩니다.
사용량 전환	워크로드에 할당된 보호 계획에서 요청하는 기능에 따라 제공 항목이 워크로드에 재할당됩니다.	

예: Cyber Protect Advanced Edition에서 워크로드당 요금 청구로 전환

고객 테넌트가 워크스테이션 8대에서 Cyber Protect Advanced Edition을 사용 중이며 할당량이 워크로드 10개로 설정되어 있는 시나리오입니다. 워크스테이션 중 3대에서는 보호 계획의 소프트웨어 인벤토리 및 패치 관리를 사용합니다. 워크스테이션 2대의 보호 계획에서는 URL 필터링이 활성화되어 있습니다. 그리고 머신 1대에서는 지속적인 데이터 보호를 사용합니다. 이 시나리오에서 버전을 새 제공 항목으로 변환하는 방식이 아래 표에 나와 있습니다.

소스 제공 항목 - 사용량/할당량	대상 제공 항목 - 사용량/할당량
Cyber Protect Advanced Workstation 8/10	• 워크스테이션 - 8/10 • Advanced Security + EDR - 2/10 • Advanced Backup 워크스테이션 - 1/10 • Advanced Management - 3/10

전환 과정에서 실행한 단계는 다음과 같습니다.

1. 소스 버전에서 제공되었던 기능이 포함된 제공 항목이 자동으로 활성화되었습니다.
2. 새 제공 항목에서 할당량이 복제되었습니다.
3. 보호 계획의 실제 사용량에 따라 사용량이 조정되었습니다. 워크로드 3개는 Advanced Management 팩의 기능을 사용하고, 2개는 Advanced Security + EDR 팩의 기능을 사용하며, 1개는 Advanced Backup 팩의 기능을 사용합니다.

예: Cyber Protect 워크로드당 버전에서 워크로드당 요금 청구로 전환

고객의 워크로드에 여러 버전이 할당되어 있는 예제입니다. 각 워크로드에는 버전이나 청구 모드를 하나만 할당할 수 있습니다.

소스 제공 항목 - 사용량/할당량	대상 제공 항목 - 사용량/할당량
Cyber Protect Essentials Workstation - 6/12	• 워크스테이션 - 14/42 • Advanced Backup 워크스테이션 - 2/42 • Advanced Security + EDR - 13/42 • Advanced Management - 5/42
Cyber Protect Standard 워크스테이션 - 5/10	
Cyber Protect Advanced 워크스테이션 - 2/10	
Cyber Backup Standard 워크스테이션 - 1/10	

전환 과정에서 실행한 단계는 다음과 같습니다.

1. 모든 소스 버전에서 제공되었던 기능이 포함된 제공 항목이 자동으로 활성화되었습니다. 청구 모드에서는 필요에 따라 워크로드 하나에 여러 제공 항목을 할당할 수 있습니다.
2. 할당량이 요약되어 복제되었습니다.
3. 보호 계획에 따라 사용량이 조정되었습니다.

파트너 테넌트의 청구 모드 변경

파트너 테넌트의 청구 모드를 변경하려면

1. 관리 포털에서 **클라이언트**로 이동합니다.
2. 청구 모드를 변경하려는 파트너 테넌트를 선택하고 말줄임표 아이콘 을 클릭한 후 **구성**을 클릭합니다.
3. **Cyber Protect** 탭에서 청구 모드를 변경할 서비스를 선택하고 **편집**을 클릭합니다.
4. 원하는 청구 모드를 선택하고 필요에 따라 사용 가능한 제공 항목을 활성화하거나 비활성화합니다.
5. **저장**을 클릭합니다.

고객 테넌트의 청구 모드 변경

다음을 수행하여 고객 테넌트의 청구 방법을 변경할 수 있습니다.

- 제공 항목을 활성화 또는 비활성화하여 원래 청구 모드 편집
- 완전히 새로운 청구 모드로 전환

사용 가능한 제공 항목 편집 방법에 대한 자세한 내용은 제공 항목 활성화 또는 비활성화를 참조하십시오.

고객 테넌트의 청구 모드를 전환하려면

1. 관리 포털에서 **클라이언트**로 이동합니다.
2. 버전을 변경하려는 고객 테넌트를 선택하고 말줄임표 아이콘 을 클릭한 후 **구성**을 클릭합니다.
3. **구성** 탭의 **서비스**에서 새 청구 모드를 선택합니다.
   새 청구 모드로 변경하는 경우의 결과를 알려 주는 팝업 대화 상자가 표시됩니다.
4. 사용자 이름을 입력하여 선택 내용을 확인합니다.

참고
이 변경을 완료하는 데 최대 10분 정도 걸릴 수 있습니다.

제공 항목 및 할당량 관리

이 섹션에서는 다음에 대해 설명합니다.

- 서비스 및 제공 항목 소개?
- 제공 항목은 어떻게 활성화 또는 비활성화합니까?
- 요금 청구 모드 소개?
- Advanced Protection 팩 소개?
- 레거시 버전 및 하위 버전 소개?
- 소프트 및 하드 할당량은 무엇입니까?
- 하드 할당량은 언제 초과할 수 있습니까?
- 백업 할당량 전환은 무엇입니까?
- 제공 항목 가용성이 Cyber Protect 콘솔의 워크로드 유형 가용성에 주는 영향은 무엇입니까?

서비스 및 제공 항목

서비스

클라우드 서비스는 파트너 또는 최종 고객의 사설 클라우드에서 호스팅되는 기능 세트입니다. 서비스는 보통 가입 또는 종량과금제 형식으로 판매됩니다.

Cyber Protect 서비스에서는 엔드포인트, 시스템, 데이터를 사이버 위협으로부터 보호하는 사이버 보안, 데이터 보호 및 관리 기능을 통합 제공합니다. Cyber Protect 서비스에는 보호, File Sync & Share, 공증, 실제 데이터 전달 등의 여러 컴퍼넌트가 포함되어 있습니다.Advanced Protection 팩을 사용하면 고급 기능을 통해 이러한 컴퍼넌트 중 일부를 확장할 수 있습니다. 포함된 기능과 고급 기능에 대한 상세 정보는 "Cyber Protect 서비스"(7페이지)의 내용을 참조하십시오.

제공 항목

제공 항목은 스토리지, 재해 복구 인프라 등의 특정 워크로드 유형이나 기능별로 그룹화된 서비스 기능 세트입니다. 특정 제공 항목을 활성화하면 보호 가능한 워크로드, 할당량을 설정하여 보호할 수 있는 워크로드의 수, 그리고 Advanced Protection 팩을 활성화하거나 비활성화하여 파트너, 고객, 최종 사용자에게 제공할 보호 수준이 결정됩니다.

활성화되지 않은 기능은 업셀 시나리오를 구성하지 않으면 숨겨지므로 고객과 사용자가 확인할 수 없습니다. 업셀 시나리오 관련 추가 정보는 "고객에 대한 업셀 시나리오 구성"(64페이지)의 내용을 참조하십시오.

기능 사용량은 서비스에서 수집되어 제공 항목에 반영됩니다. 이 정보가 보고서와 추가 요금 청구에 사용됩니다.

요금 청구 모드 및 버전

레거시 버전의 경우 워크로드당 제공 항목 하나를 활성화할 수 있습니다. 반면 요금 청구 모드 사용 시에는 기능이 분할되므로 워크로드당 여러 제공 항목(서비스 기능 및 Advanced 팩)을 활성화하여 고객의 요구를 더욱 효율적으로 충족할 수 있습니다. 또한 고객이 실제로 사용하는 기능만을 대상으로 하여 더욱 정확한 요금 청구를 적용할 수 있습니다.

Cyber Protect용 요금 청구 모드 관련 추가 정보는 "Cyber Protect의 청구 모드"(8페이지)의 내용을 참조하십시오.

요금 청구 모드 또는 버전을 사용하여 테넌트에게 제공할 서비스를 구성할 수 있습니다. 고객 테넌트당 요금 청구 모드나 버전 하나를 선택할 수 있습니다. 따라서 서비스 기능별로 다른 요금 청구 모드를 적용하려면 고객 한 명에 해당하는 테넌트를 여러 개 생성해야 합니다. 예를 들어 고객이 Microsoft 365 사서함은 기가바이트당 요금 청구 모드로, Teams는 워크로드당 요금 청구 모드로 사용하려는 경우에는 해당 고객용으로 고객 테넌트 2개를 생성해야 합니다.

제공 항목에서 서비스 사용을 제한하려는 경우 해당 제공 항목의 할당량을 정의하면 됩니다. "소프트 및 하드 할당량"(15페이지)을(를) 참조하십시오.

제공 항목 활성화 또는 비활성화

테넌트 생성에 설명된 대로 지정된 버전이나 요금 청구 모드에 대해 사용할 수 있는 모든 제공 항목을 활성화할 수 있습니다.

참고
서비스의 제공 항목을 모두 비활성화해도 서비스가 자동으로 비활성화되지는 않습니다.

아래 표에 나열된 제공 항목을 비활성화하는 데는 몇 가지 제한이 적용됩니다.

제공 항목	비활성화	결과
백업 스토리지	사용량이 0일 때 비활성화할 수 있습니다.	고객 테넌트 내의 백업 대상으로 클라우드 스토리지를 사용할 수 없게 됩니다.

로컬 백업	사용량이 0일 때 비활성화할 수 있습니다.	고객 테넌트 내의 백업 대상으로 로컬 스토리지를 사용할 수 없게 됩니다.
데이터 소스(Microsoft 365 및 Google Workspace 포함)*	사용량이 0일 때 비활성화할 수 있습니다.	다음과 같이 고객 테넌트 내에서 비활성화된 데이터 소스(Microsoft 365 및 Google Workspace 포함)의 보호 기능을 사용할 수 없게 됩니다.
모든 재해 복구 제공 항목	사용량이 0보다 많을 때 비활성화할 수 있습니다.	자세한 내용은 "소프트 및 하드 할당량"을 참조하십시오.
모든 공증 제공 항목	사용량이 0일 때 비활성화할 수 있습니다.	고객 테넌트 내에서 공증 서비스를 사용할 수 없게 됩니다.
모든 File Sync & Share 제공 항목	제공 항목은 개별적으로 활성화하거나 비활성화할 수 없습니다.	고객 테넌트 내에서 File Sync & Share 서비스를 사용할 수 없게 됩니다.
모든 실제 데이터 전달 제공 항목	사용량이 0일 때 비활성화할 수 있습니다.	고객 테넌트 내에서 실제 데이터 전달 서비스를 사용할 수 없게 됩니다.

사용량이 0보다 많을 때 비활성화할 수 없는 제공 항목은 수동으로 사용량을 제거한 다음 해당 제공 항목을 비활성화 할 수 있습니다.

* 제공 항목은 Cyber Protect 콘솔에서 추가할 수 있는 워크로드 관련 항목입니다. 자세한 내용은 "제공 항목에 대한 워크로드 종속성"(23페이지) 항목을 참조하십시오. 아래 표에는 관리 포털에서 제공 항목, 제공 항목 조합 또는 어드밴스드 팩이 활성화되어 있지 않으면 사용할 수 없는 워크로드 유형이 요약되어 있습니다.

비활성화하는 제공 항목 또는 어드밴스드 팩	추가할 수 없는 워크로드 유형
다음 조합: • Microsoft 365 시트 • Microsoft 365 SharePoint online • Microsoft 365 Teams	Microsoft 365 Business
다음 조합: • Google Workspace • Google Workspace Shared Drive	Google Workspace
다음 조합: • 서버 • 가상 머신	• Microsoft SQL Server • Microsoft Exchange Server • Microsoft Active Directory
다음 제공 항목: • NAS	Synology

비활성화하는 제공 항목 또는 어드밴스드 팩	추가할 수 없는 워크로드 유형
다음 제공 항목: • 모바일	• iOS 장치 • Android 장치
다음 어드밴스드 팩: • Advanced Backup	Oracle 데이터베이스

소프트 및 하드 할당량

할당량으로 테넌트의 서비스 사용을 제한할 수 있습니다. 할당량을 설정하려면 **클라이언트** 탭에서 서비스 탭을 선택한 다음 **편집**을 클릭합니다.

할당량을 초과하면 사용자의 이메일 주소로 알림이 전송됩니다. 할당량 초과분을 설정하지 않을 경우 "**소프트**" 할당량으로 간주됩니다. 즉, Cyber Protection 서비스 사용에 대한 제한 사항이 적용되지 않습니다.

할당량 초과분을 지정할 경우 "**하드**" 할당량으로 간주됩니다. **초과분**은 사용자가 지정된 값까지 할당량을 초과하도록 허용합니다. 초과분까지 초과되면 서비스 사용에 대한 제한이 적용됩니다.

예

소프트 할당량: 워크스테이션의 할당량을 20으로 설정했습니다. 고객의 보호된 워크스테이션의 수가 20이 되면 고객은 이메일로 알림을 받게 되지만 Cyber Protection 서비스는 그대로 사용 가능합니다.

하드 할당량: 워크스테이션의 할당량을 20으로 설정하고 초과분이 5인 경우, 고객은 보호된 워크스테이션의 수가 20에 도달하면 이메일로 알림을 받게 되고, 그 수가 25에 도달할 경우 Cyber Protection 서비스가 비활성화됩니다.

하드 할당량에 도달하면 서비스 사용이 제한됩니다. 다른 워크로드를 보호하거나 스토리지를 추가로 사용할 수 없습니다. 하드 할당량을 초과하면 사용자의 이메일 주소로 알림이 전송됩니다.

할당량 정의가 가능한 수준

할당량을 설정할 수 있는 수준은 아래 표에 나열된 목록과 같습니다.

테넌트/사용자	소프트 할당량(할당량만)	하드 할당량(할당량 및 초과분)
파트너	예	아니오
폴더	예	아니오
고객	예	예
단위	아니오	아니오
사용자	예	예

소프트 할당량은 파트너 및 폴더 수준에서 설정할 수 있습니다. 부서 수준에서는 할당량을 설정할 수 없습니다. 하드 할당량은 고객 및 사용자 수준에서 설정할 수 있습니다.

사용자 수준에서 설정된 총 하드 할당량은 관련 고객 하드 할당량을 초과할 수 없습니다.

소프트 및 하드 할당량 설정

클라이언트 할당량 설정 방법

1. 관리 포털에서 **클라이언트**로 이동합니다.
2. 할당량을 설정할 클라이언트를 선택합니다.
3. **보호 탭**을 선택한 다음 **편집**을 클릭합니다.
4. 설정하고 싶은 할당량 유형을 선택합니다. 예를 들어 **워크스테이션** 또는 **서버**를 선택합니다.
5. 우측의 **무제한** 링크를 클릭하여 **할당량 편집** 창을 엽니다.
   - 클라이언트에게 할당량을 알리고 싶지만 클라이언트의 서비스 사용을 제한하고 싶지 않다면 **소프트 할당량** 필드에서 할당량 값을 설정합니다.
     클라이언트가 할당량에 도달하면 이메일으로 알림을 받지만 Cyber Protection 서비스는 계속 사용할 수 있습니다.
   - 클라이언트의 서비스 사용을 제한하고 싶다면 **하드 할당량**을 선택하고 **하드 할당량** 아래에 있는 필드에 할당량 값을 입력합니다.
     클라이언트가 할당량에 도달하면 이메일로 알림을 받고 Cyber Protection 서비스가 비활성화됩니다.
6. **할당량 편집** 창에서 **완료**를 클릭한 다음 **저장**을 클릭합니다.

백업 할당량

사용자가 보호하도록 허용된 클라우드 스토리지 할당량, 로컬 백업용 할당량 및 최대 머신/장치/웹사이트 수를 지정할 수 있습니다. 다음 할당량을 사용할 수 있습니다.

장치 할당량

- **워크스테이션**
- **서버**
- **가상 머신**
- **모바일 장치**
- **웹 호스팅 서버** (Plesk, cPanel, DirectAdmin, VirtualMin, 또는 ISPManager 제어판을 구동 중인 Linux 기반 실제 또는 가상 서버)
- **웹사이트**

하나 이상의 보호 계획이 적용된 경우 해당 머신/장치/웹사이트는 보호된 것으로 간주합니다. 모바일 장치는 첫 번째 백업 후에 보호됩니다.

장치 수 초과분을 넘어선 경우 사용자는 더 이상 추가 장치에 대한 보호 계획을 적용할 수 없습니다.

클라우드 데이터 소스 할당량

- **Microsoft 365 시트**

  이 할당량은 서비스 제공업체를 통해 전사적으로 적용됩니다. 회사 관리자는 관리 포털에서 할당량 및 사용량을 볼 수 있습니다.

  Microsoft 365 시트의 라이센스는 Cyber Protection에 대해 선택한 청구 모드에 따라 다릅니다.

  중요

  로컬 에이전트와 클라우드 에이전트는 각기 별도의 할당량을 사용합니다. 두 에이전트를 모두 사용하여 동일 워크로드를 백업하면 요금이 두 번 부과됩니다. 예:

  - 가령 로컬 에이전트로 사용자 120명의 사서함을 백업하고 클라우드 에이전트로 동일한 사용자 120명의 OneDrive 파일을 백업한다면 Microsoft 365 시트 240개에 해당하는 요금이 부과됩니다.
  - 그리고 로컬 에이전트로 사용자 120명의 사서함을 백업하고 클라우드 에이전트로도 동일한 사서함을 백업한다면 Microsoft 365 시트 240개에 해당하는 요금이 부과됩니다.

  워크로드당 청구 모드에서는 고유 사용자 단위로 **Microsoft 365 시트** 할당량이 계산됩니다. 고유 사용자는 다음 항목 중 하나 이상을 소유한 사용자입니다.

  - 보호되는 사서함
  - 보호되는 OneDrive
  - 보호되는 회사 수준 리소스인 Microsoft 365 SharePoint Online 사이트 또는 Microsoft 365 Teams 중 하나 이상에 대한 액세스 권한

    Microsoft 365 SharePoint 혹은 Teams 사이트의 구성원 수를 확인하는 방법은 본 지식 베이스 문서를 참조하십시오.

  참고

  보호된 개인 사서함 또는 OneDrive가 없고 공유 리소스(공유 사서함, SharePoint 사이트, Microsoft Teams)만 액세스할 수 있는 차단된 Microsoft 365 사용자는 요금이 부과되지 않습니다.

  차단된 사용자는 유효한 로그인 권한이 없고 Microsoft 365 서비스에 액세스할 수 없는 사용자를 의미합니다. Microsoft 365 조직에서 라이선스가 없는 사용자를 모두 차단하는 방법은 "라이선스가 없는 Microsoft 365 사용자의 로그인 방지"(19페이지)에서 확인할 수 있습니다.

  다음 Microsoft 365 시트에는 요금이 부과되지 않으며 시트당 라이센스가 필요하지 않습니다.

  - 공유 사서함
  - 공간 및 장비
  - 백업된 SharePoint 사이트 및/또는 Microsoft Teams에 액세스할 수 있는 외부 사용자

  기가바이트당 청구 모드로 사용 가능한 라이센스 옵션에 대한 자세한 내용은 Cyber Protect 클라우드: Microsoft 365 GB당 라이센스를 참조하십시오.

  워크로드당 청구 모드로 사용 가능한 라이센스 옵션에 대한 자세한 내용은 Cyber Protect 클라우드: Microsoft 365 라이센스 및 가격 책정 변경 사항을 참조하십시오.

- **Microsoft 365 Teams**

이 할당량은 서비스 제공업체를 통해 전사적으로 적용됩니다. 이 할당량은 Microsoft 365 Teams에 대한 보호 기능을 활성화 또는 비활성화하고 보호할 수 있는 팀의 최대 개수를 설정합니다. 한 팀을 보호하려면 멤버 또는 채널 수와 관계없이 할당량 한 개가 필수입니다. 회사 관리자는 관리 포털에서 할당량 및 사용량을 볼 수 있습니다.

- **Microsoft 365 SharePoint Online**

  이 할당량은 서비스 제공업체를 통해 전사적으로 적용됩니다. 이 할당량은 SharePoint 온라인 사이트에 대한 보호 기능을 활성화 또는 비활성화하고 보호할 수 있는 사이트 컬렉션 및 그룹 사이트의 최대 개수를 설정합니다.

  회사 관리자는 관리 포털에서 할당량을 볼 수 있습니다. 할당량과 함께, 사용 리포트에서 SharePoint 온라인 백업이 차지하는 스토리지 용량도 볼 수 있습니다.

- **Google Workspace 시트**

  이 할당량은 서비스 제공업체를 통해 전사적으로 적용됩니다. 회사는 **Gmail** 사서함(캘린더 및 연락처 포함)이나 **Google Drive** 파일, 또는 둘 모두를 보호하도록 허용할 수 있습니다. 회사 관리자는 관리 포털에서 할당량 및 사용량을 볼 수 있습니다.

- **Google Workspace Shared Drive**

  이 할당량은 서비스 제공업체를 통해 전사적으로 적용됩니다. 이 할당량은 Google Workspace Shared Drive에 대한 보호 기능을 활성화 또는 비활성화합니다. 할당량이 활성화되면 수에 제한 없이 Shared Drive를 보호할 수 있습니다. 회사 관리자는 관리 포털에서 할당량을 볼 수 없지만, 사용 리포트에서 Shared Drive 백업이 차지하는 스토리지 용량은 볼 수 있습니다.

  Google Workspace Shared Drive 백업은 추가로 최소 1개의 Google Workspace 시트 할당량을 보유한 고객만 사용할 수 있습니다. 이러한 할당량은 검증만을 위한 것이며 실제로 사용되지 않습니다.

하나 이상의 보호 계획이 사용자의 사서함 또는 OneDrive에 적용된 경우 해당 Microsoft 365 시트는 보호된 것으로 간주합니다. 하나 이상의 보호 계획이 사용자의 사서함 또는 Google Drive에 적용된 경우 해당 Google Workspace 시트는 보호된 것으로 간주합니다.

시트 수 초과분을 넘어선 경우 회사 관리자는 더 이상 추가 시트에 대한 보호 계획을 적용할 수 없습니다.

스토리지 할당량

- **로컬 백업**

  로컬 백업 할당량은 클라우드 인프라를 사용하여 생성된 로컬 백업의 총 크기를 제한합니다. 이 할당량에 대한 초과분을 설정할 수 없습니다.

- **클라우드 리소스**

  클라우드 리소스 할당량은 백업 스토리지의 할당량과 재해 복구 할당량을 병합합니다. 백업 스토리지 할당량은 클라우드 스토리지에 위치한 백업의 총 크기를 제한합니다. 백업 스토리지 할당량 초과분을 초과하면 백업에 실패합니다.

백업 스토리지 할당량 초과

백업 스토리지 할당량을 초과할 수 없습니다. 보호 에이전트 인증서는 테넌트의 백업 할당량에 초과분을 합한 것과 동일한 기술적 할당량이 있습니다. 할당량을 초과한 경우 백업을 시작할 수 없습

니다. 백업 생성 중 인증서의 할당량에 도달하였으나 초과분에는 도달하지 않는 경우 백업은 성공적으로 완료됩니다. 백업 생성 중 초과분에 도달한 경우 백업은 실패합니다.

예:

사용자 테넌트는 할당량으로 1TB의 여유 공간이 있으며, 초과분은 본 사용자에 대해서 5TB입니다. 사용자가 백업을 시작합니다. 생성된 백업의 크기가 예를 들어 3TB인 경우 초과분에 도달하지 않았으므로 백업은 성공적으로 완료됩니다. 생성된 백업의 크기가 6TB인 경우 초과분에 도달하였으므로 백업은 실패합니다.

백업 할당량 전환

일반적으로 백업 할당량 가져오기와 리소스 유형으로의 제공 항목 매핑은 다음과 같이 진행됩니다. 시스템에서 사용 가능한 제공 항목을 리소스 유형과 비교한 다음, 일치하는 제공 항목에 대한 할당량을 가져옵니다.

또한, 리소스 유형과 정확히 일치하지 않아도 다른 제공 항목 할당량을 지정할 수 있는 기능도 있습니다. 이를 **백업 할당량 전환**이라고 합니다. 일치하는 제공 항목이 없으면 시스템에서 리소스 유형에 대해 더 비용이 높은 적절한 할당량 지정을 시도합니다(자동 백업 할당량 전환). 적절한 항목을 찾지 못할 경우, Cyber Protect 콘솔에서 리소스 유형에 서비스 할당량을 수동으로 지정할 수 있습니다.

예

가상 머신(워크스테이션, 에이전트 기반 등)을 백업하려고 합니다.

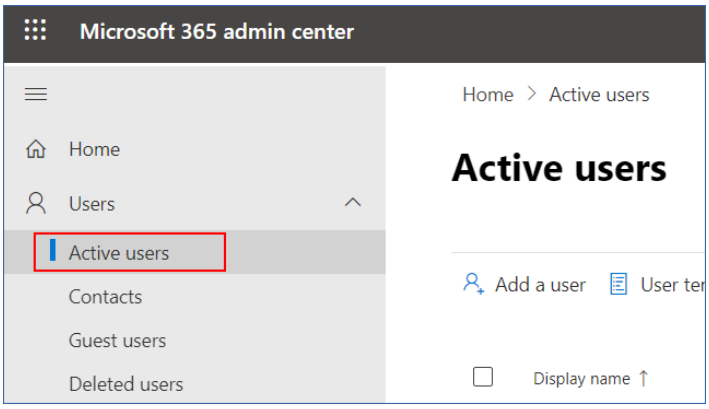
우선 시스템에서 **가상 머신**에 지정된 할당량이 있는지 확인합니다. 할당량을 찾지 못할 경우, 시스템에서 자동으로 **워크스테이션 할당량** 가져오기를 시도합니다. 그 할당량도 찾지 못하면 다른 할당량을 자동으로 가져오지 않습니다. **가상 머신** 할당량보다 비용이 더 높고 가상 머신에 적용 가능한 할당량이 충분히 있다면 Cyber Protect 콘솔에 로그인하여 **서버** 할당량을 수동으로 지정할 수 있습니다.

라이선스가 없는 Microsoft 365 사용자의 로그인 방지

라이선스가 없는 사용자의 로그인 상태를 편집하면 Microsoft 365 조직 내 모든 해당 사용자의 로그인을 방지할 수 있습니다.

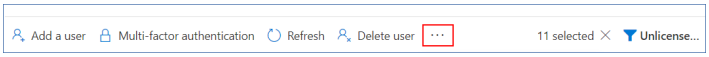
라이선스가 없는 사용자의 로그인 방지

1. 전역 관리자로 Microsoft 365 관리자 센터(https://admin.microsoft.com)에 로그인합니다.
2. 탐색 메뉴에서 **사용자** > **활성 사용자**로 이동합니다.



3. **필터**를 클릭하고 **라이선스가 없는 사용자**를 클릭합니다.

4. 사용자 이름 옆의 확인란을 선택하고 말줄임표 아이콘(...)을 클릭합니다.



5. 메뉴에서 **로그인 상태 편집**을 선택합니다.
6. **사용자의 로그인 차단** 확인란을 선택하고 **저장**을 클릭합니다.

재해 복구 할당량

참고
재해 복구 제공 항목은 재해 복구 애드온에서만 사용 가능합니다.

이 할당량은 서비스 제공업체가 전체 회사에 적용합니다. 회사 관리자는 관리 포털에서 할당량 및 사용량을 볼 수 있지만 사용자에 대한 할당량을 설정할 수는 없습니다.

- **재해 복구 스토리지**
  Disaster Recovery 스토리지에는 Disaster Recovery를 통해 보호되는 서버의 백업 스토리지 크기가 표시됩니다. 재해 복구 스토리지 사용량은 재해 복구 서버를 통해 보호되는 워크로드의 백업 스토리지 사용량과 같습니다. 이 스토리지의 크기는 서버가 현재 실행 중인지 여부에 관계없이 복구 서버가 생성된 시점부터 계산됩니다. 이 할당량 초과분에 도달한 경우 기본 및 복구 서버를 생성하거나 기존 기본 서버에 디스크를 추가/확장할 수 없습니다. 이 할당량 초과분이 초과된 경우 장애 조치를 시작하거나 중지된 서버를 시작할 수 없습니다. 실행 중인 서버는 계속 실행됩니다.
- **컴퓨팅 포인트**
  이 할당량은 청구 기간 동안 기본 및 복구 서버에서 사용되는 CPU 및 RAM 리소스를 제한합니다. 이 할당량 초과분에 도달한 경우 모든 기본 서버 및 복구 서버가 중단됩니다. 다음 청구 기간이 시작될 때까지 이러한 서버를 사용할 수 없습니다. 기본 청구 기간은 1개월입니다.
  할당량을 비활성화하면 청구 기간에 관계없이 서버를 사용할 수 없습니다.
- **공용 IP 주소**
  이 할당량은 기본 및 복구 서버에 할당할 수 있는 공용 IP 주소 수를 제한합니다. 이 할당량 초과분에 도달한 경우 더 많은 서버에 대해 공용 IP 주소를 활성화할 수 없습니다. 서버 설정에서 **공용 IP 주소** 확인란의 선택을 취소하여 서버가 공용 IP 주소를 사용하지 못하게 할 수 있습니다.

그런 다음 다른 서버가 공용 IP 주소를 사용할 수 있도록 허용할 수 있습니다. 공용 IP 주소는 일반적으로 같은 주소가 아닙니다.

할당량을 비활성화하면 모든 서버가 공용 IP 주소 사용을 중지하므로 인터넷에서 연결할 수 없게 됩니다.

- **클라우드 서버**

  이 할당량은 기본 및 복구 서버의 총 수를 제한합니다. 이 할당량 초과분에 도달한 경우 기본 및 복구 서버를 생성할 수 없습니다.

  할당량을 사용하지 않으면 Cyber Protect 콘솔에 서버가 표시되기는 하지만 사용 가능한 작업은 **삭제**뿐입니다.

- **인터넷 액세스**

  이 할당량은 기본 및 복구 서버에서 인터넷 액세스를 활성화하거나 비활성화합니다.

  할당량을 비활성화하면 기본 및 복구 서버가 인터넷에 연결할 수 없게 됩니다.

File Sync & Share 할당량

테넌트의 File Sync & Share 할당량을 다음과 같이 정의할 수 있습니다.

- **사용자**

  File Sync & Share 사용자 수의 제한을 정의합니다.

  참고
  사용자 및 사용자 + 관리자 사용자 역할만 이 할당량 계산에 포함됩니다.
  관리자 및 게스트 사용자 역할은 이 할당량 계산에서 제외됩니다.

- **클라우드 스토리지**

  테넌트에게 할당되는 클라우드 스토리지의 제한을 정의합니다.

실제 데이터 전달 할당량

실제 데이터 전달 서비스 할당량은 드라이브별로 사용됩니다. 하나의 하드 드라이브에 여러 머신의 최초 백업을 저장할 수 있습니다.

테넌트의 실제 데이터 전달 할당량을 다음과 같이 정의할 수 있습니다.

- **클라우드로**

  하드 디스크 드라이브를 사용하여 클라우드 데이터 센터로 최초 백업을 전송할 수 있습니다. 이 할당량은 클라우드 데이터 센터로 전송할 수 있는 최대 드라이브 수를 정의합니다.

공증 할당량

테넌트의 공증 할당량을 다음과 같이 정의할 수 있습니다.

- **공증 스토리지**

  공증된 파일, 서명된 파일 및 공증이나 서명이 진행 중인 파일용 최대 클라우드 스토리지 공간을 정의합니다.

  이 할당량의 사용량을 축소하려는 경우 공증 스토리지에서 이미 공증되었거나 서명된 파일을 삭제하면 됩니다.

- **공증**
  공증 서비스를 사용하여 공증할 수 있는 최대 파일 수를 정의합니다.
  파일은 공증 스토리지에 업로드되고 공증 상태가 **진행 중**으로 변경되는 즉시 공증된 것으로 간주됩니다.
  동일한 파일이 여러 번 공증되는 경우 각 공증마다 새로운 공증으로 계산됩니다.
- **전자 서명**
  디지털 전자 서명의 최대 수를 정의합니다.

머신의 서비스 할당량 변경

머신의 보호 수준은 적용된 서비스 할당량에 따라 정의됩니다. 서비스 할당량은 머신이 등록된 테넌트에 사용할 수 있는 제공 항목과 관련이 있습니다.

서비스 할당량은 보호 계획이 처음으로 머신에 적용될 때 자동으로 할당됩니다.

보호되는 시스템, 시스템의 운영 체제, 필요한 보호 수준 및 사용 가능한 할당량에 따라 가장 적절한 할당량이 할당됩니다. 조직에서 가장 적절한 할당량을 사용할 수 없다면 두 번째로 적합한 할당량이 할당됩니다. 예를 들어 가장 적절한 할당량인 **웹 호스팅 서버**를 사용할 수 없다면 **서버** 할당량이 할당됩니다.

할당량 할당의 예는 다음과 같습니다.

- Windows Server 또는 Linux 서버 운영 체제(예: Ubuntu Server)를 실행하는 실제 머신에는 **서버** 할당량이 할당됩니다.
- Windows 또는 Linux 데스크탑 운영 체제(예: Ubuntu Desktop)를 실행하는 실제 머신에는 **워크스테이션** 할당량이 할당됩니다.
- Hyper-V 역할이 활성화된 Windows 10을 실행하는 실제 머신에는 **워크스테이션** 할당량이 할당됩니다.
- 가상 데스크탑 인프라에서 실행되며 게스트 운영 체제 내에 보호 에이전트(예: Agent for Windows)가 설치되어 있는 데스크탑 머신에는 **가상 머신** 할당량이 할당됩니다. **가상 머신** 할당량을 사용할 수 없는 경우 이 머신 유형은 **워크스테이션** 할당량을 사용할 수도 있습니다.
- 가상 데스크탑 인프라에서 실행되며 에이전트 없는 모드에서 백업(예: Agent for VMware 또는 Agent for Hyper-V를 통해 백업)되는 데스크탑 머신에는 **가상 머신** 할당량이 할당됩니다.
- Hyper-V 또는 vSphere 서버에는 **서버**할당량이 할당됩니다.
- cPanel 또는 Plesk가 설치된 서버에는 **웹 호스팅 서버** 할당량이 할당됩니다. 웹 호스팅 서버 할당량을 사용할 수 없는 경우 이 서버는 웹 서버가 실행되는 머신 유형에 따라 **가상 머신** 또는 **서버** 할당량을 사용할 수도 있습니다.
- 애플리케이션 인식 백업을 수행하려면 워크스테이션에서도 **서버** 할당량이 필요합니다.

나중에 원래 할당을 수동으로 변경할 수 있습니다. 예를 들어, 좀 더 고급 보호 계획을 동일한 머신에 적용하려면 머신의 서비스 할당량을 업그레이드해야 할 수 있습니다. 이 보호 계획에 필요한 기능을 현재 할당된 서비스 할당량이 지원하지 않는 경우 보호 계획은 실패합니다.

원래 할당량이 할당된 후 더 적절한 할당량을 구매할 경우 서비스 할당량을 변경할 수도 있습니다. **워크스테이션** 할당량이 가상 머신에 할당된 경우를 예로 들 수 있습니다. 이 경우에는 **가상 머신** 할당량을 구매한 후 원래 **워크스테이션** 할당량 대신 수동으로 이 머신에 할당할 수 있습니다.

현재 할당되어 있는 서비스 할당량을 해제한 후 다른 머신에 해당 할당량을 할당할 수도 있습니다.

개별 머신 또는 머신 그룹의 서비스 할당량을 변경할 수 있습니다.

개별 머신의 서비스 할당량을 변경하려면

1. Cyber Protect 콘솔에서 **장치**로 이동합니다.
2. 원하는 머신을 선택한 다음, **상세 정보**를 클릭합니다.
3. **서비스 할당량** 섹션에서 **변경**을 클릭합니다.
4. **할당량 변경** 창에서 원하는 서비스 할당량을 선택하거나 **할당량 없음**을 선택한 다음 **변경**을 클릭합니다.

머신 그룹의 서비스 할당량을 변경하려면

1. Cyber Protect 콘솔에서 **장치**로 이동합니다.
2. 2개 이상의 머신을 선택한 다음 **할당량 지정**을 클릭합니다.
3. **할당량 변경** 창에서 원하는 서비스 할당량을 선택하거나 **할당량 없음**을 선택한 다음 **변경**을 클릭합니다.

제공 항목에 대한 워크로드 종속성

활성화된 제공 항목에 따라 콘솔의 **장치 추가** 창에서 각기 다른 워크로드 유형을 사용할 수 있습니다. 아래 표에서 각 제공 항목에 사용 가능한 워크로드 유형을 확인할 수 있습니다.

워크로드 유형 (에이전트 인스톨러)	**활성화된 제공 항목**							
	서버	**워크스테이션**	**가상 머신**	**Microsoft 365 시트**	**Google Workspace 시트**	**모바일 장치**	**웹 호스팅 서버**	**웹사이트**
워크스테이션 – Agent for Windows		+	+					+
워크스테이션 – Agent for macOS		+	+					+
서버 – Agent for Windows	+		+				+	+
서버 – Agent for Linux	+		+				+	+
Agent for Hyper-V			+					
Agent for VMware			+					
Agent for Virtuozzo			+					

워크로드 유형 (에이전트 인스톨러)	활성화된 제공 항목							
	서버	워크스테이션	가상 머신	Microsoft 365 시트	Google Workspace 시트	모바일 장치	웹 호스팅 서버	웹사이트
Agent for SQL	+		+					
Agent for Exchange	+		+					
Agent for Active Directory	+		+					
Microsoft 365 Business 워크로드				+				
Google Workspace 워크로드					+			
Windows용 정식 설치 프로그램	+	+	+				+	+
모바일(iOS 및 Android)						+		

관리 포털 사용

다음 단계에서는 관리 포털의 기본적인 사용에 대해 안내합니다.

지원되는 웹 브라우저

웹 인터페이스는 다음 웹 브라우저를 지원합니다.

- Google Chrome 29 이상 버전
- Mozilla Firefox 23 이상 버전
- Opera 16 이상 버전
- Microsoft Edge 25 이상 버전
- macOS 및 iOS 운영 체제에서 실행되는 Safari 8 이상

다른 웹 브라우저(다른 운영 체제에서 실행 중인 Safari 포함)에서는 사용자 인터페이스가 제대로 표시되지 않거나 일부 기능을 사용하지 못할 수 있습니다.

관리자 계정 활성화

파트너십 계약에 서명하면 다음 정보가 포함된 이메일 메시지를 받게 됩니다.

- **사용자 로그인.** 로그인하는 데 사용하는 사용자 이름입니다. 사용자 로그인 정보는 계정 활성화 페이지에도 표시됩니다.
- **계정 활성화** 버튼. 이 버튼을 클릭하여 계정의 비밀번호를 설정합니다. 비밀번호의 길이는 9자 이상이어야 합니다. 비밀번호에 대한 자세한 내용은 "비밀번호 요구 사항"(25페이지) 항목을 참조하십시오.

비밀번호 요구 사항

사용자 계정의 비밀번호는 9자 이상이어야 합니다. 또한 비밀번호의 복잡성이 확인되고 다음 범주 중 하나로 분류됩니다.

- 약함
- 중간
- 강함

약한 비밀번호는 9자 이상이어도 저장할 수 없습니다. 사용자 이름, 로그인, 사용자 이메일 또는 사용자 계정이 속한 테넌트의 이름이 포함된 비밀번호는 항상 약한 비밀번호로 간주됩니다. 대부분의 일반적인 비밀번호는 약한 비밀번호로 간주됩니다.

비밀번호를 강화하려면 문자를 더 추가하십시오. 숫자, 대문자와 소문자, 특수 문자 등 다양한 유형의 문자를 사용하는 것은 필수는 아니지만 짧아도 더 강력한 비밀번호가 될 수 있습니다.

관리 포털 액세스

1. 서비스 로그인 페이지로 이동합니다.
2. 로그인 페이지 주소는 수신된 활성화 이메일 메시지에 포함되어 있습니다.
3. 로그인 정보를 입력하고 **다음**을 클릭합니다.
4. 패스워드 정보를 입력하고 **다음**을 클릭합니다.

> **참고**
> Cyber Protect Cloud에서 무차별 암호 대입 공격을 방지하기 위해 로그인 시도가 10번 실패하면 포털에서 계정이 잠깁니다. 잠금 기간은 5분입니다. 로그인 실패 횟수는 15분 후에 재설정됩니다.

5. 오른쪽 메뉴를 사용하여 관리 포털을 탐색할 수 있습니다.

관리 포털의 시간 초과 기간은 활성 세션에 대해 24시간, 유휴 세션에 대해 1시간입니다.

일부 서비스에는 서비스 콘솔에서 관리 포털로 전환하는 기능이 포함되어 있습니다.

회사 프로필 마법사에서 연락처 구성

회사의 연락처 정보를 구성할 수 있습니다. 제공한 연락처로 플랫폼의 새로운 기능 및 기타 중요한 변경 내용에 대한 업데이트를 보내드립니다.

관리 포털에 처음으로 로그인하면 회사 프로필 마법사가 회사 및 제공할 연락처에 대한 기본 정보를 안내합니다.

Cyber Protect 플랫폼에 존재하는 사용자로부터 연락처를 생성하거나 서비스에 대한 액세스 권한이 없는 사용자의 연락처 정보를 추가할 수 있습니다.

회사 프로필 마법사를 사용하여 회사 연락처를 구성하는 방법

1. **회사 정보**에서 다음과 같은 회사 상세 정보를 지정합니다.
   - **공식(법적) 회사명**
   - **회사 법인 주소(본사 주소)**
     - **국가**
     - **우편 번호**
2. **다음**을 클릭합니다.
3. **회사 연락처**에서 다음과 같은 용도의 연락처를 구성합니다.
   - **요금 청구 연락처** - 플랫폼의 사용량 보고와 관련된 중요한 변경 내용에 대한 업데이트를 보내기 위한 연락처입니다.
   - **비즈니스 연락처** - 플랫폼에서 비즈니스와 관련된 중요한 변경 내용에 대한 업데이트를 보내기 위한 연락처입니다.
   - **기술 지원 연락처** - 플랫폼 기술과 관련된 중요한 변경 내용에 대한 업데이트를 보내기 위한 연락처입니다.

   연락처 하나를 둘 이상의 용도로 사용할 수 있습니다.

연락처를 생성할 옵션을 선택합니다.

- **기존 사용자에서 생성**. 드롭다운 목록에서 사용자를 선택합니다.
- **새 연락처 생성**. 다음 연락처 정보를 제공합니다.
  - **이름** - 연락처 사용자의 이름입니다. 이 필드는 필수 필드입니다.
  - **성** - 연락처 사용자의 성입니다. 이 필드는 필수 필드입니다.
  - **비즈니스 이메일** - 연락처 사용자의 이메일 주소입니다. 이 필드는 필수 필드입니다.
  - **직장 전화** - 이 필드는 선택 사항입니다.
  - **직함** - 이 필드는 선택 사항입니다.

4. 요금 청구 연락처를 비즈니스 또는 기술 지원 연락처로 사용하려는 경우 **요금 청구 연락처** 섹션에서 해당 플래그를 선택합니다.
   - **비즈니스 연락처로 동일한 연락처 사용**
   - **기술 지원 연락처로 동일한 연락처 사용**
5. **완료**를 클릭합니다.

   그러면 연락처가 생성됩니다. 회사 연락처 구성에 설명된 대로 관리 콘솔의 **회사 관리 > 회사 프로필** 섹션에서 정보를 편집하고 다른 연락처를 구성할 수 있습니다.

관리 포털에서 Cyber Protect 콘솔 액세스

1. 관리 포털에서 **모니터링** > **사용**으로 이동합니다.
2. **Cyber Protect**에서 **보호**를 선택하고 **서비스 관리**를 클릭합니다.

   또는 **클라이언트**에서 고객을 선택하고 **서비스 관리**를 클릭합니다.

그러면 Cyber Protect 콘솔로 리디렉션됩니다.

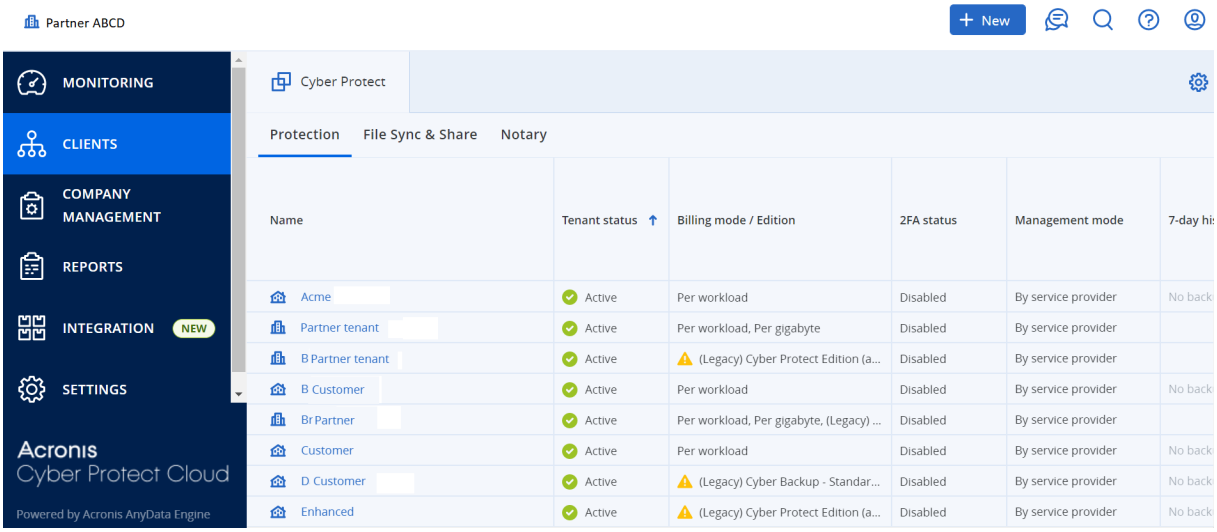
중요

관리 모드가 **셀프 서비스**인 고객의 서비스는 관리할 수 없습니다. 고객 관리자만 고객 모드를 **서비스 제공업체가 관리**로 변경한 후 서비스를 관리할 수 있습니다.

관리 포털의 탐색

관리 포털을 사용한다면 이 시점에 항상 테넌트 내에서 운영하고 있는 중입니다. 이 테넌트의 이름은 왼쪽 위에 표시됩니다.

기본적으로 사용할 수 있는 최상위 계층의 수준이 선택됩니다. 목록에서 테넌트 이름을 클릭하여 계층을 드릴다운합니다. 상위 수준으로 돌아가 탐색하려면 왼쪽 위에 있는 이름을 클릭합니다.



사용자 인터페이스의 모든 부분은 현재 운영 중인 테넌트만 표시하고 영향을 줍니다. 예:

- **클라이언트** 탭은 현재 운영 중인 테넌트의 직속 하위 테넌트만 표시합니다.
- **회사 관리** 탭에는 현재 운영 중인 테넌트에 있는 사용자 계정과 회사 프로필이 표시됩니다.
- **새로 만들기** 버튼을 사용해 현재 운영 중인 테넌트 내에서만 테넌트 또는 새 사용자 계정을 생성할 수 있습니다. 가입한 서비스에 따라 이 메뉴에서 추가 옵션이 제공될 수도 있습니다.

관리 포털의 새로운 기능

Cyber Protect Cloud의 새 기능이 릴리스되면 관리 포털 로그인 시에 이러한 기능의 간략한 설명이 포함된 팝업 창이 표시됩니다.

기본 관리 포털 창 왼쪽 아래의 **새로운 기능** 링크를 클릭하여 새 기능의 설명을 확인할 수도 있습니다.

웹 인터페이스에 대한 액세스 제한

관리자는 테넌트 구성원이 로그인할 수 있도록 허용되는 IP 주소 목록을 지정하여 웹 인터페이스에 대한 액세스를 제한할 수 있습니다.

또한 이러한 제한은 API를 통해 관리 포털에 액세스할 때 적용됩니다.

참고
이 제한은 설정된 수준에서만 적용됩니다. 하위 테넌트의 멤버에게는 적용되지 않습니다.

웹 인터페이스에 대한 액세스를 제한하려면

1. 관리 포털에 로그인합니다.
2. 액세스를 제한하려는 테넌트로 이동합니다.
3. **설정** > **보안**을 클릭합니다.
4. **로그인 제어** 스위치를 활성화합니다.
5. **허용되는 IP 주소**에서 허용되는 IP 주소를 지정합니다.

다음과 같은 매개변수를 세미콜론으로 구분하여 입력할 수 있습니다.

- IP 주소(예: 192.0.2.0)
- IP 범위(예: 192.0.2.0-192.0.2.255)
- 서브넷(예: 192.0.2.0/24)

6. **저장**을 클릭합니다.

참고
Cyber Infrastructure(하이브리드 모델)를 사용하는 서비스 제공업체:

관리 포털의 **설정** > **보안**에서 **로그인 제어** 스위치가 활성화되어 있으면 Cyber Infrastructure 노드의 외부 공용 IP 주소(또는 주소 여러 개)를 **허용되는 IP 주소** 목록에 추가합니다.

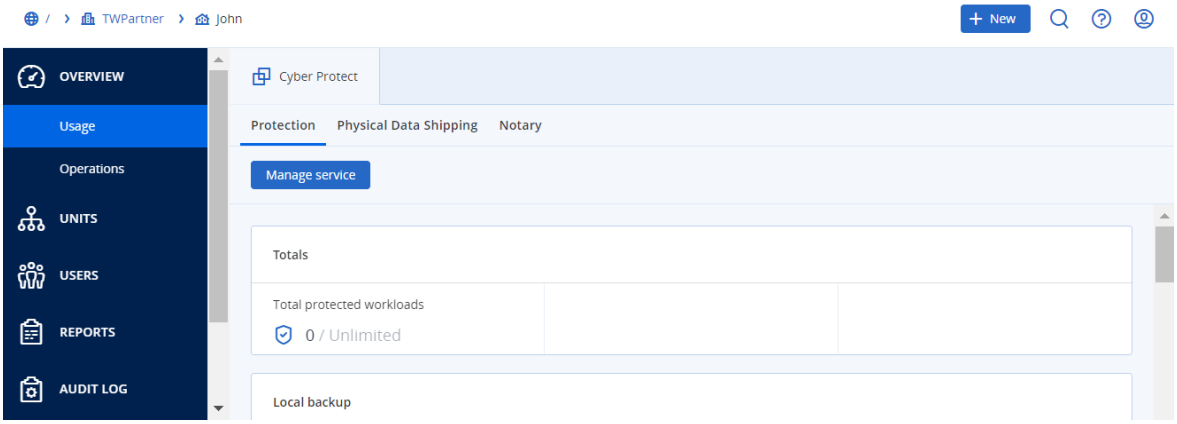
서비스 액세스

개요 탭

개요 > **사용** 섹션에서는 서비스 사용에 대한 개요를 제공하고 사용자가 운영 중인 테넌트 내의 서비스에 액세스할 수 있습니다.

개요 탭을 이용하여 테넌트에 대한 서비스를 관리하려면

1. 서비스를 관리할 테넌트로 이동한 다음, **개요** > **사용**을 클릭합니다.
   파트너 테넌트 수준과 고객 테넌트 수준에서 관리할 수 있는 서비스도 있지만 고객 테넌트 수준에서만 관리할 수 있는 서비스도 있습니다.
2. 관리할 서비스 이름을 클릭한 다음, 서비스 이름 옆의 **서비스 관리** 또는 **서비스 구성**을 클릭합니다.
   서비스 사용에 대한 자세한 내용은 서비스 콘솔에서 확인할 수 있는 사용자 안내서를 참조하십시오.

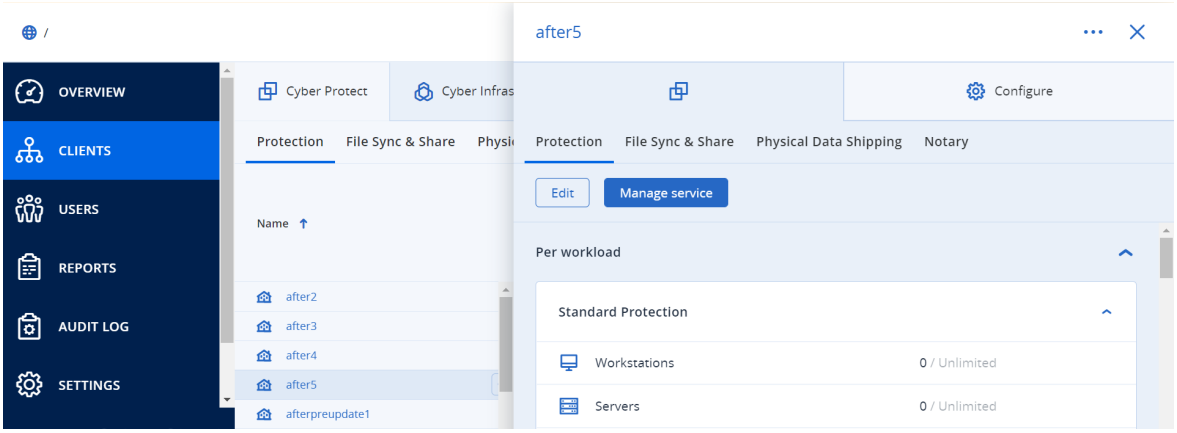


클라이언트 탭

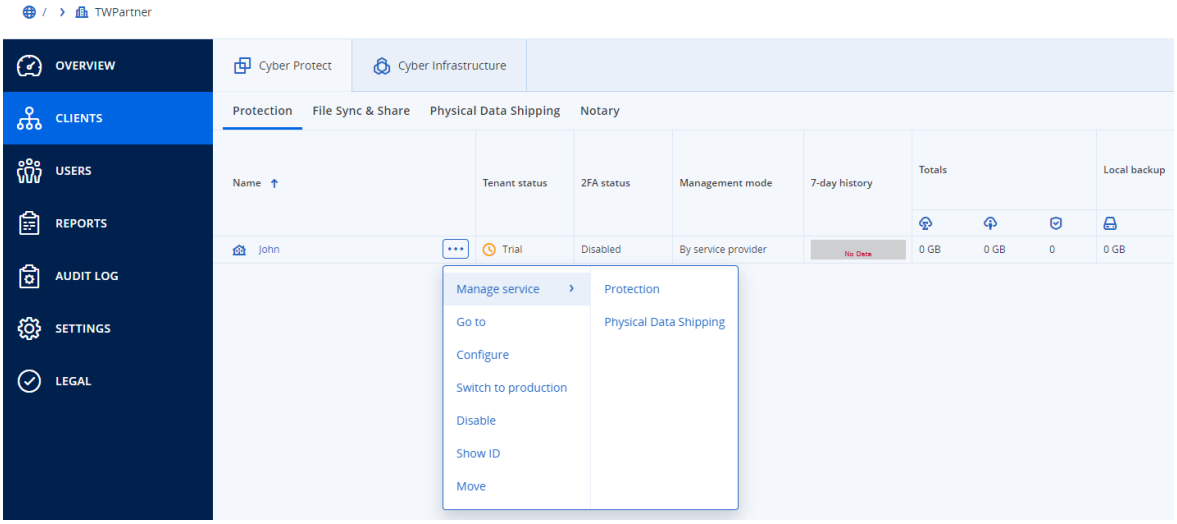
클라이언트 탭은 운영하려는 테넌트의 하위 테넌트가 표시되며, 이 탭을 사용해 테넌트 내의 서비스에 액세스할 수 있습니다.

클라이언트 탭을 이용하여 테넌트에 대한 서비스를 관리하려면

1. 다음 중 하나를 수행하십시오.
   - **클라이언트**를 클릭하고 관리할 테넌트를 선택하고 관리할 서비스 이름이나 아이콘을 클릭한 다음, **서비스 관리** 또는 **서비스 구성**을 클릭합니다.



   - **클라이언트**를 클릭하고 서비스를 관리할 테넌트의 이름 옆에 있는 말줄임표 아이콘을 클릭한 다음 **서비스 관리**를 클릭하고 관리할 서비스를 선택합니다.



   파트너 테넌트 수준과 고객 테넌트 수준에서 관리할 수 있는 서비스도 있지만 고객 테넌트 수준에서만 관리할 수 있는 서비스도 있습니다.

   서비스 사용에 대한 자세한 내용은 서비스 콘솔에서 확인할 수 있는 사용자 안내서를 참조하십시오.

7일 내역 표시줄

클라이언트 화면의 **7일 내역** 표시줄에는 지난 7일 동안의 각 고객 테넌트 대상 워크로드 백업 상태가 표시됩니다. 이 표시줄은 다양한 색이 지정된 줄 168개로 구분되어 있습니다. 1시간 간격에 해당되는 각 줄에는 해당 1시간 간격 동안의 최악 백업 상태가 표시됩니다.

다음 표에는 줄에 지정된 각 색상의 의미에 대한 자세한 내용이 나와 있습니다.

색상	설명
적색	1시간 간격 동안 백업이 하나 이상 실패함
오렌지색	1시간 간격 동안 백업이 하나 이상 완료되었으나 경고가 발생함(백업 오류는 발생하지 않음)
초록색	1시간 간격 동안 백업이 하나 이상 정상 완료됨(백업 오류나 경고는 발생하지 않음)
회색	1시간 간격 동안 완료된 백업이 없음

해당 통계가 수집될 때까지는 **7일 내역** 표시줄에 "백업 없음"이 표시됩니다.

파트너 테넌트의 경우에는 집계 통계가 지원되지 않으므로 **7일 내역** 표시줄이 비어 있습니다.

사용자 계정 및 테넌트

사용자 계정에는 관리자 계정과 사용자 계정, 이렇게 두 가지 유형이 있습니다.

- **관리자**는 관리 포털에 대한 액세스 권한이 있습니다. 관리자는 모든 서비스에 대한 관리자 역할을 갖습니다.
- **사용자**는 관리 포털에 대한 액세스 권한이 없습니다. 사용자의 서비스 액세스 권한 및 서비스에서 갖게 되는 역할은 관리자가 정의합니다.

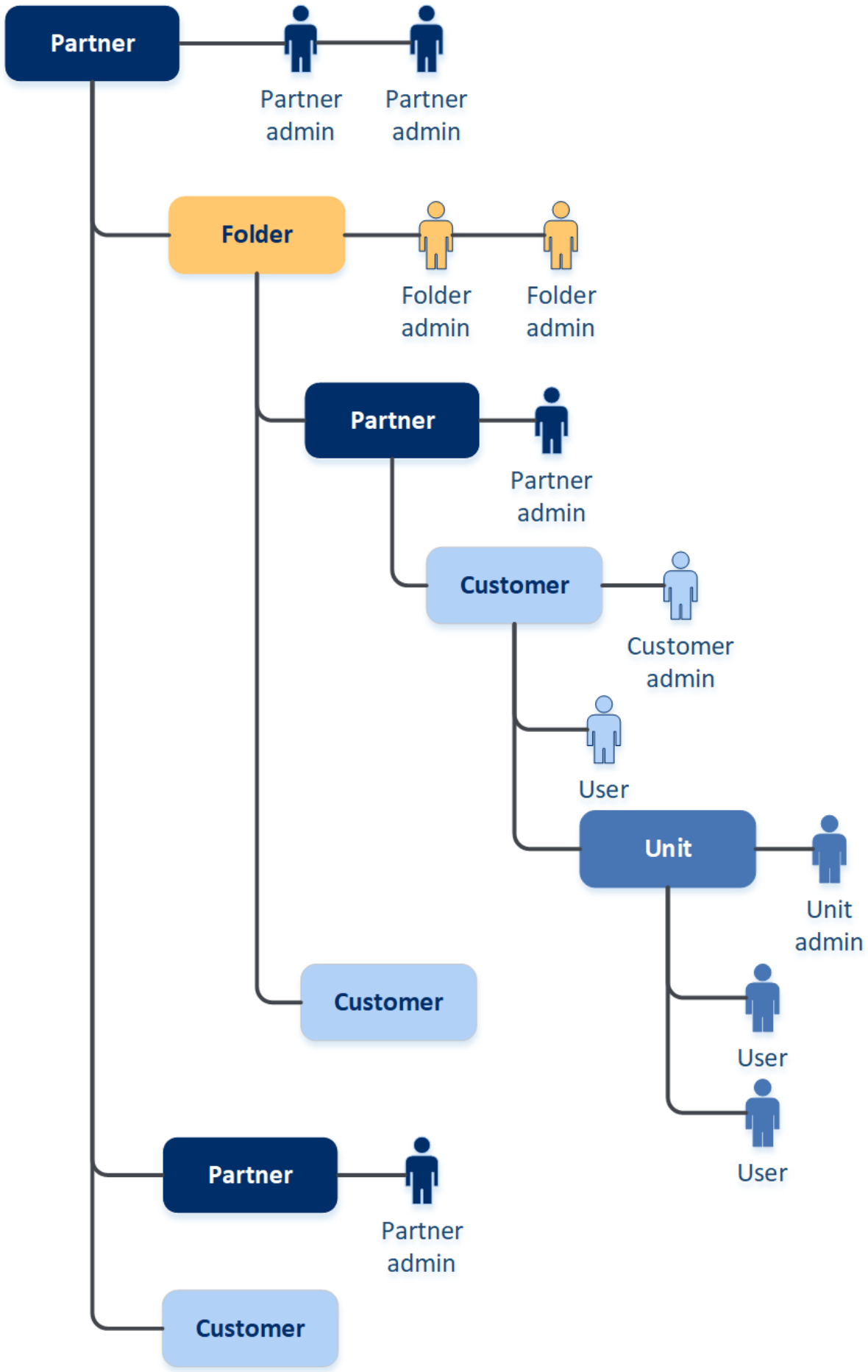
각 계정은 테넌트에 속해 있습니다. 테넌트는 관리 포털 리소스(사용자 계정, 하위 테넌트 등)와 파트너 또는 고객에 대한 전용 서비스 제공 사항(활성화된 서비스 및 제공 항목)의 일부입니다. 테넌트 계층은 서비스 사용자와 제공자 간의 클라이언트/공급업체 관계와 일치합니다.

- **파트너** 테넌트 유형은 일반적으로 서비스를 리셀링하는 서비스 제공업체에 해당합니다.
- **폴더** 테넌트 유형은 일반적으로 파트너 및 고객을 그룹화하여 별도의 제공 사항 및/또는 서로 다른 브랜딩을 구성하기 위해 파트너 관리자가 사용하는 보조 테넌트입니다.
- **고객** 테넌트 유형은 서비스를 사용하는 조직에 해당합니다.
- **단위** 테넌트 유형은 조직 내 단위 또는 부서에 해당합니다.

관리자는 계층 구조에서 자신의 수준 또는 그 아래 수준의 테넌트, 관리자 계정 및 사용자 계정을 생성 및 관리할 수 있습니다.

파트너 유형의 부모 테넌트 관리자는 **고객** 또는 **파트너** 유형 테넌트에서 하위 수준 관리자 역할을 수행할 수 있으며, 이 경우 관리 모드는 **서비스 제공업체가 관리**입니다. 따라서 가령 파트너 수준 관리자는 사용자 계정 및 서비스를 관리하거나 자식 테넌트의 백업 및 기타 리소스에 액세스할 수 있습니다. 하지만 이보다 수준이 낮은 관리자는 수준이 더 높은 관리자에 대해 자신의 테넌트에 대한 액세스를 제한할 수 있습니다.

다음 다이어그램은 파트너, 폴더, 고객 및 단위 테넌트의 예를 보여줍니다.


Partner
Partner admin
Partner admin
Folder
Folder admin
Folder admin
Partner
Partner admin
Customer
Customer admin
User
Unit
Unit admin
User
User
Customer
Partner
Partner admin
Customer

다음 표는 관리자 및 사용자가 수행할 수 있는 작업을 요약해서 보여줍니다.

작업	사용자	고객 및 단위 관리자	파트너 및 폴더 관리자
테넌트 생성	아니요	예	예
10, 15.	아니요	예	예
소프트웨어 다운로드 및 설치	예	예	아니요*
서비스 관리	예	예	예
서비스 사용에 대한 리포트 생성	아니요	예	예
브랜딩 구성	아니요	아니요	예

참고
어떤 테넌트 유형에서나 사용자를 생성할 수 있으며, 권한 수준이 높은 테넌트가 하위 테넌트를 생성한다면 이메일 주소도 공유할 수 있습니다. 예를 들어 파트너 테넌트는 폴더, 고객, 부서 테넌트를 생성할 수 있는 반면 고객 테넌트는 폴더 테넌트를 생성할 수 없습니다.

테넌트 관리

Cyber Protect에서 사용할 수 있는 테넌트는 다음과 같습니다.

- **파트너** 테넌트는 일반적으로 파트너십 계약에 서명한 각 파트너에 대해 생성됩니다.
- **폴더** 테넌트는 일반적으로 파트너 및 고객을 그룹화하여 별도의 제공 사항 및/또는 서로 다른 브랜딩을 구성하기 위해 생성됩니다.
- **고객** 테넌트는 일반적으로 서비스에 등록하는 각 조직을 위해 생성됩니다.
- 서비스를 새 조직 단위로 확장하려는 경우 고객 테넌트 내에서 새 **단위** 테넌트가 생성됩니다.

테넌트 생성 및 구성 단계는 생성하는 테넌트별로 다릅니다. 하지만 일반적으로 프로세스에 포함되는 단계는 다음과 같습니다.

1. 테넌트를 생성합니다.
2. 테넌트용 서비스를 선택합니다.
3. 테넌트에 대한 제공 항목을 구성합니다.

테넌트 생성

1. 관리 포털에 로그인합니다.
2. 테넌트를 생성하려는 테넌트로 이동합니다.
3. 오른쪽 위에서 **새로 만들기**를 클릭한 다음 생성하려는 테넌트의 유형에 따라 다음 중 하나를 클릭합니다.
   - **파트너** 테넌트는 일반적으로 파트너십 계약에 서명한 각 파트너에 대해 생성됩니다.
   - **폴더** 테넌트는 일반적으로 파트너 및 고객을 그룹화하여 별도의 제공 사항 및/또는 서로 다른 브랜딩을 구성하기 위해 생성됩니다.

- **고객** 테넌트는 일반적으로 서비스에 등록하는 각 조직을 위해 생성됩니다.
- 서비스를 새 조직 단위로 확장하려는 경우 고객 테넌트 내에서 새 **단위** 테넌트가 생성됩니다.

사용 가능한 유형은 상위 테넌트 유형에 따라 달라집니다.

4. **이름**에서 새 테넌트의 이름을 지정합니다.
5. [파트너 테넌트 생성 시에만 해당] **공식(합법) 회사명**(필수) 및 **VAT 번호/TAX ID/회사 등록 번호**(선택 사항)를 입력합니다.
6. [고객 테넌트 생성 시에만 해당됨] **모드**에서 테넌트가 서비스를 사용하는 모드(평가판 모드 또는 프로덕션 모드)를 선택합니다. 월간 서비스 사용 내역 보고서에는 이 두 모드의 테넌트 사용 내역 데이터가 포함됩니다.

중요

평가판 모드를 통해 30일 평가 기간을 사용할 수 있으며, 제품에 대한 전체 액세스 권한이 부여됩니다. 고객이 프로덕션 모드로 전환되면 사용량이 가장 가까운 청구 주기에 자동으로 포함됩니다.

언제든지 프로덕션 모드로 전환할 수 있습니다. 그러나 프로덕션에서 평가판 모드로 되돌릴 수는 없습니다.

고객의 평가판 사용 취소를 결정하는 경우에는 해당 고객 테넌트도 삭제해야 합니다. 이렇게 하지 않으면 30일 평가 기간 만료 시 고객 상태가 프로덕션 모드로 자동 전환되며 차기 도래하는 청구 주기에 해당 사용량 요금이 포함됩니다. 자세한 내용은 이 기술 자료 문서를 참조하십시오.

---

7. **관리 모드**에서 다음 모드 중 하나를 선택해 테넌트의 권한을 관리합니다.
   - **셀프 서비스** - 이 모드는 부모 테넌트 관리자의 이 테넌트에 대한 액세스 권한을 제한합니다. 이러한 관리자는 테넌트 속성만 수정할 수 있고 테넌트 내의 어떠한 항목(예: 테넌트, 사용자, 서비스, 백업 및 기타 리소스)도 액세스하거나 관리할 수 없습니다.
   - **서비스 제공업체가 관리** - 이 모드는 상위 테넌트 관리자에게 해당 테넌트에 대한 속성 수정 권한, 테넌트, 사용자, 서비스 관리 권한, 백업 및 기타 리소스에 대한 액세스 권한을 비롯한 모든 권한을 부여합니다. 이 모드는 기본적으로 선택됩니다.

   사용자가 생성한 테넌트의 관리자만 **셀프 서비스** 관리 모드를 변경할 수 있습니다. 이를 위해 생성된 테넌트의 관리자는 **설정** > **보안**으로 이동하여 **지원 액세스** 스위치를 설정할 수 있습니다.

   클라이언트 탭에서 하위 테넌트에 대해 선택한 관리 모드를 확인할 수 있습니다.
8. **보안**에서 테넌트에 대한 2단계 인증을 활성화 또는 비활성화합니다.
   활성화된 경우, 이 테넌트의 모든 사용자는 보안이 강화된 액세스를 위해 사용자 계정에 2단계 인증을 설정해야 합니다. 사용자는 2단계 인증의 두 번째 장치에 인증 애플리케이션을 설치하고, 생성된 일회성 TOTP 코드를 기존 로그인 및 패스워드와 함께 사용하여 콘솔에 로그인해야 합니다. 자세한 내용은 "2단계 인증 설정"을 참고하십시오. 고객의 2단계 인증 상태를 확인하려면 **클라이언트**로 이동합니다.
9. [규제 준수 모드에서 고객 테넌트를 생성할 때만 해당됨] **보안**에서 **규제 준수 모드** 확인란을 선택합니다.

이 모드에서는 암호화된 백업만 사용할 수 있습니다. 암호화 비밀번호는 보호된 장치에서 설정해야 하며 비밀번호가 없으면 백업 생성이 실패합니다. 그러면 클라우드 서비스에 암호화 비밀번호를 입력해야 하는 모든 작업을 수행할 수 없습니다. 자세한 내용은 "규제 준수 모드"(35페이지)을(를) 참조하십시오.

중요
테넌트를 생성한 후에는 규제 준수 모드를 비활성화할 수 없습니다.

10. **관리자 생성**에서 관리자 계정을 구성합니다.

    참고
    관리 모드가 **셀프 서비스**로 설정된 파트너 테넌트와 고객 테넌트의 경우 관리자를 반드시 생성해야 합니다.

    a. 관리자 계정의 이메일을 입력합니다. 로그인으로도 사용되는 이메일입니다.
    b. 이메일과 다른 로그인을 사용하려는 경우 **이메일과 다른 로그인 사용** 확인란을 선택하고 관리자 계정의 로그인 이름과 이메일을 입력합니다.
    나머지 필드는 선택 사항이지만 당사가 관리자에게 연락을 취해야 할 경우 더 많은 통신 채널을 제공합니다.
    c. 언어를 선택합니다.
    언어를 선택하지 않으면 영어가 기본으로 사용됩니다.
    d. 회사 연락처를 지정합니다.
    - **청구** - 플랫폼의 사용량 보고와 관련된 중요한 변경 내용에 대한 업데이트를 보내기 위한 연락처입니다.
    - **기술** - 플랫폼 기술과 관련된 중요한 변경 내용에 대한 업데이트를 보내기 위한 연락처입니다.
    - **비즈니스** - 플랫폼에서 비즈니스와 관련된 중요한 변경 내용에 대한 업데이트를 보내기 위한 연락처입니다.

    사용자 한 명에게 회사 연락처 여러 개를 할당할 수 있습니다.
11. **언어**에서 이 테넌트에 사용될 알림, 보고서, 소프트웨어의 기본 언어를 변경합니다.
12. 다음 중 하나를 수행하십시오.
    - 테넌트 생성을 완료하려면 **저장 및 닫기**를 클릭합니다. 이 경우 해당 테넌트에 대해 모든 서비스가 활성화됩니다. 보호 서비스의 요금 청구 모드는 워크로드당으로 설정됩니다.
    - 테넌트용 서비스를 선택하려면 **다음**을 클릭합니다. "테넌트용 서비스 선택"(36페이지)을(를) 참조하십시오.

규제 준수 모드

일반적인 수준보다 더 높은 보안 관련 요구를 충족해야 하는 고객은 규제 준수 모드를 사용할 수 있습니다. 이 모드에서는 모든 백업을 암호화해야 하며 로컬에서 설정한 암호화 암호만 사용 가능합니다.

규제 준수 모드에서는 고객 테넌트 및 해당 단위에서 생성하는 모든 백업이 AES 알고리즘과 256비트 키를 사용하여 자동 암호화됩니다. 사용자는 암호화 암호를 보호되는 장치에서만 설정할 수 있으며 보호 계획에서는 설정할 수 없습니다.

중요
파트너 관리자는 새 고객 테넌트 생성 시에만 규제 준수 모드를 활성화할 수 있으며 나중에 이 모드를 비활성화할 수는 없습니다. 기존 테넌트의 경우에는 규제 준수 모드를 활성화할 수 없습니다.

제한 사항

- 규제 준수 모드는 버전이 15.0.26390 이상의 에이전트 버전과만 호환됩니다.
- Red Hat Enterprise Linux 4.x 또는 5.x 버전과 해당 파생 버전을 실행하는 장치에서는 규제 준수 모드를 사용할 수 없습니다.
- 클라우드 서비스는 암호화 암호에 액세스할 수 없습니다. 이 제한으로 인해 규제 준수 모드가 적용된 테넌트에서는 일부 기능을 사용할 수 없습니다.

지원되지 않는 기능

규제 준수 모드가 설정된 테넌트에 사용할 수 없는 기능은 다음과 같습니다.

- Cyber Protect 콘솔을 통한 복구
- Cyber Protect 콘솔을 통해 파일 수준에서 백업 찾아보기
- 클라우드 간 백업
- 웹 사이트 백업
- 애플리케이션 백업
- 모바일 장치 백업
- 백업 맬웨어 방지 스캔
- 안전 복구
- 회사 허용 목록 자동 생성
- 데이터 보호 맵
- 재해 복구
- 사용 불가능 기능 관련 보고서 및 대시보드

테넌트용 서비스 선택

기본적으로는 새 테넌트를 생성하면 모든 서비스가 활성화됩니다. 테넌트 및 하위 테넌트 내의 사용자에게 제공할 서비스를 선택할 수 있습니다.

한 작업에서 여러 기존 테넌트를 선택한 후 서비스를 활성화할 수도 있습니다. 자세한 내용은 "여러 기존 테넌트에 대해 서비스 활성화"(38페이지)을(를) 참조하십시오.

단위 테넌트에는 이 절차가 적용되지 않습니다.

테넌트용 서비스를 선택하려면

1. 테넌트 생성/편집 대화 상자의 **서비스 선택** 섹션에서 요금 청구 모드나 버전을 선택합니다.
   - **워크로드당** 또는 **기가바이트당** 요금 청구 모드를 선택하고 테넌트에 대해 비활성화하려는 서비스의 확인란을 선택 취소합니다.
     두 요금 청구 모드의 서비스 세트는 동일합니다.
     Advanced Disaster Recovery의 경우 계정에 재해 복구 위치를 직접 등록했다면 드롭다운 목록에서 재해 복구 위치를 선택할 수 있습니다.
   - 레거시 버전을 사용하려면 **레거시 버전** 라디오 버튼을 선택하고 드롭다운 목록에서 버전을 선택합니다.

   비활성화된 서비스는 해당 테넌트 및 하위 테넌트에 있는 사용자에게 숨겨집니다.
2. 다음 중 하나를 수행하십시오.
   - 테넌트 생성을 완료하려면 **저장 및 닫기**를 클릭합니다. 이 경우 선택한 서비스의 모든 제공 항목이 테넌트가 사용 가능하도록 활성화되며 할당량은 무제한으로 설정됩니다.
   - 테넌트에 대한 제공 항목을 구성하려면 **다음**을 클릭합니다. "테넌트용 제공 항목 구성"(37페이지)을(를) 참조하십시오.

테넌트용 제공 항목 구성

새 테넌트를 생성하면 선택한 서비스의 모든 제공 항목이 활성화됩니다. 테넌트 및 하위 테넌트 내의 사용자에게 제공할 제공 항목을 선택하고 이러한 제공 항목의 할당량을 설정할 수 있습니다.

단위 테넌트에는 이 절차가 적용되지 않습니다.

테넌트용 제공 항목을 구성하려면

1. 테넌트 생성/편집 대화 상자의 **서비스 구성** 섹션에 있는 각 서비스 탭에서 비활성화하려는 제공 항목의 확인란을 선택 취소합니다.
   비활성화된 제공 항목에 해당하는 기능은 해당 테넌트 및 하위 테넌트에 있는 사용자가 사용할 수 없습니다.
2. 새 테넌트에 제공할 스토리지를 선택할 수 있는 서비스도 있습니다. 스토리지는 위치별로 분류됩니다. 테넌트에 대해 사용 가능한 위치와 스토리지 목록 중에서 선택할 수 있습니다.
   - 파트너/폴더 테넌트를 생성할 때 각 서비스에 대해 여러 위치와 스토리지를 선택할 수 있습니다.
   - 고객 테넌트를 생성할 때는 하나의 위치를 선택한 후 이 위치 안에서 서비스당 하나의 스토리지를 선택해야 합니다. 고객에게 할당된 스토리지는 나중에 변경할 수 있지만, 고객이 스토리지를 사용하기 전 또는 고객이 이 스토리지에서 모든 백업을 삭제한 후에 사용량이 0GB인 경우에만 변경이 가능합니다. 스토리지 공간 사용에 대한 정보는 실시간으로 업데이트되지 않습니다. 정보가 업데이트되는 데 최대 24시간이 필요합니다.

   스토리지 관련 상세정보는 "위치 및 스토리지 관리"를 참조하십시오.
3. 한 항목에 대한 할당량을 지정하려면 제공 항목 옆의 **무제한** 링크를 클릭합니다.
   이러한 할당량은 "유연"합니다. 이러한 값이 초과되면 테넌트 관리자와 상위 테넌트의 관리자에게 이메일 알림이 전송됩니다. 서비스 사용에 대한 제한 사항은 적용되지 않습니다. 파트너 테넌트의 경우 파트너 테넌트 생성 시 초과분을 설정할 수 없기 때문에 제공 항목 사용량이 할당량을 초과할 수 있습니다.

4. [고객 테넌트를 생성하는 경우에만 해당] 할당량 초과분을 지정합니다.
   초과분은 고객 테넌트가 특정 값까지 할당량을 초과하도록 허용합니다. 초과분이 초과하면 해당 서비스 사용에 대한 제한이 적용됩니다.
5. **저장 후 닫기**를 클릭합니다.

새로 생성된 테넌트는 관리 콘솔의 **클라이언트** 탭에 표시됩니다.

테넌트 설정을 편집하거나 관리자를 변경하려면 **클라이언트** 탭에서 테넌트를 선택한 다음 편집하려는 섹션의 연필 아이콘을 클릭합니다.

여러 기존 테넌트에 대해 서비스 활성화

여러 테넌트(한 세션에서 최대 100개 테넌트)에 대해 서비스, 버전, 팩 및 제공 항목을 대량으로 활성화할 수 있습니다.

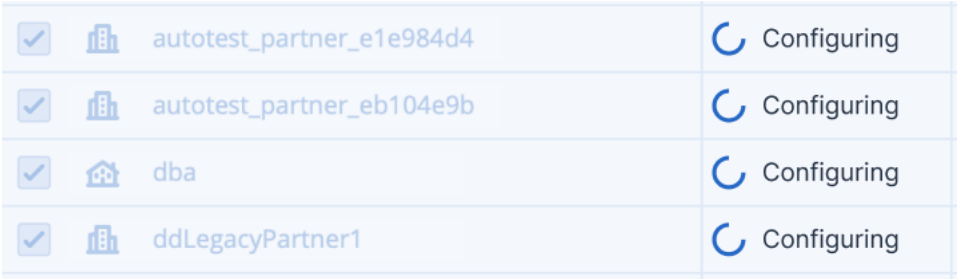
이 절차는 하위 루트, 파트너, 폴더 및 고객 테넌트에 적용됩니다. 이러한 여러 유형의 테넌트를 동시에 선택할 수 있습니다.

여러 테넌트에 대해 서비스를 활성화하려면

1. 관리 포털에서 **클라이언트**로 이동합니다.
2. 오른쪽 위의 **서비스 구성**을 클릭합니다.
3. 테넌트 이름 옆의 확인란을 선택하여 서비스를 활성화할 각 테넌트를 선택한 후 **다음**을 클릭합니다.
4. **서비스 선택** 섹션에서 선택한 모든 테넌트에 적용할 관련 서비스를 선택하고 **다음**을 클릭합니다.

   참고
   이 화면에서 이전에 활성화한 서비스를 비활성화할 수는 없습니다. 이 절차를 시작하기 전에 선택한 모든 서비스, 버전 및 제공 항목은 활성화된 상태로 유지됩니다.

5. **서비스 구성** 섹션에서 선택한 테넌트에 대해 활성화할 서비스 기능과 제공 항목을 선택하고 **다음**을 클릭합니다.
6. **요약** 섹션에서 선택한 테넌트에 적용할 변경 사항을 검토합니다.
   모두 펼치기를 클릭하면 모든 테넌트에 적용하도록 선택한 서비스와 제공 항목을 확인할 수 있습니다. 각 테넌트를 확장하여 해당 테넌트에 적용하도록 선택한 서비스와 제공 항목을 확인할 수도 있습니다.
7. **변경 사항 적용**을 클릭합니다. 각 테넌트에 대해 서비스를 구성하는 동안에는 테넌트가 비활성화되며 다음과 같이 **테넌트 상태** 열에 현재 구성 중인 서비스 및 제공 항목이 표시됩니다.



8. 서비스 및 제공 항목 구성이 선택한 테넌트에 정상적으로 적용되면 확인 메시지가 표시됩니다. 테넌트에 서비스 및 제공 항목을 적용할 수 없는 경우에는 **테넌트 상태** 열에 **적용되지 않음**이 표시됩니다. **다시 시도**를 클릭하여 선택한 테넌트의 구성을 검토합니다.

유지보수 알림 활성화

파트너 사용자는 자식 테넌트(파트너와 고객)가 Cyber Protect 데이터 센터에서 유지보수 알림 이메일을 직접 수신하고 관리 포털 내에서 제품 내 유지보수 알림을 수신하도록 허용할 수 있습니다. 그러면 유지보수 관련 지원 요청 수를 줄일 수 있습니다.

참고
데이터 센터에서 유지보수 알림 이메일에 브랜드를 적용합니다. 이러한 알림에는 사용자 정의 브랜딩이 지원되지 않습니다.

하위 파트너 또는 고객을 대상으로 유지보수 알림을 활성화하려면

1. 파트너 사용자로 관리 포털에 로그인하여 **고객**을 클릭한 후 유지보수 알림을 활성화할 파트너 또는 고객 테넌트의 이름을 클릭합니다.
2. **구성**을 클릭합니다.
3. **일반 설정** 탭에서 **유지보수 알림** 옵션을 찾아서 활성화합니다.
   유지보수 알림 옵션이 표시되지 않으면 서비스 제공업체에 문의하십시오.

참고
이 단계를 수행하면 유지보수 알림이 활성화되기는 하지만 선택한 테넌트가 사용자를 대상으로 알림을 활성화하거나 하위 파트너 또는 고객에게 해당 옵션을 다시 전파하여 해당 사용자를 대상으로 알림을 활성화할 때까지는 전송되지 않습니다.

사용자를 대상으로 유지보수 알림을 활성화하려면

1. 파트너 사용자 또는 회사 관리자로 관리 포털에 로그인합니다.
   파트너는 관리 대상인 모든 테넌트의 사용자를 대상으로 유지보수 알림을 활성화할 수 있습니다.
2. **회사 관리** > **사용자**를 클릭한 후 유지보수 알림을 활성화할 사용자의 이름을 클릭합니다.
3. **서비스** 탭의 **설정** 섹션에서 연필 아이콘을 클릭하여 옵션을 편집합니다.
4. **유지보수 알림** 확인란을 선택하고 **완료**를 클릭합니다.

그러면 선택한 사용자가 데이터 센터에서 진행될 예정인 유지보수 활동 관련 이메일 알림을 받게 됩니다.

자체 관리 고객 프로필 구성

파트너는 관리 대상 테넌트의 자체 관리 고객 프로필을 구성할 수 있습니다. 이 옵션을 사용하면 각 고객의 테넌트 프로필과 연락처 정보 표시 유형을 제어할 수 있습니다.

자체 관리 고객 프로필을 구성하려면

1. 관리 포털에서 **클라이언트**로 이동합니다.
2. 자체 관리 고객 프로필을 구성할 고객을 선택합니다.
3. **구성** 탭을 선택하고 **일반 설정** 탭을 선택합니다.
4. **자체 관리 고객 프로필 활성화** 스위치를 활성화하거나 비활성화합니다.

자체 관리 고객 프로필을 활성화하면 해당 고객이 탐색 메뉴의 **회사 프로필** 섹션, 그리고 사용자 생성 마법사의 연락처 관련 필드(**직장 전화번호**, **회사 연락처**, **직함**)를 확인할 수 있습니다.

자체 관리 고객 프로필을 비활성화하면 탐색 메뉴의 **회사 프로필** 섹션과 사용자 생성 마법사의 연락처 관련 필드가 숨겨집니다.

회사 연락처 구성

파트너로서 회사 및 사용자가 관리하는 테넌트에 대한 연락처 정보를 구성할 수 있습니다. 이 목록에 있는 연락처로 플랫폼의 새로운 기능 및 기타 중요한 변경 사항에 대한 업데이트를 보내드립니다.

사용자 역할에 따라 여러 연락처를 추가하고 회사 연락처를 할당할 수 있습니다. Cyber Protect 플랫폼에 존재하는 사용자로부터 연락처를 생성하거나 서비스에 대한 액세스 권한이 없는 사용자의 연락처 정보를 추가할 수 있습니다.

회사용 연락처를 구성하려면

1. 관리 콘솔에서 **회사 관리** > **회사 프로필**로 이동합니다.
2. **연락처** 섹션에서 **+**를 클릭합니다.
3. 연락처를 생성할 옵션을 선택합니다.
   - **기존 사용자에서 생성**
     - 드롭다운 목록에서 사용자를 선택합니다.
     - 회사 연락처를 선택합니다.
       - **청구** - 플랫폼의 사용량 보고와 관련된 중요한 변경 내용에 대한 업데이트를 보내기 위한 연락처입니다.
       - **기술** - 플랫폼 기술과 관련된 중요한 변경 내용에 대한 업데이트를 보내기 위한 연락처입니다.
       - **비즈니스** - 플랫폼에서 비즈니스와 관련된 중요한 변경 내용에 대한 업데이트를 보내기 위한 연락처입니다.

       사용자 한 명에게 회사 연락처 여러 개를 할당할 수 있습니다.

     회사너 프로필의 연락처 목록에서 사용자와 연결된 연락처를 삭제해도 해당 사용자는 삭제되지 않습니다. 시스템에서 사용자에 대한 모든 회사 연락처를 할당 해제하므로 **사용자** 목록의 **회사 연락처** 열에 회사 연락처가 더 이상 표시되지 않습니다.

     사용자와 연결된 연락처의 이메일 주소를 변경하고 싶다면 시스템에서 새로 정의된 주소의 확인을 요청할 것입니다. 이 주소로 이메일이 전송되며 사용자는 변경 내용을 확인해야 합니다.

- **새 연락처 생성**
  - 연락처 정보를 입력합니다.
    - **이름** - 연락처 사용자의 이름입니다. 이 필드는 필수 필드입니다.
    - **성** - 연락처 사용자의 성입니다. 이 필드는 필수 필드입니다.
    - **비즈니스 이메일** - 연락처 사용자의 이메일 주소입니다. 이 필드는 필수 필드입니다.
    - **직장 전화** - 이 필드는 선택 사항입니다.
    - **직함** - 이 필드는 선택 사항입니다.
  - **회사 연락처**를 선택합니다.
    - **청구** - 플랫폼의 사용량 보고와 관련된 중요한 변경 내용에 대한 업데이트를 보내기 위한 연락처입니다.
    - **기술** - 플랫폼 기술과 관련된 중요한 변경 내용에 대한 업데이트를 보내기 위한 연락처입니다.
    - **비즈니스** - 플랫폼에서 비즈니스와 관련된 중요한 변경 내용에 대한 업데이트를 보내기 위한 연락처입니다.

      사용자 한 명에게 회사 연락처 여러 개를 할당할 수 있습니다.
4. **추가**를 클릭합니다.

테넌트용 연락처를 구성하려면

참고
하위 테넌트에 대한 연락처 정보를 수정하면 변경 내용이 테넌트에 표시됩니다.

1. 관리 포털에서 **클라이언트**로 이동합니다.
2. 테넌트를 클릭한 후 **구성**을 클릭합니다.
3. **연락처** 섹션에서 **+**를 클릭합니다.
4. 연락처를 생성할 옵션을 선택합니다.
   - **기존 사용자에서 생성**
     - 드롭다운 목록에서 사용자를 선택합니다.
     - 회사 연락처를 선택합니다.
       - **청구** - 플랫폼의 사용량 보고와 관련된 중요한 변경 내용에 대한 업데이트를 보내기 위한 연락처입니다.
       - **기술** - 플랫폼 기술과 관련된 중요한 변경 내용에 대한 업데이트를 보내기 위한 연락처입니다.
       - **비즈니스** - 플랫폼에서 비즈니스와 관련된 중요한 변경 내용에 대한 업데이트를 보내기 위한 연락처입니다.

         사용자 한 명에게 회사 연락처 여러 개를 할당할 수 있습니다.

     회사너 프로필의 연락처 목록에서 사용자와 연결된 연락처를 삭제해도 해당 사용자는 삭제되지 않습니다. 시스템에서 사용자에 대한 모든 회사 연락처를 할당 해제하므로 **사용자** 목록의 **회사 연락처** 열에 회사 연락처가 더 이상 표시되지 않습니다.

     사용자와 연결된 연락처의 이메일 주소를 변경하고 싶다면 시스템에서 새로 정의된 주소의 확인을 요청할 것입니다. 이 주소로 이메일이 전송되며 사용자는 변경 내용을 확인해야 합니다.

- **새 연락처 생성**
  - 연락처 정보를 입력합니다.
    - **이름** - 연락처 사용자의 이름입니다. 이 필드는 필수 필드입니다.
    - **성** - 연락처 사용자의 성입니다. 이 필드는 필수 필드입니다.
    - **비즈니스 이메일** - 연락처 사용자의 이메일 주소입니다. 이 필드는 필수 필드입니다.
    - **직장 전화** - 이 필드는 선택 사항입니다.
    - **직함** - 이 필드는 선택 사항입니다.
  - **회사 연락처**를 선택합니다.
    - **청구** - 플랫폼의 사용량 보고와 관련된 중요한 변경 내용에 대한 업데이트를 보내기 위한 연락처입니다.
    - **기술** - 플랫폼 기술과 관련된 중요한 변경 내용에 대한 업데이트를 보내기 위한 연락처입니다.
    - **비즈니스** - 플랫폼에서 비즈니스와 관련된 중요한 변경 내용에 대한 업데이트를 보내기 위한 연락처입니다.

      사용자 한 명에게 회사 연락처 여러 개를 할당할 수 있습니다.
5. **추가**를 클릭합니다.

테넌트의 사용량 데이터 새로 고침

기본적으로 사용량 데이터 새로 고침은 고정된 간격으로 수행됩니다. 테넌트의 사용량 데이터를 수동으로 새로 고칠 수 있습니다.

1. 관리 콘솔에서 **클라이언트**로 이동합니다.
2. 테넌트를 클릭하고 테넌트 행에서 말줄임표를 클릭합니다.
3. **사용량 새로 고침**을 선택합니다.

> **참고**
> 데이터를 페치하려면 최대 10분 정도 걸릴 수 있습니다.

4. 업데이트된 데이터를 확인하려면 페이지를 다시 로드하십시오.

테넌트 비활성화 및 활성화

테넌트를 일시적으로 비활성화해야 할 수도 있습니다. 예를 들면, 테넌트에 서비스 사용에 따른 부채가 있는 경우입니다.

테넌트를 비활성화하려면

1. 관리 포털에서 **클라이언트**로 이동합니다.
2. 비활성화할 테넌트를 선택한 다음, 말줄임표 아이콘 > **비활성화**를 클릭합니다.
3. **비활성화**를 클릭하여 작업을 확인합니다.

결과:

- 이 테넌트와 해당하는 모든 하위 테넌트가 비활성화되고, 그 서비스가 중지됩니다.
- 이 테넌트와 해당 하위 테넌트의 데이터는 Cyber Protect Cloud에 그대로 유지 및 저장되기 때문에 그 청구는 계속됩니다.
- 테넌트와 그 하위 테넌트 안의 모든 API 클라이언트는 비활성화되고 이러한 클라이언트를 사용한 모든 통합은 작동이 중지됩니다.

테넌트를 활성화하려면 클라이언트 목록에서 이를 선택한 다음 말줄임표 아이콘 > **활성화**를 클릭합니다.

네넌트를 다른 테넌트로 이동

관리 포털을 사용하면 테넌트를 특정 상위 테넌트에서 다른 상위 테넌트로 이동할 수 있습니다. 이는 고객을 특정 파트너에서 다른 파트너를 이전하려는 경우나, 클라이언트를 조직하기 위해 폴더 테넌트를 만든 다음 이 중 일부를 새로 만든 폴더 테넌트로 이동하려는 경우 유용할 수 있습니다.

이동 가능한 테넌트 유형

테넌트 유형	이동 가능	대상 테넌트
파트너	예	파트너 또는 폴더
폴더	예	파트너 또는 폴더
고객	예	파트너 또는 폴더
단위	아니요	없음

요구 및 제한 사항

- 원래 상위테넌트와 비교했을 때 대상 상위 테넌트에 같거나 더 많은 세트의 서비스 및 제공 항목이 있는 경우에만 테넌트를 이동할 수 있습니다.
- 고객 테넌트를 이동할 때는 원래 상위 테넌트에 있는 고객 테넌트에 할당된 모든 스토리지가 대상 상위 테넌트에 있어야 합니다. 고객 서비스 관련 데이터는 한 스토리지에서 다른 스토리지로 이동할 수 없으므로 이러한 요건이 필요합니다.
- 계획서비스 제공업체에서 관리하는 고객 테넌트의 경우, 서비스 제공업체 수준에서 고객 워크로드에 맞게 적용 가능한 계획이 있을 수 있습니다(예: 스크립팅 계획).

  이러한 고객 테넌트를 이동할 때는 서비스 제공업체의 계획이 고객 워크로드에서 해지되며, 이 계획과 관련된 모든 서비스가 이 고객에 대해 작동이 중지됩니다.
- 테넌트는 파트너 계정 계층 내에서 이동할 수 있습니다. 또한, 일부 고객 테넌트를 파트너 계정 계층 밖에 있는 대상 테넌트로 이동할 수도 있습니다. 해당 작업이 가능하지 알아보려면 계정 관리자에게 문의하십시오.
- 관리자(예: 관리 포털의 관리자 또는 회사 관리자)만 테넌트를 다른 상위 테넌트로 이동할 수 있습니다.

테넌트 이동 방법

1. 관리 포털에 로그인합니다.
2. 테넌트를 이동할 대상 파트너 또는 폴더 테넌트의 **내부 ID**를 찾아 복사합니다. 다음을 수행합니다.
   a. **클라이언트** 탭에서 테넌트를 이동할 대상 테넌트를 선택합니다.
   b. 테넌트 속성 패널에서 세로 말줄임표 아이콘을 클릭하고 **ID 표시**를 클릭합니다.
   c. **내부 ID** 필드에 표시된 텍스트 문자열을 복사한 다음 **취소**를 클릭합니다.
3. 이동할 테넌트를 선택한 후 대상 파트너/폴더로 이동합니다. 다음을 수행합니다.
   a. **클라이언트** 탭에서 이동할 테넌트를 선택합니다.
   b. 테넌트 속성 패널에서 세로 말줄임표 아이콘을 클릭하고 **이동**을 클릭합니다.
   c. 대상 테넌트의 내부 식별자를 붙여넣은 다음 **이동**을 클릭합니다.

작업은 즉시 시작되며, 최대 10분 정도 소요됩니다.

이동하는 테넌트에 하위 테넌트(예: 고객 테넌트가 안에 있는 파트너 또는 폴더 테넌트)가 있는 경우, 전체 테넌트 하위 트리가 대상 테넌트로 이동됩니다.

파트너 테넌트를 폴더 테넌트로 변환하거나 그 반대로 변환

관리 포털을 사용하면 파트너 테넌트를 폴더 테넌트로 변환할 수 있습니다.

이것은 그룹 용도로 파트너 테넌트를 사용하고 이제 테넌트 인프라를 적절하게 구성하려는 경우에 유용할 수 있습니다. 이는 운영 대시보드가 테넌트에 대한 집계 정보를 포함하기를 원할 때 유용합니다

또한 폴더 테넌트를 파트너 테넌트로 변환할 수 있습니다.

참고
변환은 안전한 작업이며 테넌트 및 서비스 관련 데이터 내의 사용자에게 영향을 주지 않습니다.

테넌트를 변환하려면:

1. 관리 포털에 로그인합니다.
2. **클라이언트** 탭에서 변환할 테넌트를 선택합니다.
3. 다음 중 하나를 수행하십시오.
   - 테넌트 이름 옆에 있는 말줄임표 아이콘을 클릭합니다.
   - 테넌트를 선택하고 테넌트 속성 패널에서 말줄임표 아이콘을 클릭합니다.
4. **폴더로 변환** 또는 **파트너로 변환**을 클릭합니다.
5. 결정을 확인합니다.

테넌트에 대한 액세스 제한

고객 수준 이상의 관리자는 수준이 더 높은 관리자만 자신의 테넌트에 액세스할 수 있도록 제한할 수 있습니다.

테넌트에 대한 액세스가 제한되지 않은 경우 상위 테넌트의 관리자는 테넌트에 대한 완전한 액세스 권한을 가지게 되며, 다음과 같은 작업을 수행할 수 있습니다:

- 속성 수정
- 테넌트, 사용자 및 서비스 관리
- 백업 및 기타 리소스에 액세스

테넌트에 대한 액세스가 제한된 경우 상위 테넌트 관리자는 테넌트 속성만 수정할 수 있습니다. 상위 테넌트 관리자는 해당 계정과 하위 테넌트를 전혀 볼 수 없습니다.

수준이 더 높은 관리자가 사용자의 테넌트에 액세스하지 못하게 하려면

1. 관리 포털에 로그인합니다.
2. **설정** > **보안**으로 이동합니다.
3. **액세스 지원** 스위치를 비활성화합니다.

결과적으로 상위 테넌트의 관리자는 테넌트에 대한 액세스 권한이 제한됩니다. 해당 관리자는 테넌트 속성을 수정할 수만 있으며, 테넌트, 사용자, 서비스, 백업 및 기타 리소스와 같은 내부의 모든 것에 액세스하거나 관리할 수 없습니다.

테넌트 삭제

사용하는 리소스 공간을 확보하기 위해 테넌트를 지워야 할 수 있습니다. 사용 통계는 삭제 후 1일 이내로 업데이트됩니다. 테넌트의 크기가 큰 경우, 더 많은 시간이 소요될 수 있습니다.

테넌트를 삭제하기 전에 비활성화해야 합니다. 작업의 수행 방법에 대한 자세한 내용은 테넌트 비활성화 및 활성화를 참조하십시오.

참고
Cyber Protect에서 테넌트를 복구할 수는 있지만 File Sync & Share 서비스에서는 복구가 지원되지 않습니다.

테넌트를 삭제하려면

1. 관리 포털에서 **클라이언트**로 이동합니다.
2. 삭제하려는 비활성화된 테넌트를 선택한 다음, 말줄임표 아이콘 > **삭제**를 클릭합니다.
3. 작업을 확인하려면 로그인한 다음 **삭제**를 클릭합니다.

결과:

- 테넌트와 그 하위 테넌트가 삭제됩니다.
- 테넌트와 그 하위 테넌트에서 활성화된 모든 서비스가 중지됩니다.
- 테넌트와 그 하위 테넌트에 있는 모든 사용자가 삭제됩니다.
- 테넌트와 그 하위 테넌트에 있는 모든 머신의 등록이 해제됩니다.
- 테넌트와 그 하위 테넌트에 있는 모든 서비스 관련 데이터(예: 백업 및 동기화된 파일)가 삭제됩니다.

- 테넌트와 그 하위 테넌트 안의 모든 API 클라이언트는 삭제되고 이러한 클라이언트를 사용한 모든 통합은 작동이 중지됩니다.
- **테넌트 상태**가 **삭제됨**으로 표시됩니다. **삭제됨** 상태를 마우스로 가리키면 테넌트가 삭제된 날짜, 그리고 이 삭제 날짜로부터 30일 내에 모든 관련 데이터와 설정을 복구할 수 있다는 참고 사항이 표시됩니다.

테넌트 복구

테넌트를 실제로 삭제하는 경우에 대비하여 Cyber Protect에서는 테넌트 복구 기능을 제공합니다.

예를 들어 다음과 같은 경우 테넌트를 복구해야 할 수 있습니다.

- 파트너가 테넌트를 실수로 삭제한 경우.
- 파트너 개발 팀이 통합을 테스트하다가 테넌트 계층의 일부분이나 전체 테넌트 계층을 실수로 삭제한 경우.
- 파트너 통합 중에 새 버전으로 전환해야 하는데 실수로 애플리케이션의 프로비저닝을 취소하여 데이터를 복원해야 하는 경우.
- 파트너가 새 라이선스로 전환하다가 실수로 애플리케이션을 비활성화하여 비활성화된 애플리케이션의 데이터를 복원해야 하는 경우.

테넌트 복구 방법

1. 관리 포털에서 **클라이언트**로 이동합니다.
2. **Cyber Protect** 탭에서 복구할 테넌트를 찾습니다. 테넌트의 상태는 **삭제됨**으로 표시됩니다.
3. 테넌트를 마우스로 가리키고 말줄임표 아이콘 을 클릭합니다.
4. **복구**를 클릭합니다.
   테넌트가 삭제되기 전과 같은 상태로 복구되며 기본적으로 비활성화된다는 메시지가 포함된 확인 창이 나타납니다.
5. [선택 사항] 테넌트를 활성화해야 하는 경우 **테넌트를 활성화합니다** 확인란을 선택합니다. 테넌트는 나중에 언제든지 활성화할 수 있습니다.
6. **복구**를 클릭합니다.

결과:

- 테넌트와 그 하위 테넌트가 복구됩니다.
- 테넌트와 그 하위 테넌트 내에서 활성화되어 있었던 모든 서비스가 다시 시작됩니다.

참고
File Sync & Share 서비스에서는 복구가 지원되지 않습니다.

- 테넌트와 그 하위 테넌트에 있는 모든 사용자가 복구됩니다.
- 테넌트와 그 하위 테넌트에 있는 모든 머신이 다시 등록됩니다.
- 테넌트 및 하위 테넌트에 있는 모든 서비스 관련 데이터(예: 백업)가 복구됩니다.

- 테넌트와 그 하위 테넌트 안의 모든 API 클라이언트가 복구되고 이러한 클라이언트를 사용한 모든 통합의 작동이 다시 시작됩니다.
- **테넌트 상태**는 테넌트를 활성화한 경우에는 **활성**으로 표시되고 아직 활성화하지 않은 경우에는 **비활성화됨**으로 표시됩니다.

사용자 관리

파트너 관리자, 고객 관리자 및 부서 관리자는 액세스 가능한 테넌트에서 사용자 계정을 구성하고 관리할 수 있습니다.

사용자 계정 생성

다음과 같은 경우 추가 계정 생성을 원할 수 있습니다.

- 파트너/폴더 관리자 계정 — 다른 사람과 서비스 관리 역할을 공유하려는 경우.
- 고객/잠재 고객/단위 관리자 계정 — 액세스 권한이 해당 고객/잠재 고객/단위로 엄격히 제한될 다른 사용자에게 서비스 관리를 위임하려는 경우.
- 고객 또는 단위 테넌트 내의 사용자 계정 — 사용자가 서비스의 하위 세트에만 액세스할 수 있도록 하려는 경우.

기존 계정은 테넌트 간에 이동할 수 없음을 명심하십시오. 우선 테넌트를 생성한 다음 여기에 계정을 채웁니다.

사용자 계정을 생성하려면

1. 관리 포털에 로그인합니다.
2. 사용자 계정을 생성하려는 테넌트로 이동합니다. "관리 포털의 탐색"(27페이지)을(를) 참조하십시오.
3. 오른쪽 위에서 **새로 만들기** > **사용자**를 클릭합니다.
   또는 **회사 관리** > **사용자**로 이동하여 **+ 새로 만들기**를 클릭합니다.
4. 계정에 대한 다음 연락처 정보를 지정합니다.
   a. **이메일**. 로그인으로도 사용되는 이메일입니다.
   b. 이메일과 다른 로그인을 사용하려는 경우 **이메일과 다른 로그인 사용** 확인란을 선택하고 **로그인** 및 **이메일**을 입력합니다.

      중요
      각 계정에는 고유한 로그인 정보가 있어야 합니다.

      중요
      사용자가 File Sync & Share 서비스에 등록되어 있으면 File Sync & Share 등록에 사용한 이메일을 입력하십시오.
      각 고객 사용자 계정의 이메일 주소는 고유해야 합니다.

   c. **이름**

d. **성**

e. [선택 사항] **직장 전화**

> **참고**
> 상위 파트너가 고객 테넌트를 대상으로 자체 관리 고객 프로필 활성화 옵션을 활성화한 경우에만 **직장 전화**, **직함**, **회사 연락처** 등의 필드가 사용자 생성 마법사에 표시됩니다. 그렇지 않은 경우에는 이러한 필드가 표시되지 않습니다.

f. [선택 사항] **직함**

g. **언어**에서 이 계정에 사용될 알림, 보고서, 소프트웨어의 기본 언어를 변경합니다.

5. [선택 사항] 회사 연락처를 지정합니다.
   - **청구** - 플랫폼의 사용량 보고와 관련된 중요한 변경 내용에 대한 업데이트를 보내기 위한 연락처입니다.
   - **기술** - 플랫폼 기술과 관련된 중요한 변경 내용에 대한 업데이트를 보내기 위한 연락처입니다.
   - **비즈니스** - 플랫폼에서 비즈니스와 관련된 중요한 변경 내용에 대한 업데이트를 보내기 위한 연락처입니다.

   사용자 한 명에게 회사 연락처 여러 개를 할당할 수 있습니다.

   사용자 목록의 **회사 연락처** 열에서 사용자에게 할당된 회사 연락처를 보고 필요한 경우 사용자 계정을 편집하여 회사 연락처를 변경할 수 있습니다.
6. [파트너/폴더 테넌트에서 계정을 생성할 때는 사용할 수 없음] 각 서비스에서 사용자가 액세스와 역할을 갖게 될 서비스를 선택합니다.

   사용 가능한 서비스는 사용자 계정이 생성된 테넌트에 대해 활성화된 서비스에 따라 다릅니다.
   - **회사 관리자** 확인란을 선택한 경우 사용자는 테넌트에 대해 현재 활성화된 모든 서비스의 관리 포털과 관리자 역할에 대한 액세스 권한을 갖게 됩니다. 사용자는 향후에 테넌트에 대해 활성화될 모든 서비스에서 관리자 역할도 갖게 됩니다.
   - **단위 관리자** 확인란을 선택한 경우 사용자는 관리 포털에 대한 액세스 권한을 갖지만, 서비스 관리자 역할의 유무는 서비스에 따라 달라집니다.
   - 확인란을 선택하지 않은 경우 사용자는 지정한 서비스에서 지정한 역할만 갖게 됩니다.
7. **생성**을 클릭합니다.

새로 생성된 사용자 계정은 **회사 관리** 아래의 **사용자** 탭에 표시됩니다.

사용자 설정을 편집하거나 사용자에 대해 알림 설정 및 할당량(파트너/폴더 관리자는 사용할 수 없음)을 지정하려면 **사용자** 탭에서 사용자를 선택한 다음 편집하려는 섹션의 연필 아이콘을 클릭합니다.

사용자의 비밀번호를 재설정하는 방법

1. 관리 포털에서 **회사 관리** > **사용자**로 이동합니다.
2. 비밀번호를 재설정하려는 사용자를 선택한 다음, 말줄임표 아이콘 > **비밀번호 재설정**을 클릭합니다.
3. **재설정**을 클릭하여 작업을 확인합니다.

사용자는 이제 수신한 이메일의 지침을 따라 재설정 프로세스를 완료할 수 있습니다.

2단계 인증을 지원하지 않는 서비스(예: Cyber Infrastructure의 등록 서비스)에서는 사용자 계정을 *서비스 계정*으로 변환해야 할 수도 있습니다. 서비스 계정은 2단계 인증을 진행할 필요가 없는 계정입니다.

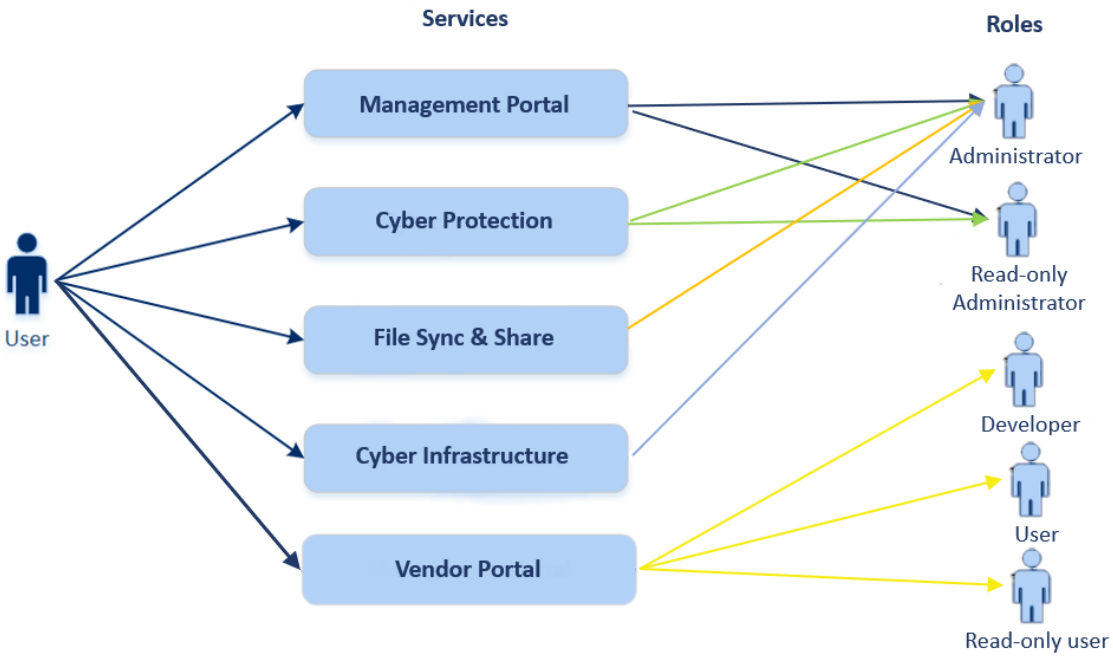
사용자 계정을 서비스 계정 유형으로 변환하려면

1. 관리 포털에서 **회사 관리** > **사용자**로 이동합니다.
2. 계정을 서비스 계정 유형으로 변환하려는 사용자를 선택한 다음 말줄임표 아이콘 > **서비스 계정으로 표시**를 클릭합니다.
3. 확인 창에서 2단계 인증 코드를 입력하고 작업을 확인합니다.

이제 2단계 인증을 지원하지 않는 서비스에 계정을 사용할 수 있습니다.

각 서비스에 사용 가능한 사용자 역할

한 명의 사용자는 여러 개의 역할을 가질 수 있지만, 각 서비스에 대해서는 한 개의 역할만 가질 수 있습니다.



각 서비스에 대해 사용자가 할당받을 역할을 정의할 수 있습니다.

서비스	역할	설명
해당 없음	회사 관리자	이 역할은 관리자에게 모든 서비스에 대한 전체 권한을 부여합니다. 이 역할은 기업 허용 목록에 대한 액세스 권한을 부여합니다. 회사에 대해 Cyber Protection 서비스의 재해 복구 애드온이 활성화되어 있으면 이 역할을 통해 재해 복구 기능 액세스 권한이 부여됩니다.

관리 포털	관리자	이 역할은 전체 조직 내에서 관리자가 사용자를 관리할 수 있는 관리 포털에 대한 액세스 권한을 부여합니다.
	읽기 전용 관리자 파트너 수준	이 역할은 파트너의 관리 포털과 이 파트너의 모든 고객의 관리 포털에 있는 모든 객체에 대한 읽기 전용 액세스 권한을 제공합니다. 이러한 사용자는 조직의 다른 사용자의 데이터에 읽기 전용 모드로 액세스할 수 있으며, 보호 계획을 편집할 수 있지만 스크립팅 계획, 모니터링 계획 또는 에이전트 계획에 대한 변경 사항을 저장할 수는 없습니다.
	읽기 전용 관리자 고객 수준	이 역할은 전체 회사의 관리 포털 내 모든 개체에 대한 읽기 전용 권한을 제공합니다. 해당 역할의 사용자는 읽기 전용 모드로 조직 내 다른 사용자의 데이터에 액세스할 수 있습니다.
	읽기 전용 관리자 부서 수준	이 역할은 회사 부서 및 하위 부서의 관리 포털 내 모든 개체에 대한 읽기 전용 액세스를 제공합니다. 해당 역할의 사용자는 읽기 전용 모드로 조직 내 다른 사용자의 데이터에 액세스할 수 있습니다.
공급 업체 포털	개발자	이 역할은 공급 업체 포털에 대한 전체 권한을 제공합니다. 개발자는 CyberApp, CyberApp 설명 및 CyberApp 버전을 생성하고 관리할 수 있습니다. 또한 디플로이먼트 요청을 제출하고 CyberApp 지표도 모니터링할 수 있습니다.
	사용자	이 역할이 할당된 사용자는 CyberApp 설명을 생성 및 관리하고 승인을 요청할 수 있습니다.
	읽기 전용 사용자	이 역할에서는 공급 업체 포털에 대한 읽기 전용 권한이 제공됩니다.
Cyber Protection	Cyber 관리자	관리자 역할 권한 외에도 이 역할은 Cyber Protection 서비스를 구성 및 관리하고 Cyber Scripting에서 작업을 승인할 수 있습니다. Cyber 관리자 역할은 Advanced Management 팩이 활성화되어 있는 테넌트에만 사용할 수 있습니다.
	관리자	이 역할은 귀하의 고객에 대한 Cyber Protection을 구성하고 관리할 수 있습니다. 이 역할은 재해 복구 기능 및 기업 허용 목록을 구성 및 관리하는 데 필요합니다.
	읽기 전용 관리자	이 역할은 Cyber Protection 서비스의 모든 개체에 대한 읽기 전용 액세스를 제공합니다. 해당 역할의 사용자는 읽기 전용 모드로 조직 내 다른 사용자의 데이터에 액세스할 수 있습니다. 읽기 전용 관리자는 재해 복구 기능 또는 기업 허용 목록을 구성 및 관리할 수 없습니다.
	사용자	이 역할은 관리자 권한 없이 보호 서비스 사용을 가능하게 합니다. 엔드포인트 탐지 및 대응 등의 기능 액세스 권한은 제공되지만 이 역할이 할당된 사용자는 조직 내 다른 사용자의 데이터에는 액세스할 수 없습니다.

	복원 연산자	이 역할을 사용하면 민감한 컨텐츠 액세스는 제한하면서 Microsoft 365 및 Google Workspace 조직 백업 액세스 및 백업 복구를 허용할 수 있습니다.
File Sync & Share	관리자	이 역할은 사용자에 대해 File Sync & Share를 구성하고 관리할 수 있습니다.
Cyber Infrastructure	관리자	이 역할은 사용자에 대해 Cyber Infrastructure를 구성하고 관리할 수 있습니다.
파트너 포털	파트너 포털 사용자에게 할당할 수 있는 여러 역할이 있습니다. 자세한 정보는 "파트너 포털 역할"(117페이지)을(를) 참조하십시오.	

참고
2023년 10월 4일 이후 Acronis Technology Ecosystem 웹 사이트에 등록한 기술 파트너만 공급 업체 포털을 사용할 수 있습니다.
Acronis와의 협력을 추진 중이며 공급 업체 포털과 전용 샌드박스에 액세스해야 하는 공급 업체는 관련 지침을 따르십시오.

읽기 전용 관리자 역할

이 역할이 있는 계정은 Cyber Protect 콘솔에 읽기 전용으로 액세스하고 다음을 수행할 수 있습니다.

- 진단 데이터(예: 시스템 보고서)를 수집할 수 있습니다.
- 백업의 복구 지점을 볼 수 있지만, 백업 내용을 자세히 살펴보고 파일, 폴더 또는 이메일을 확인할 수는 없습니다.

읽기 전용 관리자는 다음을 수행할 수 없습니다.

- 작업을 시작하거나 중지할 수 없습니다.
  예를 들어 읽기 전용 관리자는 복구를 시작하거나 실행 중인 백업을 중지할 수 없습니다.
- 소스 또는 대상 머신에서 파일 시스템에 액세스할 수 있습니다.
  예를 들어 읽기 전용 관리자는 백업된 머신에서 파일, 폴더 또는 이메일을 확인할 수 없습니다.
- 설정을 변경할 수 없습니다.
  예를 들어 읽기 전용 관리자는 보호 계획을 생성하거나 해당 설정을 변경할 수 없습니다.
- 데이터를 생성하거나, 업데이트하거나, 삭제할 수 없습니다.
  예를 들어 읽기 전용 관리자는 백업을 삭제할 수 없습니다.

읽기 전용 관리자가 액세스할 수 없는 모든 UI 개체는 숨겨져 있지만 보호 계획의 기본 설정은 예외입니다. 이러한 설정은 표시되지만 **저장** 버튼이 활성화되지 않습니다.

계정 및 역할과 관련한 모든 변경 사항은 **작업** 탭에 다음 상세 정보와 함께 표시됩니다.

- 변경된 사항
- 변경을 수행한 사용자
- 변경 날짜 및 시간

복원 연산자 역할

이 역할은 Cyber Protection 서비스에서만 사용 가능하며 Microsoft 365 및 Google Workspace 백업만 복원할 수 있습니다.

복원 연산자가 수행할 수 있는 작업은 다음과 같습니다.

- 경보 및 활동 보기.
- 백업 목록 찾아보기 및 새로 고침.
- 컨텐츠에 액세스하지 않고 백업 찾아보기. 복원 연산자는 백업된 파일의 이름과 백업된 이메일의 제목 및 보낸 사람을 확인할 수 있습니다.
- 백업 검색(전체 텍스트 검색은 지원되지 않음).
- 클라우드 간 백업을 원래 Microsoft 365 또는 Google Workspace 조직 내의 원래 위치에 복구.

복원 연산자가 수행할 수 없는 작업은 다음과 같습니다.

- 경보 삭제.
- Microsoft 365 또는 Google Workspace 조직 추가 또는 삭제.
- 백업 위치 추가, 삭제 또는 이름 변경.
- 백업 삭제 또는 이름 변경.
- 백업을 사용자 정의 위치에 복구할 때 폴더 생성, 삭제 또는 이름 변경.
- 백업 계획 적용 또는 백업 실행.
- 백업된 파일 또는 백업된 이메일의 내용 액세스.
- 백업된 파일 또는 이메일 첨부 파일 다운로드.
- 이메일 또는 달력 항목과 같은 백업된 클라우드 리소스를 이메일로 전송.
- Microsoft 365 Teams 대화 확인 또는 복구.
- 클라우드 간 백업을 원래 위치가 아닌 위치(예: 다른 사서함, OneDrive, Google Drive 또는 Microsoft 365 팀)에 복구.

사용자 역할 및 Cyber Scripting 권한

스크립트 및 스크립팅 계획에 사용할 수 있는 작업은 스크립트 상태 및 사용자의 사용자 역할에 따라 달라집니다.

관리자는 자신의 테넌트 및 하위 테넌트에서 객체를 관리할 수 있습니다. 상위 관리 수준의 객체는 보거나 액세스할 수 없습니다.

하위 관리자는 상위 관리자가 워크로드에 적용한 스크립팅 계획에 대한 읽기 전용 권한만 갖습니다.

다음 역할은 Cyber Scripting과 관련된 권한을 제공합니다.

- **회사 관리자**
  이 역할은 모든 서비스에 대한 모든 관리자 권한을 부여합니다. Cyber Scripting과 관련해서는 Cyber 관리자 역할과 동일한 권한을 부여합니다.

- **Cyber 관리자**
  이 역할은 테넌트에서 사용할 수 있는 스크립트의 승인과 **테스트 중** 상태의 스크립트를 실행할 수 있는 권한을 포함하여 전체 권한을 부여합니다.
- **관리자**
  이 역할은 승인된 스크립트를 실행할 수 있는 권한과 승인된 스크립트를 사용하는 스크립팅 계획을 생성 및 실행할 수 있는 권한과 함께 부분 권한을 부여합니다.
- **읽기 전용 관리자**
  이 역할은 테넌트에서 사용되는 스크립트 및 보호 계획을 볼 수 있는 권한과 함께 제한된 권한을 부여합니다.
- **사용자**
  이 역할은 승인된 스크립트를 실행할 수 있는 권한과 승인된 스크립트를 사용하는 스크립팅 계획을 생성 및 실행할 수 있는 권한과 함께 부분 권한을 부여합니다. 단, 생성 및 실행할 수 있는 위치는 사용자의 머신으로 제한됩니다.

다음 표에는 사용 가능한 모든 작업(스크립트 상태 및 사용자 역할에 따라 달라짐)이 요약되어 있습니다.

역할	객체	스크립트 상태		
		초안	테스트 중	승인됨
Cyber 관리자 **회사 관리자**	스크립팅 계획	편집(계획에서 초안 스크립트 제거) 삭제 철회 비활성화 중지	생성 편집 적용 활성화 실행 삭제 철회 비활성화 중지	생성 편집 적용 활성화 실행 삭제 철회 비활성화 중지
	스크립트	생성 편집 상태 변경 복제 삭제 실행 취소	생성 편집 상태 변경 실행 복제 삭제 실행 취소	생성 편집 상태 변경 실행 복제 삭제 실행 취소

관리자 **사용자**(자신의 워크로드인 경우)	스크립팅 계획	보기 철회 비활성화 중지	보기 실행 취소	생성 편집 적용 활성화 실행 삭제 철회 비활성화 중지
	스크립트	생성 편집 복제 삭제 실행 취소	보기 복제 실행 취소	실행 복제 실행 취소
읽기 전용 관리자	스크립팅 계획	보기	보기	보기
	스크립트	보기	보기	보기

사용자를 위한 알림 설정 변경

사용자를 위한 알림 설정을 변경하려면 **회사 관리** > **사용자**로 이동합니다. 알림을 구성할 사용자를 선택한 다음 **설정** 섹션의 연필 아이콘을 클릭합니다. 사용자가 생성된 테넌트에 대해 Cyber Protection 서비스가 활성화되어 있으면 다음 알림 설정을 사용할 수 있습니다.

- **할당량 초과 사용 알림** (기본적으로 활성화됨)
  초과된 할당량에 대한 알림.
- **예약된 사용 보고서**(기본적으로 활성화됨)
  매월 1일에 전송되는 사용 보고서.
- **URL 브랜딩 알림**(기본적으로 비활성화됨)
  Cyber Protect Cloud 서비스의 사용자 지정 URL에 사용되는 인증서 만료 예정 관련 알림입니다. 인증서 만료 30일, 15일, 7일, 3일, 1일 전에 선택한 테넌트의 모든 관리자에게 알림이 전송됩니다.
- **실패 알림**, **경고 알림...** 및 **성공 알림** (기본적으로 비활성화됨)
  보호 계획의 실행 결과와 각 장치별 재해 복구 작업 결과에 대한 알림.
- **활성 경보에 대한 일일 확인**(기본적으로 활성화됨)
  일일 요약은 생성 당시 Cyber Protect 콘솔에 있는 활성 경보 목록을 기반으로 합니다. 이 요약은 하루에 한 번 10:00~23:59 UTC 사이에 생성되고 전송됩니다. 보고서가 생성되고 전송되는 시간

은 데이터 센터의 워크로드에 따라 다릅니다. 그 당시 활성 경보가 없다면 요약이 전송되지 않습니다. 요약은 더 이상 활성 상태가 아닌 이전 경보에 대한 정보를 포함하지 않습니다. 예를 들어, 사용자가 실패한 백업을 발견하고 경보를 해제하거나 요약이 생성되기 전에 백업을 다시 시도해 성공할 경우, 경보는 더 이상 존재하지 않게 되며 요약에 포함되지 않습니다.

- **장치 제어 알림**(기본적으로 비활성화됨)
  장치 제어 모듈이 활성화된 보호 계획을 통해 제한되는 주변 장치와 포트 사용 시도 관련 알림.
- **복구 알림**(기본적으로 비활성화됨)
  다음 리소스에 대한 복구 작업 관련 알림: 사용자 이메일 메시지와 전체 사서함, 공용 폴더, OneDrive/GoogleDrive: 전체 OneDrive 및 파일이나 폴더, Sharepoint 파일, Teams: 채널, 전체 Teams, 이메일 메시지 및 팀 사이트.
  이러한 알림과 관련하여 복구 작업으로 간주되는 작업은 이메일로 보내기, 다운로드, 복구 작업 시작 등이 있습니다.
- **데이터 손실 방지 알림**(기본적으로 비활성화됨)
  네트워크에서 이 사용자의 활동과 관련된 데이터 손실 방지 경고에 대한 알림입니다.
- **보안 인시던트 알림**(기본적으로 비활성화됨)
  온액세스, 온엑시큐션 및 온디맨드 스캔 중에 감지된 맬웨어와 동작 엔진 및 URL 필터링 엔진의 감지에 대한 알림입니다.
  사용 가능한 두 가지 옵션은 **완화됨** 및 **완화되지 않음**입니다. EDR(엔드포인트 탐지 및 대응) 인시던트 경보, 위협 피드의 EDR 경보, 그리고 개별 경보(EDR이 활성화되지 않은 워크로드에 대한 경보)에 이러한 옵션을 사용할 수 있습니다.
  EDR 경보가 생성되면 관련 사용자에게 이메일이 전송됩니다. 인시던트의 위협 상태가 변경되면 새 이메일이 전송됩니다. 사용자는 이메일에 포함된 작업 버튼을 사용해 인시던트 상세 정보를 확인(완화된 인시던트의 경우)하거나 인시던트를 조사 및 수정(완화되지 않은 인시던트의 경우)할 수 있습니다.
- **인프라 알림**(기본적으로 비활성화됨)
  재해 복구 인프라 문제와 관련된 알림: 재해 복구 인프라를 사용할 수 없거나 VPN 터널을 사용할 수 없는 경우.

모든 알림은 사용자의 이메일 주소로 전송됩니다.

사용자 역할별로 수신하는 알림

Cyber Protection에서 보내는 알림은 사용자 역할에 따라 다릅니다.

알림 유형\사용자 역할	사용자	고객 및 단위 관리자	파트너 및 폴더 관리자
사용자 장치에 대한 알림	예	예	해당 없음*
자식 테넌트의 모든 장치에 대한 알림	해당 없음	예(**보안 인시던트 알림** 제외)	예
Microsoft 365, Google Workspace 및 기타 클라우드 기반 백업에 대한 알림	해당 없음	예	예

*파트너 관리자는 장치를 직접 등록할 수 없지만, 자체 고객 관리자 계정을 생성하고 그 계정을 사용해 장치를 추가할 수 있습니다. 사용자 계정 및 테넌트를 참고하십시오.

사용자 계정 비활성화 및 활성화

클라우드 플랫폼에 대한 액세스를 일시적으로 제한하려면 사용자 계정을 비활성화해야 할 수 있습니다.

사용자 계정을 비활성화하려면

1. 관리 포털에서 **사용자**로 이동합니다.
2. 비활성화할 사용자 계정을 선택한 다음, 말줄임표 아이콘 > **비활성화**를 클릭합니다.
3. **비활성화**를 클릭하여 작업을 확인합니다.

이렇게 하면 이 사용자는 클라우드 플랫폼을 사용하거나 다른 알림을 받을 수 없게 됩니다.

비활성화된 사용자 계정을 활성화하려면 사용자 목록에서 이를 선택한 다음, 말줄임표 아이콘 > **활성화**를 클릭합니다.

사용자 계정 삭제

사용자 계정이 사용하는 리소스(예: 스토리지 공간 또는 라이센스)의 공간을 확보하려면 사용자 계정을 영구적으로 삭제해야 할 수 있습니다. 사용 통계는 삭제 후 1일 이내로 업데이트됩니다. 데이터가 많은 계정의 경우 더 많은 시간이 소요될 수 있습니다.

사용자 계정을 삭제하기 전에 비활성화해야 합니다. 작업의 수행 방법에 대한 자세한 내용은 사용자 계정 비활성화 및 활성화를 참조하십시오.

사용자 계정을 삭제하려면

1. 관리 포털에서 **사용자**로 이동합니다.
2. 비활성화된 사용자 계정을 선택한 다음, 말줄임표 아이콘 > **삭제**를 클릭합니다.
3. 작업을 확인하려면 로그인한 다음 **삭제**를 클릭합니다.

결과:

- 이 계정에 구성되어 있는 모든 알림이 비활성화됩니다.
- 이 사용자 계정에 속한 모든 데이터가 삭제됩니다.
- 관리자가 관리 포털에 액세스할 수 없게 됩니다.
- 이 사용자와 연결된 워크로드의 모든 백업이 삭제됩니다.
- 이 사용자 계정과 연결된 모든 머신의 등록이 해제됩니다.
- 이 사용자와 연결된 모든 워크로드에서 모든 보호 계획이 해지됩니다.
- 이 사용자가 소유한 모든 File Sync & Share 데이터(예: 파일 및 폴더)가 삭제됩니다.
- 이 사용자가 소유한 공증 데이터(예: 공증된 파일, 전자 서명한 파일)가 삭제됩니다.

- 사용자 **상태**가 **삭제됨**으로 표시됩니다. **삭제됨** 상태를 마우스로 가리키면 사용자가 삭제된 날짜, 그리고 이 삭제 날짜로부터 30일 내에 모든 관련 사용자 데이터와 설정을 복구할 수 있다는 참고 사항이 표시됩니다.

사용자 계정 복구

사용자 계정을 실제로 삭제하는 경우에 대비하여 Cyber Protection에서는 사용자 계정 복구 기능을 제공합니다.

예를 들어 회사 관리자가 퇴사한 사용자를 삭제했는데 해당 사용자에게 등록되어 있는 모든 리소스는 계속 필요한 경우 사용자 계정을 복구해야 할 수 있습니다.

사용자 계정 복구 방법

1. 관리 포털에서 **회사 관리** > **사용자**로 이동합니다.
2. **사용자** 탭에서 복구할 사용자 계정을 찾습니다. 사용자 계정의 상태는 **삭제됨**으로 표시됩니다.
3. 사용자 계정을 마우스로 가리키고 말줄임표 아이콘 을 클릭합니다.
4. **복구**를 클릭합니다.
   사용자 계정이 삭제되기 전과 같은 상태로 복구되며 기본적으로 비활성화된다는 메시지가 포함된 확인 창이 나타납니다.
5. [선택 사항] 사용자 계정을 활성화해야 하는 경우 **사용자를 활성화합니다** 확인란을 선택합니다. 사용자 계정은 나중에 언제든지 활성화할 수 있습니다.
6. **복구**를 클릭합니다.

결과:

- 이 사용자 계정이 복구됩니다.
- 이 사용자 계정에 속한 모든 데이터가 복구됩니다.
- 이 사용자 계정과 연결된 모든 머신이 다시 등록됩니다.
- 사용자 상태는 사용자 계정을 활성화한 경우에는 **활성**으로 표시되고 아직 활성화하지 않은 경우에는 **비활성화됨**으로 표시됩니다.

사용자 계정의 소유권 이전

제한된 사용자 데이터에 대한 액세스를 유지하려면 사용자 계정의 소유권을 이전해야 할 수 있습니다.

중요
삭제된 계정의 콘텐츠는 재할당할 수 없습니다.

사용자 계정의 소유권을 이전하려면:

1. 관리 포털에서 **사용자**로 이동합니다.
2. 소유권을 이전할 사용자 계정을 선택한 다음 **일반 정보** 섹션의 연필 아이콘을 클릭합니다.
3. 기존 이메일을 향후 계정 소유자의 이메일로 대체한 다음 **완료**를 클릭합니다.

4. **예**를 클리하여 작업을 확인합니다.
5. 향후 계정 소유자가 전송된 지침을 따라 이메일 주소를 인증하도록 하십시오.
6. 소유권을 이전할 사용자 계정을 선택한 다음, 말줄임표 아이콘 > **비밀번호 재설정**을 클릭합니다.
7. **재설정**을 클릭하여 작업을 확인합니다.
8. 향후 계정 소유자가 이메일 주소로 전송된 지침을 따라 비밀번호를 재설정하도록 하십시오.

이제 새로운 소유자가 이 계정에 액세스할 수 있습니다.

2단계 인증 설정

2FA(2단계 인증)는 다단계 인증의 일종으로, 사용자의 신원을 다음과 같은 요소 중 두 가지를 사용하여 확인합니다.

- 사용자가 알고 있는 것(PIN 또는 비밀번호)
- 사용자가 소유하고 있는 것(토큰)
- 사용자인 것(생체 인식)

2단계 인증은 사용자의 계정을 무단 액세스로부터 더 강력하게 보호할 수 있습니다.

플랫폼은 **TOTP(시간 기반 일회성 비밀번호)** 인증을 지원합니다. TOTP 인증이 시스템에서 활성화되어 있다면 사용자는 기존 비밀번호와 일회성 TOTP 코드를 모두 입력해야 시스템에 액세스할 수 있습니다. 즉, 사용자는 비밀번호(첫 번째 요소)와 TOTP 코드(두 번째 요소)를 제공하는 것입니다. TOTP 코드는 사용자의 두 번째 요소 생성 장치의 인증 애플리케이션에서 생성되며, 플랫폼에서 제공한 암호(QR 코드 또는 영숫자 코드)와 현재 시간을 기반으로 합니다.

작동법

1. 조직 수준에서 2단계 인증을 활성화합니다.
2. 모든 조직 사용자는 두 번째 요소 생성 장치(휴대전화, 노트북, 데스크톱, 태블릿 등)에 인증 애플리케이션을 설치해야 합니다. 이 애플리케이션으로 일회성 TOTP 코드를 생성합니다. 권장되는 인증 앱은 다음과 같습니다.
   - Google Authenticator
     iOS 앱 버전(https://apps.apple.com/app/google-authenticator/id388497605)
     Android 버전
     (https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2)
   - Microsoft Authenticator
     iOS 앱 버전(https://apps.apple.com/app/microsoft-authenticator/id983156458)
     Android 버전(https://play.google.com/store/apps/details?id=com.azure.authenticator)

중요
사용자는 인증 애플리케이션을 설치한 장치의 시간이 올바르며 현재 시간과 일치함을 확인해야 합니다.

3. 조직 사용자들은 시스템에 다시 로그인해야 합니다.
4. 로그인 및 비밀번호를 입력하고 나면 사용자 계정에 대한 2단계 인증을 설정하라는 메시지가 표시됩니다.
5. 반드시 인증 애플리케이션으로 QR 코드를 스캔해야 합니다. QR 코드를 스캔할 수 없는 경우, QR 코드 밑에 표시된 32자리 코드를 사용하여 수동으로 인증 애플리케이션에 추가할 수 있습니다.

중요
인증 수단을 꼭 저장해 두는 것이 좋습니다(QR 코드 인쇄, TOTP(임시 일회성 비밀번호) 암호 메모, 코드의 클라우드 백업을 지원하는 애플리케이션 사용 등). TOTP(임시 일회성 암호)는 두 번째 요소 생성 장치를 분실했을 경우 2단계 인증을 재설정할 때 필요합니다.

6. TOTP(임시 일회성 암호) 코드는 인증 애플리케이션에서 생성되며, 30초마다 자동으로 재생성됩니다.
7. 사용자는 암호를 입력한 후에 표시되는 **2단계 인증 설정** 창에 TOTP 코드를 입력해야 합니다.
8. 그러면 사용자에 대한 2단계 인증이 설정됩니다.

이제 사용자가 시스템에 로그인할 때 로그인 및 비밀번호와 함께 인증 애플리케이션에서 생성된 일회성 TOTP 코드를 입력해야 합니다. 시스템에 로그인할 때 해당 브라우저를 신뢰할 수 있는 브라우저로 지정해 두면 그 다음부터 같은 브라우저로 로그인할 때에는 TOTP 코드를 입력할 필요가 없습니다.

새 장치에서 2단계 인증을 복원하려면

이전에 설정한 모바일 인증 앱에 액세스할 수 있는 경우:

1. 새 장치에 인증 프로그램 앱을 설치합니다.
2. 장치에서 2FA를 설정할 때 저장했던 PDF 파일을 사용합니다. 이 파일에는 Acronis 계정에 인증 프로그램 앱을 다시 연결하려면 인증 프로그램 앱에서 입력해야 하는 32자리 코드가 포함되어 있습니다.

중요
코드가 올바른데 앱이 작동하지 않으면 인증 프로그램 모바일 앱에서 시간을 동기화하십시오.

3. 설정 시에 PDF 파일을 저장하지 않은 경우:

a. ***2FA(2단계 인증) 재설정****을 입력하고 이전에 설정했던 모바일 인증 프로그램 앱에 표시된 일회성 암호를 입력합니다.*
b. 화면에 나타나는 지침을 따릅니다.

이전에 설정한 모바일 인증 프로그램 앱에 액세스할 수 없는 경우:

1. 새 모바일 장치를 가져옵니다.
2. 저장해 둔 PDF 파일을 사용하여 새 장치를 연결합니다. 이 파일의 기본 이름은 `cyberprotect-2fa-backupcode.pdf`입니다.
3. 백업에서 계정 액세스를 복원합니다. 모바일 앱에서 백업이 지원되는지 확인합니다.
4. 앱이 지원하는 경우 다른 모바일 장치에서 동일 계정으로 앱을 엽니다.

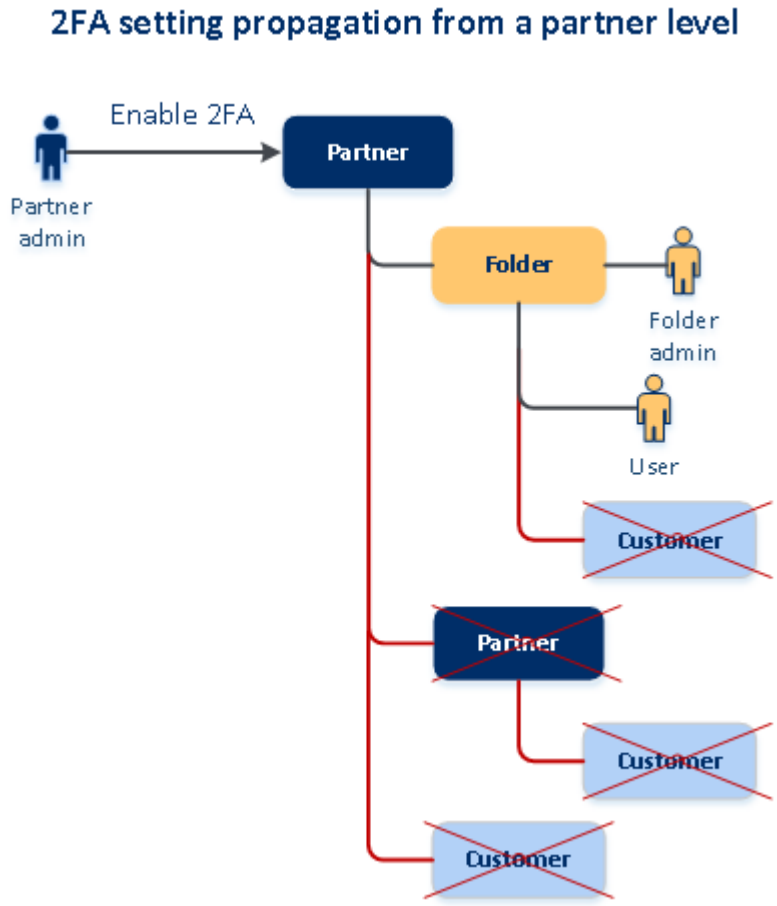
테넌트 수준으로 2단계 인증 설정 전파

2단계 인증은 **조직** 수준에서 설정되며, 다음과 같이 2단계 인증을 활성화 또는 비활성할 수 있습니다.

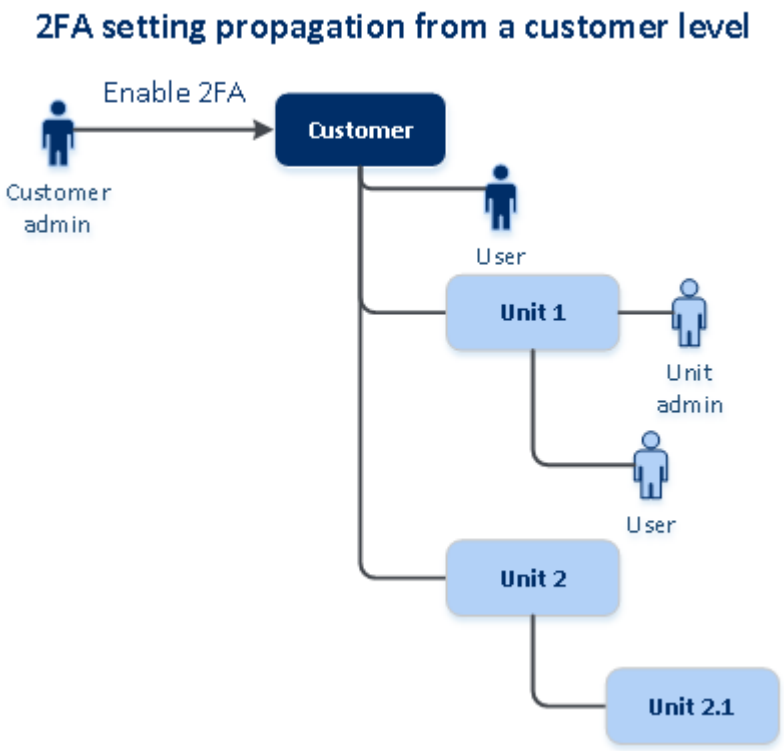
- 소유한 조직에 대해.
- 하위 테넌트에 대해(해당 하위 테넌트 내에서 **지원 액세스** 옵션이 활성화되어 있는 경우에만 가능).

2단계 인증 관련 설정은 다음과 같이 테넌트 수준으로 전파됩니다.

- 각 폴더는 파트너 조직의 2단계 인증 설정을 자동으로 상속합니다. 아래의 구성표에서 빨간 줄은 2단계 인증 설정의 전파가 불가능하다는 의미입니다.



- 각 부서는 고객 조직의 2단계 인증 설정을 자동으로 상속합니다.



참고

1. 하위 조직에 대한 2단계 인증은 해당 하위 조직 내에서 **지원 액세스** 옵션이 활성화되어 있는 경우에만 활성화 또는 비활성화할 수 있습니다.
2. 하위 조직의 사용자에 대한 2단계 인증 설정은 해당 하위 조직 내에서 **지원 액세스** 옵션이 활성화되어 있는 경우에만 관리할 수 있습니다.
3. 부서 또는 폴더 수준에서는 2단계 인증을 설정할 수 없습니다.
4. 부모 조직이 이 설정을 활성화하지 않았더라도 2단계 인증을 설정할 수 있습니다.

테넌트에 대한 2단계 인증 설정

관리자는 조직에서 2단계 인증을 활성화할 수 있습니다.

테넌트에 대한 2단계 인증을 활성화하려면

1. 관리 포털에서 **설정** > **보안**으로 이동합니다.
2. **2단계 인증** 토글을 옆으로 밀고 **활성화**를 클릭합니다.

이제 조직의 모든 사용자가 자신의 계정에 2단계 인증을 설정해야 하며, 사용자가 다음번에 로그인하거나 현재 세션이 만료되면 2단계 인증을 설정하라는 메시지가 표시됩니다.

계정에 2단계 인증을 설정한 사용자 수가 토글 아래의 진행률 표시줄에 나타납니다. 계정을 구성한 사용자를 확인하려면 **회사 관리** > **사용자** 탭으로 이동하여 **2FA 상태** 열을 확인합니다. 계정에 2단계 인증을 아직 구성하지 않은 사용자의 2FA 상태는 **설정 필요**입니다.

2단계 인증을 정상적으로 구성한 사용자는 서비스 콘솔에 로그인할 때마다 로그인, 비밀번호 및 TOTP 코드를 입력해야 합니다.

테넌트에 대한 2단계 인증을 비활성화하려면

1. 관리 포털에서 **설정** > **보안**으로 이동합니다.
2. 2단계 인증을 비활성화하려면 토글을 끄고 **비활성화**를 클릭합니다.
3. [한 명 이상의 사용자가 조직 내에서 2단계 인증을 구성한 경우] 모바일 장치의 인증 애플리케이션에서 생성된 TOTP 코드를 입력합니다.

그러면 조직에 대한 2단계 인증이 비활성화되고, 모든 암호가 삭제되고, 신뢰할 수 있는 브라우저가 모두 지워집니다. 모든 사용자가 로그인과 비밀번호만으로 시스템에 로그인합니다. **회사 관리** > **사용자** 탭에서 **2FA 상태** 열이 숨김 처리됩니다.

사용자의 2단계 인증 관리

관리 포털의 **회사 관리** > **사용자** 탭에서 모든 사용자의 2단계 인증 설정을 모니터링하고 재설정할 수 있습니다.

모니터링

관리 포털의 **회사 관리** > **사용자**에서 조직의 모든 사용자 목록을 볼 수 있습니다. **2FA 상태**는 사용자의 2단계 인증 구성이 설정되어 있는지 여부를 나타냅니다.

사용자에 대한 2단계 인증을 재설정하려면

1. 관리 포털에서 **회사 관리** > **사용자**로 이동합니다.
2. **사용자** 탭에서 설정을 변경할 사용자를 찾은 다음 말줄임표 아이콘을 클릭합니다.
3. **2단계 인증 재설정**을 클릭합니다.
4. 두 번째 요소 생성 장치의 인증 애플리케이션에서 생성된 TOTP 코드를 입력한 후 **재설정**을 클릭합니다.

그러면 사용자가 2단계 인증을 다시 설정할 수 있습니다.

사용자의 신뢰할 수 있는 브라우저를 재설정하려면

1. 관리 포털에서 **회사 관리** > **사용자**로 이동합니다.
2. **사용자** 탭에서 설정을 변경할 사용자를 찾은 다음 말줄임표 아이콘을 클릭합니다.
3. **신뢰할 수 있는 브라우저 모두 재설정**을 클릭합니다.
4. 두 번째 요소 생성 장치의 인증 애플리케이션에서 생성된 TOTP 코드를 입력한 후 **재설정**을 클릭합니다.

신뢰할 수 있는 브라우저를 모두 재설정한 사용자는 다음 로그인 시 TOTP 코드를 입력해야 합니다.

사용자는 스스로 모든 신뢰할 수 있는 브라우저와 2단계 인증 설정을 재설정할 수 있습니다. 시스템에 로그인할 때 해당 링크를 클릭하고 TOTP 코드를 입력해 작업을 확인하여 이를 수행할 수 있습니다.

사용자에 대한 2단계 인증을 비활성화하려면

2단계 인증을 비활성화하면 테넌트 보안을 위반하게 될 수도 있으므로 이렇게 하지 않는 것이 좋습니다.

이에 대한 예외로, 특정 사용자에 대해서는 2단계 인증을 비활성화하고 테넌트의 다른 모든 사용자에 대해 2단계 인증을 유지할 수도 있습니다. 이는 클라우드 통합이 구성된 테넌트 내에서 2단계 인증이 활성화된 경우에 대한 해결책입니다. 이러한 통합에서는 사용자 계정(로그인 비밀번호)을 통해 플랫폼에 권한을 부여합니다. 통합을 계속 사용하려면 2단계 인증을 적용할 수 없는 서비스 계정으로 사용자를 변환하면 되지만 이는 일시적인 솔루션입니다.

중요
일반 사용자를 서비스 사용자로 전환하여 2단계 인증을 비활성화하면 테넌트 보안이 위험해지므로 이렇게 하지 않는 것이 좋습니다.

테넌트에 대해 2단계 인증을 비활성화하지 않고 클라우드 통합을 사용하기 위해 권장되는 보안 솔루션은 API 클라이언트를 만들고 클라우드 통합이 이러한 클라이언트와 연동되도록 구성하는 것입니다.

1. 관리 포털에서 **회사 관리** > **사용자**로 이동합니다.
2. **사용자** 탭에서 설정을 변경할 사용자를 찾은 다음 말줄임표 아이콘을 클릭합니다.
3. **서비스 계정으로 표시**를 클릭합니다. 그러면 해당 사용자는 **서비스 계정**이라는 특별 2단계 인증 상태로 지정됩니다.
4. [테넌트 내 최소 한 명의 사용자가 2단계 인증을 구성한 경우] 두 번째 요소 생성 장치의 인증 애플리케이션에서 생성된 TOTP 코드를 입력하여 비활성화를 확인합니다.

사용자에 대한 2단계 인증을 활성화하려면

이전에 2단계 인증을 비활성화한 사용자의 인증을 다시 활성화해야 하는 경우가 발생할 수 있습니다.

1. 관리 포털에서 **회사 관리** > **사용자**로 이동합니다.
2. **사용자** 탭에서 설정을 변경할 사용자를 찾은 다음 말줄임표 아이콘을 클릭합니다.
3. **표준 계정으로 표시**를 클릭합니다. 그러면 그 사용자는 이제 시스템 로그인 시 2단계 인증을 설정하거나 TOTP 코드를 입력해야 합니다.

두 번째 요소 생성 장치를 분실한 경우 2단계 인증 재설정

두 번째 요소 생성 장치를 분실하여 계정 액세스를 재설정해야 하는 경우, 다음 방법 중 한 가지를 따르십시오.

- 백업에서 TOTP 암호(QR 코드 또는 영숫자 코드)를 복원합니다.
  다른 두 번째 요소 생성 장치를 사용하여, 저장해 두었던 TOTP 암호를 이 장치에 설치되어 있는 인증 애플리케이션에 추가합니다.
- 관리자에게 2단계 인증 설정의 재설정을 요청합니다.

무차별 대입 보호

무차별 대입 공격은 침입자가 수많은 비밀번호를 시도해 그 중 하나가 맞기를 바라며 공격하는 방식입니다.

플랫폼의 무차별 대입 보호 메커니즘은 장치 쿠키를 기반으로 합니다.

플랫폼에서 사용되는 무차별 대입 보호의 사전 정의된 설정은 다음과 같습니다.

매개변수	비밀번호 입력	TOTP 코드 입력
시도 제한	10	5
시도 제한 기간(시간 초과 후 제한이 재설정됨)	15분(900초)	15분(900초)
다음의 경우 잠금 설정	시도 제한 + 1(11번째 시도)	시도 제한
잠금 기간	5분(300초)	5분(300초)

2단계 인증을 활성화하면 두 요소(비밀번호와 TOTP 코드)를 사용한 인증이 모두 성공한 경우에만 장치 쿠키가 클라이언트(브라우저)에 발급됩니다.

신뢰할 수 있는 브라우저의 경우 하나의 요소(비밀번호)만 사용해서 인증하면 장치 쿠키가 발급됩니다.

TOTP 코드 입력 시도 횟수는 장치당이 아니라 사용자당으로 등록됩니다. 따라서 사용자가 다른 장치를 사용해 TOTP 코드 입력을 시도해도 여전히 차단됩니다.

고객에 대한 업셀 시나리오 구성

업셀은 고객에게 추가 기능 구매 기회를 제공하는 기술입니다.

Cyber Protection에는 여러 레거시 버전이 있으며 모두 기능과 가격이 다릅니다. 현재 기본 버전을 사용 중인 기존 고객에게 보다 고급 기능을 갖추고 있으며 가격이 높은 버전을 홍보할 수 있습니다.

고객별로 업셀 기능을 활성화하거나 비활성화할 수 있습니다. 기본적으로 업셀 옵션은 비활성화되어 있습니다. 고객에 대한 업셀을 활성화하는 경우, 해당 고객은 홍보 버전을 구매할 때까지 제공되지 않는 추가 기능을 확인할 수 있습니다. 이러한 추가 기능에는 홍보 버전의 이름 또는 아이콘으로 된 레이블이 붙고, 주황색으로 강조 표시됩니다. 고객에게도 이러한 업셀 포인트가 표시되어 더욱 가격이 높은 버전을 구매하도록 유도할 수 있습니다. 고객이 업셀 포인트를 클릭하면 더 높은 가격의 버전을 구매해 원하는 기능을 활성화하도록 제안하는 대화 상자가 표시됩니다.

작업 항목은 고객 사용자의 유형에 따라 달라집니다. 사용자 유형(구매자 또는 비구매자)은 플랫폼 API를 사용해 구성할 수 있습니다. 자세한 내용은 API 문서를 참조하십시오. 작업 항목과 고객에게 표시되는 내용에 대한 자세한 정보는 아래 표를 참조하십시오.

고객 테넌트의 사용자 유형	작업 항목

관리자, 구매자	사용자 인터페이스에 **지금 구매** 버튼이 표시됩니다.*
관리자, 비구매자	사용자 인터페이스에 "버전을 업그레이드하려면 파트너사에 문의하십시오."라는 메시지가 표시됩니다.
사용자, 구매자	사용자 인터페이스에 "버전을 업그레이드하려면 파트너사에 문의하십시오."라는 메시지가 표시됩니다.
사용자, 비구매자	사용자 인터페이스에 "버전을 업그레이드하려면 파트너사에 문의하십시오."라는 메시지가 표시됩니다.

* **지금 구매** 버튼에 대한 링크는 고객이 고급 버전을 구매할 수 있는 웹 사이트로 연결됩니다. 이는 **설정** > **브랜딩**에서 구성할 수 있습니다. **업셀** 섹션에서 **구입 URL**을 지정할 수 있습니다. 브랜딩 설정은 브랜딩이 구성된 모든 직접 및 간접 자식 파트너/폴더와 테넌트 고객에게 적용됩니다.

고객에 대한 업셀 기능 활성화 또는 비활성화

1. 관리 포털에서 **클라이언트**로 이동합니다.
2. 고객을 선택하고 오른쪽 창으로 이동해 **구성** 탭을 클릭합니다.
3. **업셀** 섹션에서 다음을 수행합니다.
   - **더 많은 고급 버전 승급**을 활성화해 고객에 대한 업셀 시나리오를 켭니다.
   - **더 많은 고급 버전 승급**을 비활성화해 고객에 대한 업셀 시나리오를 끕니다.

고객에게 업셀 포인트 표시

취약성 목록

취약성 목록은 Cyber Protect 콘솔의 **소프트웨어 관리** > **취약성**에서 찾아볼 수 있습니다. 사용자가 스티치 아이콘을 클릭하면 사용자에게 더 가격이 높은 버전을 구입하라고 제안하는 버전 홍보 대화 상자가 열립니다.

보호 계획 생성 또는 편집

이는 Cyber Protect 콘솔의 **계획** > **보호**에서 찾아볼 수 있습니다. **계획 생성**을 클릭합니다. Cyber Backup 버전은 **백업**과 **취약성** 모듈만 활성화되어 있으며 이외 나머지 모듈은 Cyber Protect 버전에서만 사용 가능합니다. 고객은 Cyber Protect 버전 중 하나를 구입하면 모든 모듈을 활성화할 수 있게 됩니다.

자동 검색 마법사

이 마법사는 Cyber Protect 콘솔의 **장치** > **모든 장치**에서 찾아볼 수 있습니다. 고객은 **추가**를 클릭한 다음 **여러 개의 장치** 섹션에서 **Windows 전용**을 클릭해 자동 검색 마법사를 시작해야 합니다. 자동 머신 검색 방식은 Advanced 버전에서만 사용할 수 있습니다.

장치 목록의 작업

이러한 목록은 Cyber Protect 콘솔의 **장치** > **모든 장치**에서 찾아볼 수 있습니다. 고객이 머신을 선택하면 2개의 추가 옵션이 왼쪽 창에 표시됩니다.

- **HTML5 클라이언트를 통해 연결**
- **패치**

이러한 옵션은 고객이 현재 버전보다 가격이 높은 버전을 구입해야만 사용할 수 있습니다.

위치 및 스토리지 관리

설정 > **위치** 섹션에는 파트너 및 고객에게 **Cyber Protection**와 **File Sync & Share** 서비스를 제공하는 데 사용할 수 있는 클라우드 스토리지와 재해 복구 인프라가 표시됩니다.

다른 서비스에 대해 구성된 스토리지는 향후 릴리스에서 **위치** 섹션에 표시될 예정입니다.

위치

위치는 클라우드 스토리지와 재해 복구 인프라를 편리하게 분류할 수 있는 컨테이너입니다. 위치는 특정 데이터 센터나 인프라 컴퍼넌트의 지리적 위치와 같이 귀하가 선택하는 사항을 나타냅니다.

위치는 숫자와 관계없이 생성할 수 있으며 백업 스토리지, 재해 복구 인프라 및 **File Sync & Share** 스토리지로 채울 수 있습니다. 위치는 여러 클라우드 스토리지를 포함할 수 있지만 재해 복구 인프라는 한 개만 포함할 수 있습니다.

스토리지를 이용한 작업에 대한 내용은 "스토리지 관리"를 참조하십시오.

파트너 및 고객을 위한 위치 및 스토리지 선택

파트너/폴더 테넌트를 생성할 때 각 서비스에 대해 새 테넌트에서 사용할 수 있는 여러 위치와 여러 스토리지를 선택할 수 있습니다.

고객 테넌트를 생성할 때는 하나의 위치를 선택한 후 이 위치 안에서 서비스당 하나의 스토리지를 선택해야 합니다. 고객에게 할당된 스토리지는 나중에 변경할 수 있지만, 고객이 스토리지를 사용하기 전 또는 고객이 이 스토리지에서 모든 백업을 삭제한 후에 사용량이 0GB인 경우에만 변경이 가능합니다.

고객 테넌트에 할당된 스토리지에 대한 정보는 **클라이언트** 탭에서 테넌트를 선택하면 테넌트 세부 정보 패널에 표시됩니다. 스토리지 공간 사용에 대한 정보는 실시간으로 업데이트되지 않습니다. 정보가 업데이트되는 데 최대 24시간이 필요합니다.

지역 중복 기능에 대한 자세한 내용은 "지역 중복 스토리지"(71페이지) 항목을 참조하십시오.

위치 관련 작업

새 위치를 생성하려면, **위치 추가**를 클릭하고 위치 이름을 지정합니다.

스토리지나 재해 복구 인프라를 다른 위치로 옮기려면 스토리지나 인프라를 선택하고, **위치** 필드에서 연필 아이콘을 클릭한 후 대상 위치를 선택합니다.

위치의 이름을 변경하려면 위치 이름 옆에 있는 말줄임표 아이콘을 클릭하고 **이름 변경**을 클릭한 후 새 위치 이름을 지정합니다.

위치를 삭제하려면 위치 이름 옆에 있는 말줄임표 아이콘을 클릭하고 **삭제**를 클릭한 후 결정을 확인합니다. 빈 위치만 삭제할 수 있습니다.

스토리지 관리

새 스토리지 추가

- **Cyber Protection** 서비스:
  - 기본적으로 백업 스토리지는 데이터 센터에 있습니다.
  - 상위 관리자가 파트너 테넌트에 **파트너 소유 백업 스토리지** 항목을 제공하는 경우, 파트너 관리자는 Cyber Infrastructure 소프트웨어를 사용하여 파트너의 자체 데이터 센터에서 스토리지를 구성할 수 있습니다. **위치** 섹션에서 **백업 스토리지 추가**를 클릭하면 자체 데이터 센터에서 백업 스토리지 구성에 대한 정보를 찾을 수 있습니다.
  - 상위 관리자가 파트너 테넌트에 **파트너 재해복구 인프라** 항목을 제공하는 경우 파트너 관리자는 파트너의 자체 데이터 센터에서 재해 복구를 구성할 수 있습니다. 재해 복구 인프라 추가에 대한 자세한 내용은 기술 지원에 문의하십시오.

참고
데이터 센터에서 사용되는 Amazon S3, Microsoft Azure, Google Cloud Storage, Wasabi 같은 퍼블릭 클라우드 개체 스토리지로는 백업 유효성 검사를 수행할 수 없습니다.
백업 유효성 검사를 수행하려면 파트너가 사용하는 퍼블릭 클라우드 개체 스토리지를 사용해야 합니다. 하지만 유효성 검사 작업을 수행하면 이러한 퍼블릭 개체 스토리지에서 발생하는 송신 트래픽이 대폭 증가하여 비용이 매우 많이 발생할 수 있습니다.

- 다른 서비스에서 사용할 스토리지 추가에 대한 자세한 내용은 기술 지원에 문의하십시오.

스토리지 삭제

사용자 또는 사용자의 하위 테넌트가 추가한 스토리지를 삭제할 수 있습니다.

스토리지가 고객 테넌트에 할당된 경우 스토리지를 삭제하기 전에 모든 고객 테넌트에 스토리지를 사용하는 서비스를 비활성화해야 합니다.

스토리지를 삭제하려면:

1. 관리 포털에 로그인합니다.
2. 스토리지가 추가된 테넌트로 이동합니다.
3. **설정** > **위치**를 클릭합니다.
4. 삭제할 스토리지를 선택합니다.
5. 스토리지 속성 패널에서 말줄임표 아이콘을 클릭하고 **스토리지 삭제**를 클릭합니다.
6. 결정을 확인합니다.

변경 불가 스토리지

변경 불가능 스토리지 사용 시에는 지정된 보존 기간 동안 삭제된 백업에 액세스할 수 있습니다. 이러한 백업의 내용을 복구할 수는 있지만 백업을 변경, 이동, 삭제할 수는 없습니다. 보존 기간이

끝나면 삭제된 백업은 영구적으로 삭제됩니다.

변경 불가능 스토리지에는 다음 백업이 포함됩니다.

- 수동으로 삭제하는 백업.
- 보호 계획의 **보관 기간** 섹션 또는 정리 계획의 **보존 규칙** 섹션 내 설정에 따라 자동으로 삭제되는 백업.

변경 불가능 스토리지에서 삭제된 백업은 계속 스토리지 공간을 사용하며, 그에 따라 요금이 청구됩니다.

삭제된 테넌트는 변경 불가능 스토리지를 포함한 모든 스토리지에 대해 청구되지 않습니다.

파트너 수준과 고객 수준에서 변경 불가능 스토리지를 구성할 수 있습니다.

중요
각 수준에서 스토리지를 독립적으로 구성할 수 있습니다. 고객 관리자는 상위 파트너 테넌트에서 변경 불가 스토리지가 활성화되어 있지 않아도 테넌트에 대해 변경 불가능 스토리지를 활성화할 수 있습니다. 사용자 정의 설정이 적용되어 있지 않은 자식 테넌트만이 상위 테넌트의 설정을 상속합니다.

변경 불가능 스토리지 설정을 구성하려면 관리자 계정이 속하는 테넌트에서 2단계 인증을 사용해야 합니다.

변경 불가능 스토리지 모드

파트너 테넌트에서는 변경 불가능 스토리지 모드를 선택할 수 없습니다. 관리자는 변경 불가능 스토리지를 비활성화 및 다시 활성화할 수 있으며 스토리지의 모드와 보존 기간을 변경할 수 있습니다.

고객 테넌트에서 변경 불가능 스토리지를 사용할 수 있는 모드는 다음과 같습니다.

- **거버넌스 모드**
  변경 불가능 스토리지를 비활성화하고 다시 활성화할 수 있습니다. 보존 기간을 변경하거나 규제 준수 모드로 전환할 수 있습니다.
- **규제 준수 모드**

  경고!
  규제 준수 모드 선택은 되돌릴 수 없습니다.

  변경 불가능 스토리지를 비활성화할 수 없습니다. 보존 기간을 변경하거나 거버넌스 모드로 다시 전환할 수 없습니다.

참고
21.12 릴리스부터 새 파트너 테넌트에서는 보관 기간이 14일인 변경 불가 스토리지가 기본적으로 활성화됩니다.기존 테넌트에서는 변경 불가 스토리지를 수동으로 활성화해야 합니다.

지원되는 스토리지 및 에이전트

- 변경 불가능한 스토리지는 클라우드 스토리지에서만 지원됩니다.

  변경 불가능한 스토리지는 Cyber Infrastructure 버전 4.7.1 이상을 사용하는 Acronis 호스팅 및 파트너 호스팅 클라우드 스토리지에 사용할 수 있습니다.

  Cyber Infrastructure Backup Gateway와 함께 사용할 수 있는 모든 스토리지가 지원됩니다. Cyber Infrastructure 스토리지, Amazon S3 및 EC2 스토리지, Microsoft Azure 스토리지 등을 예로 들 수 있습니다.

  변경 불가능 스토리지는 Cyber Infrastructure에서 Backup Gateway 서비스에 대해 TCP 포트 40440이 열려 있어야 합니다. 버전 4.7.1 이상에서는 TCP 포트 40440이 **Backup(ABGW) Public** 트래픽 유형으로 자동으로 열립니다. 트래픽 유형에 대한 자세한 정보는 Acronis Cyber Infrastructure 문서를 참조하십시오.
- 변경 불가 스토리지를 사용하려면 보호 에이전트 버전 21.12(빌드 15.0.28532) 이상이 필요합니다.
- TIBX(버전 12) 백업만 지원됩니다.

변경 불가 스토리지 활성화 및 비활성화

변경 불가능 스토리지 설정을 구성하려면 관리자 계정이 속하는 테넌트에서 2단계 인증을 사용해야 합니다.

참고

삭제된 백업에 대한 액세스 권한을 허용하려면 백업 스토리지의 40440 포트를 수신 연결을 위해 활성화해야 합니다.

변경 불가 스토리지를 활성화하려면

파트너 테넌트

1. 관리 포털에 관리자로 로그인한 후 **설정** > **보안**으로 이동합니다.
2. **변경 불가 스토리지** 스위치를 활성화합니다.
3. 14~3650일 사이의 보존 기간을 지정합니다.

   기본 보관 기간은 14일입니다. 보존 기간이 길수록 스토리지 사용량도 많아집니다.
4. **저장**을 클릭합니다.

고객 테넌트

1. 관리 포털에 관리자로 로그인한 후 **클라이언트**로 이동합니다.
2. 고객 테넌트의 설정을 편집하려면 테넌트 이름을 클릭합니다.
3. 탐색 메뉴에서 **설정** > **보안**으로 이동합니다.
4. **변경 불가 스토리지** 스위치를 활성화합니다.
5. 14~3650일 사이의 보존 기간을 지정합니다.

   기본 보관 기간은 14일입니다. 보존 기간이 길수록 스토리지 사용량도 많아집니다.
6. 변경 불가능 스토리지 모드를 선택하고 메시지가 표시되면 선택 내용을 확인합니다.

7. **저장**을 클릭합니다.

경고!
규제 준수 모드를 선택한 후에는 이전 모드로 되돌릴 수 없습니다. 이 모드를 선택하고 나면 변경 불가능 스토리지를 비활성화하거나 스토리지의 모드 또는 보존 기간을 변경할 수 없습니다.

8. 기존 아카이브가 변경 불가능 스토리지를 지원하도록 설정하려면 해당 아카이브에서 새 백업을 생성합니다.
   새 백업을 생성하려면 보호 계획을 수동으로 실행하거나 스케줄에 따라 실행합니다.

경고!
아카이브가 변경 불가능 스토리지를 지원하도록 설정하기 전에 삭제하는 백업은 영구적으로 삭제됩니다.

변경 불가 스토리지를 비활성화하려면

파트너 테넌트

1. 관리 포털에 관리자로 로그인한 후 **설정** > **보안**으로 이동합니다.
2. **변경 불가 스토리지** 스위치를 비활성화합니다.

중요
이 변경 사항은 변경 불가능 스토리지의 사용자 정의 설정을 사용하지 않는 모든 자식 테넌트에 상속됩니다.

경고!
변경 불가능 스토리지 비활성화는 즉시 적용되지 않습니다. 즉, 유예 기간인 14일 동안은 변경 불가능 스토리지가 계속 활성 상태로 유지되므로 원래 보존 기간에 따라 삭제된 백업에 액세스할 수 있습니다. 유예 기간이 끝나면 변경 불가능 스토리지의 모든 백업은 영구적으로 삭제됩니다.

3. **비활성화**를 클릭하여 선택을 확인합니다.

고객 테넌트

1. 관리 포털에 관리자로 로그인한 후 **클라이언트**로 이동합니다.
2. 고객 테넌트의 설정을 편집하려면 테넌트 이름을 클릭합니다.
3. 탐색 메뉴에서 **설정** > **보안**으로 이동합니다.
4. **변경 불가 스토리지** 스위치를 비활성화합니다.

참고
변경 불가능 스토리지는 거버넌스 모드에서만 비활성화할 수 있습니다.

경고!
변경 불가능 스토리지 비활성화는 즉시 적용되지 않습니다. 즉, 유예 기간인 14일 동안은 변경 불가능 스토리지가 계속 활성 상태로 유지되므로 원래 보존 기간에 따라 삭제된 백업에 액세스할 수 있습니다. 유예 기간이 끝나면 변경 불가능 스토리지의 모든 백업은 영구적으로 삭제됩니다.

5. **비활성화**를 클릭하여 선택을 확인합니다.

변경 불가능 스토리지의 요금 청구 예제

아래 예제에는 14일(기본 보존 기간) 동안 변경 불가능 스토리지에 저장되는 삭제된 백업이 나와 있습니다. 이 기간 동안에는 삭제된 백업이 스토리지에 저장되므로 스토리지 공간이 사용됩니다. 보존 기간이 끝나면 삭제된 백업이 영구적으로 삭제되므로 스토리지 사용량이 감소합니다. 스토리지 사용량에 따라 매월 요금이 부과됩니다.

날짜	백업	스토리지 사용	요금 청구
4월 1일	백업 A(10GB) 생성됨 백업 B(1GB) 생성됨	10GB + 1GB = 11GB	
4월 20일	백업 B가 삭제되어 변경 불가능 스토리지에 저장됨 (보존 기간: 14일)	10GB + 1GB = 11GB	
4월 30일			4월 요금이 청구됨(사용량: 11GB)
5월 4일	보존 기간이 끝난 백업 B가 완전히 삭제됨	11GB - 1GB = 10GB	
5월 31일			5월 요금이 청구됨(사용량: 10GB)

지역 중복 스토리지

지역 중복 스토리지 사용 시에는 데이터가 주 위치와 멀리 떨어져 있는 보조 위치에 비동기식으로 복사되므로 데이터 내구성이 높아집니다. 이처럼 데이터가 여러 지역에 중복 저장되므로 주 위치를 사용할 수 없게 되더라도 데이터에 액세스할 수 있습니다.

지역 중복 스토리지 활성화 및 비활성화

사전 요구 사항

- 클라우드 인프라에서 지역 중복 스토리지를 사용할 수 있는지 확인합니다.
- 관리자만 지역 중복 스토리지를 활성화하거나 비활성화할 수 있습니다. 지역 중복 스토리지를 활성화하거나 비활성화하려면 관리자 권한이 있는지 확인하십시오.

기존 테넌트를 대상으로 지역 중복 스토리지를 활성화하려면

1. 관리 포털에서 **클라이언트**로 이동합니다.
2. 지역 중복 기능을 활성화하려는 테넌트로 이동합니다.

   참고
   여러 테넌트를 대상으로 지역 중복 기능을 활성화하려는 경우에는 "여러 기존 테넌트에 대해 서비스 활성화"(38페이지) 항목을 참조하십시오.

3. **편집**을 클릭하여 설정을 변경합니다.
4. **클라우드 리소스**에서 필요한 스토리지 이름 아래의 **지역 중복** 확인란을 선택합니다.
5. **저장**을 클릭합니다.
   테넌트에 대해 지역 중복 기능이 활성화됩니다. 고객 관리자는 Cyber Protect 콘솔에서 지역 중복 기능을 비활성화할 수 있습니다.

기존 테넌트를 대상으로 지역 중복 스토리지를 비활성화하려면

1. 관리 포털에서 **클라이언트**로 이동합니다.
2. 지역 중복 기능을 비활성화하려는 테넌트로 이동합니다.
3. **편집**을 클릭하여 설정을 변경합니다.
4. **클라우드 리소스**에서 필요한 스토리지 이름 아래의 **지역 중복** 확인란을 선택 취소합니다.
5. **저장**을 클릭합니다.

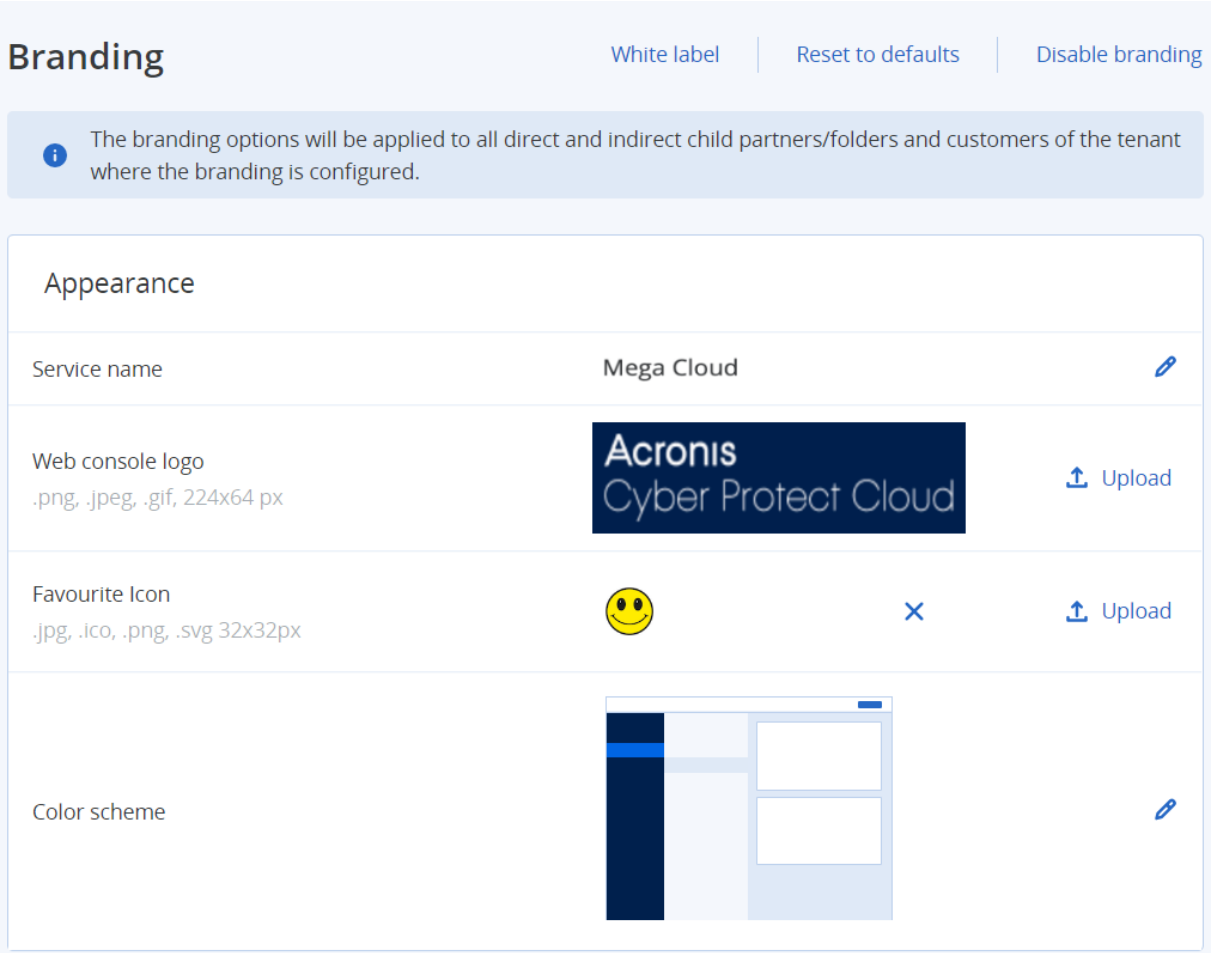
   경고!
   지역 중복 기능이 비활성화됩니다. 복제된 데이터는 1일 내에 삭제됩니다.

제한 사항

- 현재 복제된 데이터용 보조 위치는 미국과 캐나다에서만 사용 가능합니다.
- 지역 중복 기능 사용 시의 Disaster Recovery 서비스 관련 제한 사항에 대한 자세한 내용은 Disaster Recovery 설명서를 참조하십시오.

브랜딩 구성 및 화이트 레이블 작업

설정 > **브랜딩** 섹션에서 파트너 관리자는 관리 포털의 사용자 인터페이스와 **Cyber Protection** 서비스를 사용자 정의하여 상위 수준 파트너와의 모든 연결을 제거할 수 있습니다.



브랜딩은 파트너 및 폴더 수준에서 구성할 수 있습니다. 브랜딩은 브랜딩이 구성된 모든 직접 및 간접 하위 파트너/폴더와 테넌트 고객에게 적용됩니다.

기타 서비스에서는 해당 서비스 콘솔에서 별도의 브랜딩 기능을 제공합니다. 자세한 내용은 해당 서비스의 사용자 안내서를 참조하십시오.

항목 브랜딩

외관

- **서비스 이름**. 처음 로그인한 후 **시작** 화면에서 이 이름은 관리 포털 및 클라우드 서비스에서 전송한 모든 이메일 메시지에 사용되고(계정 활성화 메시지, 서비스 알림 이메일 메시지), 관리 포털 브라우저 탭 이름으로 사용됩니다.
- **웹 콘솔 로고**. 로고는 관리 포털 및 서비스에 표시됩니다. **업로드**를 클릭하여 이미지 파일을 업로드합니다.
- **즐겨찾기 아이콘**[사용자 정의 URL이 구성되어 있는 경우에만 사용 가능]. 브라우저 탭의 페이지 제목 옆에 Favicon이 표시됩니다. **업로드**를 클릭하여 이미지 파일을 업로드합니다.
- **색 구성표**. 색 구성표는 모든 사용자 인터페이스 요소에 사용되는 색 조합을 정의합니다.

참고
새 탭에서 구성표 미리 보기를 클릭하면 하위 테넌트에서 인터페이스가 어떻게 표시되는지 확인할 수 있습니다. **색 구성표 선택** 패널에서 **완료**를 클릭하기 전에는 브랜딩이 적용되지 않습니다.

에이전트 및 인스톨러 브랜딩

Windows 및 macOS용 에이전트 설치 파일 및 트레이 모니터의 브랜딩을 사용자 정의할 수 있습니다.

참고
이 브랜딩 기능을 활성화하려면 Cyber Protection 에이전트를 15.0.28816 버전(릴리스 22.01) 이상으로 업데이트해야 합니다.

- **에이전트 인스톨러 파일 이름**. 보호된 워크로드에서 다운로드한 설치 파일의 이름입니다.
- **에이전트 인스톨러 로고**. 에이전트 설치 도중 설치 마법사에 표시되는 로고입니다. **업로드**를 클릭하여 이미지 파일을 업로드합니다.
- **에이전트 이름**. 에이전트 설치 도중 설치 마법사에 표시되는 로고입니다.
- **트레이 모니터 이름**. 트레이 모니터 창 위쪽에 표시되는 이름입니다.

문서 및 지원

- **홈 URL**. 사용자가 **정보** 패널에서 회사 이름을 클릭하면 이 페이지가 열립니다.
- **지원 URL**. 사용자가 **정보** 패널 또는 관리 포털에서 전송한 이메일 메시지에 있는 **지원 센터로 문의하십시오** 링크를 클릭하면 이 페이지가 열립니다.
- **지원 전화**. 이 전화 번호는 **정보** 패널에 표시됩니다.
- **지식 베이스 URL**. 사용자가 오류 메시지의 **지식 베이스** 링크를 클릭하면 이 페이지가 열립니다.
- **관리 포털 관리자 안내서**. 사용자가 관리 포털 사용자 인터페이스 오른쪽 위에 있는 물음표 아이콘을 클릭한 다음 **정보** > **관리자 안내서**를 클릭하면 이 페이지가 열립니다.
- **관리 포털 관리자 도움말**. 사용자가 관리 포털 사용자 인터페이스 오른쪽 위에 있는 물음표 아이콘을 클릭한 다음 **도움말**을 클릭하면 이 페이지가 열립니다.

Cyber Protect Cloud 서비스 URL

사용자 정의 도메인에서 Cyber Protect Cloud 서비스를 사용할 수 있도록 설정할 수 있습니다. 처음으로 사용자 정의 URL을 설정하는 경우 **구성**을 클릭하고 기존 URL을 변경하는 경우 **재구성**을 클릭합니다. 기본 URL(https://cloud.acronis.com)을 사용하려면 **기본값으로 복구**를 클릭합니다. 사용자 정의 URL에 대한 자세한 내용은 "사용자 정의 웹 인터페이스 URL 구성"을 참조하십시오.

법률 문서 설정

- **최종 사용자 라이센스 계약(EULA) URL**. 사용자가 **정보** 패널, 처음 로그인한 후 **시작** 화면 또는 업로드 요청 랜딩 페이지에 있는 **최종 사용자 라이선스 계약** 링크를 클릭하면 이 페이지가 열

립니다.

- **플랫폼 약관 URL**. 파트너 관리자가 **정보** 패널 또는 처음 로그인한 후 **시작** 화면에 있는 **플랫폼 약관** 링크를 클릭하면 이 페이지가 열립니다.
- **개인정보처리방침 URL**. 사용자가 처음 로그인한 후 **시작** 화면 및 업로드 요청 랜딩 페이지에 있는 **개인정보처리방침** 링크를 클릭하면 이 페이지가 열립니다.

중요
시작 화면에 문서가 표시되지 않도록 하려는 경우 해당 문서의 URL을 입력하지 마십시오.

참고
File Sync & Share 업로드 요청에 대한 자세한 내용은 Cyber Files Cloud 사용자 안내서를 참조하십시오.

업셀

- **구입 URL**. Cyber Protection 서비스의 Advanced Edition으로 업그레이드하기 위해 사용자가 **지금 구입**을 클릭하는 경우 이 페이지가 열립니다. 업셀 시나리오에 대한 자세한 내용은 "고객에 대한 업셀 시나리오 구성"을 참조하십시오.

모바일 앱

- **App Store**. 사용자가 **Cyber Protection** 서비스에서 **추가** > **iOS**를 클릭하면 이 페이지가 열립니다.
- **Google Play**. 사용자가 **Cyber Protection** 서비스에서 **추가** > **Android**를 클릭하면 이 페이지가 열립니다.

이메일 서버 설정

관리 포털 및 서비스에서 이메일 알림을 보내는 데 사용할 사용자 정의 이메일 서버를 지정할 수 있습니다. 사용자 정의 이메일 서버를 지정하려면 **사용자 정의**를 클릭한 후 다음 설정을 지정합니다.

- **보낸 사람**에 이메일 알림의 **보낸 사람** 필드에 표시할 이름을 입력합니다.
- **SMTP**에 보내는 메일 서버(SMTP)의 이름을 입력합니다.
- **포트**에 보내는 메일 서버의 포트를 입력합니다. 기본적으로 포트는 25로 설정됩니다.
- **암호화**에서 SSL 또는 TLS 암호화를 사용할지 여부를 선택합니다. 암호화를 비활성화하려면 **없음**을 선택하십시오.
- **사용자 이름** 및 **비밀번호**에 메시지를 보내는 데 사용할 계정의 자격 증명을 지정합니다.

브랜딩 구성

1. 관리 포털에 로그인합니다.
2. 브랜딩을 구성하려는 테넌트로 이동합니다.
3. **설정** > **브랜딩**을 클릭합니다.

4. [브랜딩이 아직 활성화되지 않은 경우] **브랜딩 활성화**를 클릭합니다.
5. 위에 설명된 브랜딩 항목을 구성합니다.

기본 브랜딩 설정 복원

모든 브랜딩 항목을 기본값으로 재설정할 수 있습니다.

1. 관리 포털에 로그인합니다.
2. 브랜딩을 재설정하려는 테넌트로 이동합니다.
3. **설정** > **브랜딩**을 클릭합니다.
4. 오른쪽 상단에서 **기본값으로 복원**을 클릭합니다.

브랜딩 비활성화

계정 및 모든 자식 테넌트에 대해 브랜딩을 비활성화할 수 있습니다.

1. 관리 포털에 로그인합니다.
2. 브랜딩을 비활성화하려는 테넌트로 이동합니다.
3. **설정** > **브랜딩**을 클릭합니다.
4. 오른쪽 상단에서 **브랜딩 비활성화**를 클릭합니다.

화이트 레이블 작업

모든 자식 파트너와 고객에 대해 Cyber Protection 에이전트(Windows, macOS 및 Linux)와 Cyber Protection 모니터(Windows, macOS 및 Linux) 및 Connect 클라이언트의 브랜드 또는 화이트 레이블 작업 수행 여부를 제어할 수 있습니다. 화이트 레이블 작업을 활성화하면 에이전트, Connect 클라이언트 및 트레이 모니터에 대해 화이트 레이블 작업이 수행됩니다. 이 설정은 인스톨러와 Cyber Protection 모니터에 사용되는 이름 및 로고에도 영향을 줍니다.

화이트 레이블 작업 적용

1. 관리 포털에 로그인합니다.
2. 화이트 레이블 작업을 적용하려는 테넌트로 이동합니다.
3. **설정** > **브랜딩**을 클릭합니다.
4. 창 위쪽 끝부분에서 **화이트 레이블**을 클릭하여 **서비스 이름**, **최종 사용자 라이센스 계약(EULA) URL**, **관리 포털 관리자 안내서**, **관리 포털 관리자 도움말**, **이메일 서버 설정**을 제외한 모든 브랜딩 항목을 지웁니다.

사용자 정의 웹 인터페이스 URL 구성

참고
사용자 정의 URL은 기본 URL과 다른 IP 주소를 가리킵니다. 방화벽 정책을 구성할 때 이 점에 유의하십시오.

***Cyber Protect Cloud** 서비스의 웹 인터페이스 **URL**을 구성하려면*

1. 관리 포털에서 **설정** > **브랜딩**을 클릭합니다.
2. **Cyber Protect Cloud 서비스의 URL** 섹션에서
   - 처음으로 사용자 정의 URL을 설정하는 경우 **구성**을 클릭합니다.
   - 기존 사용자 정의 URL을 변경하는 경우 **재구성**을 클릭합니다.
3. **도메인 설정** 단계에서 도메인 및 CNAME 레코드를 준비합니다.

   사용자 정의 URL을 사용하려면 활성 도메인 이름이 필요하며, 계정이 있는 데이터 센터를 가리키도록 구성된 CNAME 레코드도 필요합니다. CNAME 레코드의 구성은 DNS 등록 기관에서 수행하며 전파하는 데 최대 48시간이 소요될 수 있습니다.

   데이터 센터의 도메인 이름을 확인하고 CNAME 레코드 구성을 요청하려면 브랜딩 웹 콘솔 URL (58275) 문서를 참조하십시오.
4. **URL 확인** 단계에서 사용자 정의 URL에 액세스할 수 있고 CNAME 레코드가 올바르게 구성되어 있는지 확인하십시오. 이 작업을 수행하려면 기본 URL 이름을 입력하고 **확인**을 클릭합니다. 와일드카드 SSL 인증서를 사용하면 최대 10개의 대체 도메인 이름을 추가할 수 있습니다. "Let's Encrypt" 인증서를 사용하면 대체 도메인 이름이 무시됩니다.
5. **SSL 인증서** 단계에서 다음 중 하나를 수행할 수 있습니다.
   - "Let's Encrypt" 인증서 생성. 이 작업을 수행하려면 **"Let's Encrypt"가 포함된 무료 SSL 인증서**를 클릭합니다. 이 옵션은 제삼자 법인에서 발급한 "Let's Encrypt" 인증서를 사용합니다. 서비스 제공업체는 이러한 무료 인증서의 사용으로 인해 발생하는 문제에 대해 책임을 지지 않습니다. "Let's Encrypt" 용어에 대한 자세한 내용은 https://letsencrypt.org/repository/를 참조하십시오.
   - 와일드카드 인증서 업로드. 이 작업을 수행하려면 **와일드카드 인증서 업로드**를 클릭한 다음 와일드카드 인증서와 비공개 키를 제공합니다.

     참고

     인증서 유효성 검사 오류가 발생하고 "인증서를 확인하지 못함: x509: 알려지지 않은 기관에서 서명한 인증서" 오류 메시지가 표시될 수 있습니다. 일반적으로 이 메시지는 일부 중간 인증서가 누락되었다는 의미입니다. 인증서 체인 확인자를 사용해 인증서 구조를 수정한 후 전체 인증서 체인을 업로드합니다.
6. **제출** 클릭하여 변경 사항을 적용합니다.

사용자 정의 URL을 기본값으로 재설정하려면

1. 관리 포털에서 **설정** > **브랜딩**을 클릭합니다.
2. **Acronis Cyber Protect Cloud 서비스 URL** 섹션에서 **기본값으로 복구**를 클릭하여 기본 URL (https://cloud.acronis.com)을 사용합니다.

모니터링

서비스 사용 및 작업에 대한 정보에 액세스하려면 **모니터링**을 클릭합니다.

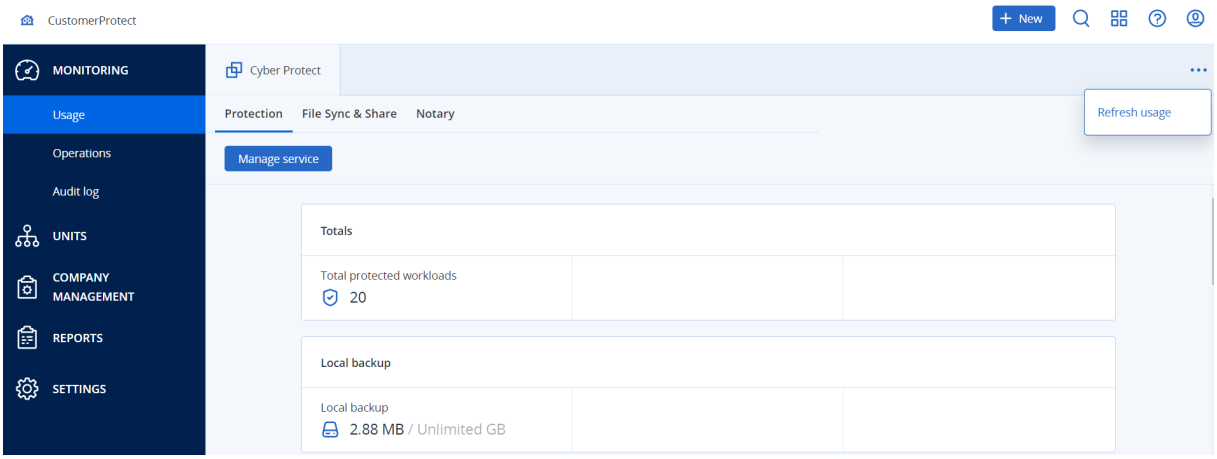
사용

사용 탭은 서비스 사용에 대한 개요를 제공하며 사용자가 운영 중인 테넌트의 서비스에 액세스할 수 있게 합니다.

사용량 데이터에는 표준 기능과 고급 기능이 모두 포함됩니다.

탭에 표시되는 사용량 데이터를 새로 고치려면 화면 오른쪽 위의 말줄임표를 클릭하고 **사용량 새로 고침**을 선택합니다.

참고
데이터를 페치하려면 최대 10분 정도 걸릴 수 있습니다. 업데이트된 데이터를 확인하려면 페이지를 다시 로드하십시오.



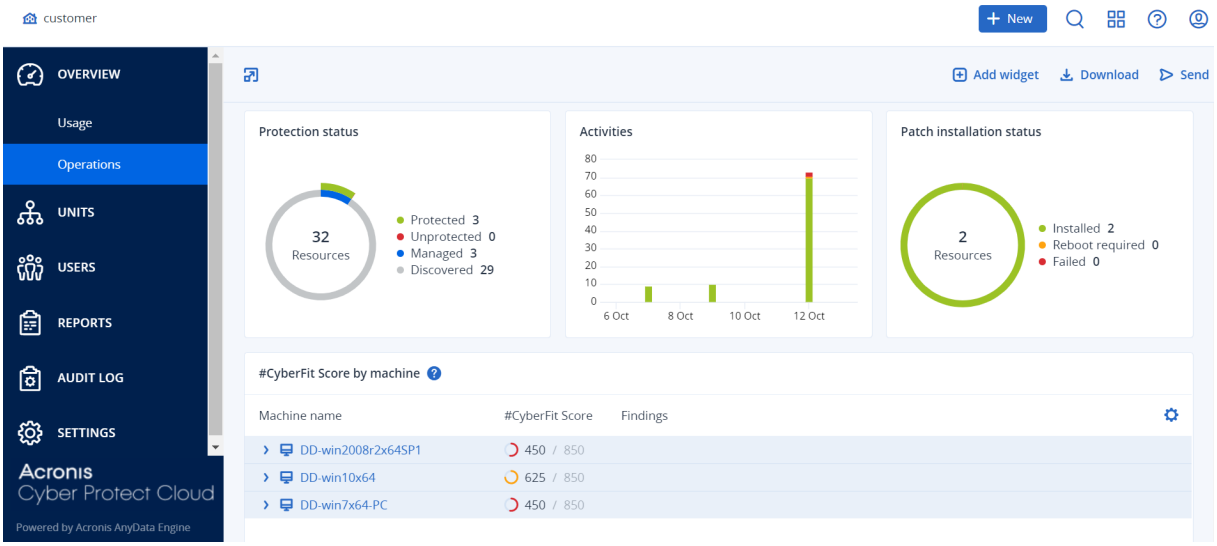
동작

작업 대시보드는 Cyber Protection 서비스와 관련된 작업의 개요를 제공하는 많은 사용자 정의 가능한 위젯을 제공합니다. 다른 서비스에 대한 위젯은 향후 릴리스에서 제공될 예정입니다.

기본적으로 사용자가 작업 중인 테넌트에 대한 데이터가 표시됩니다. 편집하여 각 위젯에 대해 표시된 테넌트를 개별적으로 변경할 수 있습니다. 폴더에 있는 테넌트를 포함하여 선택된 테넌트의 직접 하위 고객 테넌트에 대한 집계 정보도 표시됩니다. 대시보드는 하위 파트너 및 해당 하위 테넌트에 대한 정보를 표시하지 *않습니다*. 특정 파트너를 드릴다운하여 해당 대시보드를 확인해야 합니다. 그러나 하위 파트너 테넌트를 폴더 테넌트로 변환하면 이 테넌트의 하위 고객에 대한 정보가 상위 테넌트의 대시보드에 표시됩니다.

위젯은 2분마다 업데이트됩니다. 위젯에는 조사할 수 있고 문제를 해결할 수 있는 클릭 가능한 요소가 있습니다. 대시보드의 현재 상태를 .pdf 및/또는 .xlsx 형식으로 다운로드하거나, 이메일을 통해 외부 받는 사람을 포함한 모든 주소로 보낼 수 있습니다.

표, 원 그래프, 막대형 차트, 목록, 트리형 맵으로 표시되는 여러 가지 위젯 중 선택할 수 있습니다. 같은 유형의 여러 위젯을 다른 테넌트 또는 다른 필터에 추가할 수 있습니다.



대시보드에서 위젯을 재정렬하려면:

이름을 클릭하여 위젯을 끌어서 놓습니다.

위젯을 편집하려면:

위젯 이름 옆의 연필 아이콘을 클릭합니다. 위젯을 편집하면 이름을 변경하고, 시간을 변경하며, 데이터가 표시되는 테넌트를 선택하고, 필터를 설정할 수 있습니다.

위젯을 추가하려면:

위젯 추가를 클릭한 다음, 다음 중 하나를 수행합니다.

- 추가할 위젯을 클릭합니다. 위젯이 기본 설정으로 추가됩니다.
- 추가하기 전에 위젯을 편집하려면 위젯을 선택할 때 톱니 바퀴 아이콘을 클릭합니다. 위젯을 편집한 후 **완료**를 클릭합니다.

위젯을 제거하려면:

위젯 이름 옆의 X 기호를 클릭합니다.

보호 상태

보호 상태

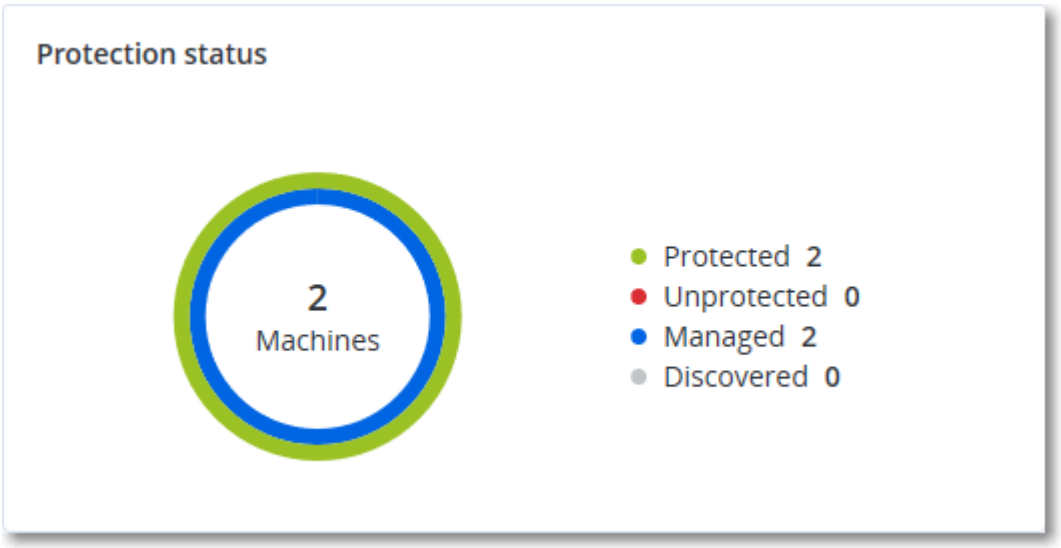
이 위젯은 모든 머신에 대한 현재 보호 상태를 표시합니다.

머신은 다음과 같은 상태일 수 있습니다.

- **보호됨** – 보호 계획이 적용되어 있는 머신입니다.
- **보호되지 않음** – 보호 계획이 적용되어 있지 않은 머신입니다. 여기에는 보호 계획이 적용되지 않은 검색된 머신 및 관리 대상 상태의 머신이 모두 포함됩니다.

- **관리 대상** – 보호 에이전트가 설치되어 있는 머신입니다.
- **검색됨** – 보호 에이전트가 설치되어 있지 않은 머신입니다.

  머신 상태를 클릭하면 해당 상태의 머신 목록으로 리디렉션되어 자세한 정보를 확인할 수 있습니다.



검색된 머신

이 위젯은 지정한 기간 동안 검색된 머신 목록을 표시합니다.

Discovered machines

Device name ↑	IP address	OS	Organizational unit	Discovery type
Windows Server 2012 R2				
win-6g34mv70qa3	10.248.90.221	Windows Server 2012 R2	-	Local Network
Windows 10 Enterprise 2016 LTSB				
device1	10.248.90.238	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory, Local Network
device2	-	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory
device3	10.248.91.243	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory, Manual, Loc...
device4	10.248.91.125	Windows 10 Enterprise 2016 LTSB	-	Active Directory, Local Network
device5	-	Windows 10 Enterprise 2016 LTSB	-	Active Directory, Manual
-				
-	10.250.41.189	-	-	Manual
-	10.248.44.199	-	-	Manual

머신별 #CyberFit Score

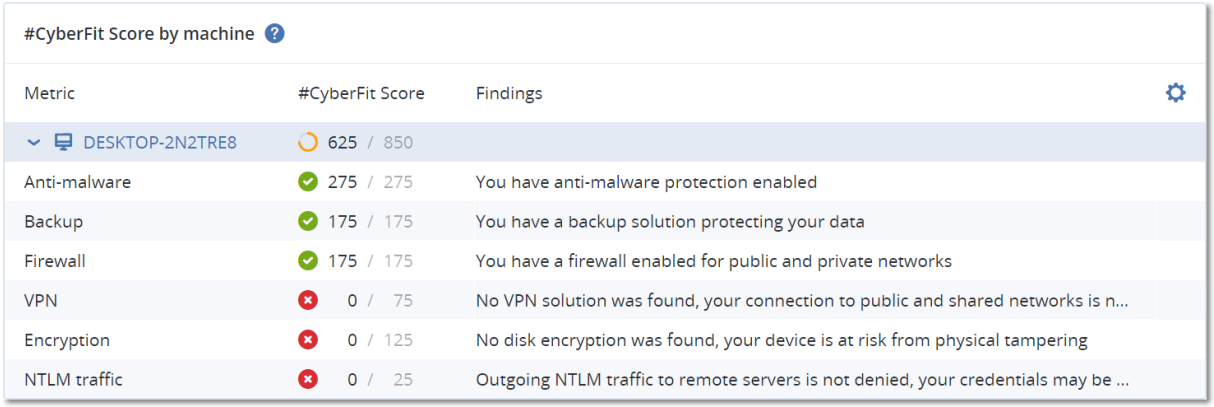
이 위젯에는 각 머신의 총 #CyberFit Score, 복합 점수 및 다음 각 평가 메트릭에 대한 결과가 표시됩니다.

- 맬웨어 방지
- 백업

- 방화벽
- VPN
- 암호화
- NTLM 트래픽

각 메트릭 점수를 개선하기 위한 권장사항은 보고서에서 확인할 수 있습니다.

#CyberFit Score에 대한 자세한 내용은 "머신의 #CyberFit Score"를 참고하십시오.



EDR(엔드포인트 탐지 및 대응) 위젯

중요
이 문서는 EDR 설명서의 Early Access 버전입니다. 따라서 일부 기능 정보와 설명이 완성되지 않았을 수도 있습니다.

EDR(엔드포인트 탐지 및 대응)에는 **동작** 대시보드에서 액세스 가능한 여러 위젯이 포함되어 있습니다.

사용 가능한 위젯은 다음과 같습니다.

- 워크로드별 상위 인시던트 분산
- 인시던트 MTTR
- 보안 인시던트 번다운(Burndown)
- 워크로드 네트워크 상태

워크로드별 상위 인시던트 분산

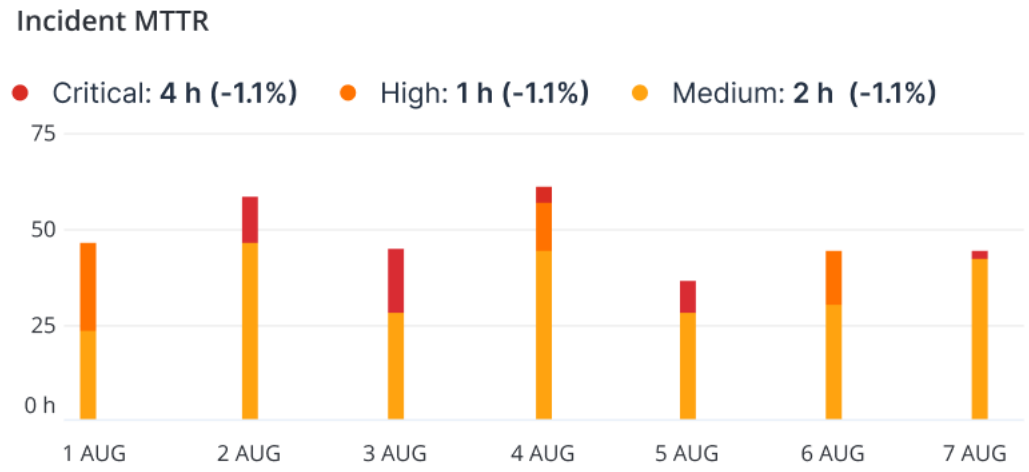
이 위젯에는 인시던트 수가 가장 많은 상위 워크로드 5개가 표시됩니다. **모두 표시**를 클릭하면 인시던트 목록으로 리디렉션됩니다. 인시던트 목록은 위젯 설정에 따라 필터링됩니다.

워크로드 행을 마우스로 가리키면 인시던트의 현재 조사 상태 세부 정보를 확인할 수 있습니다. 조사 상태는 **시작되지 않음**, **조사 중**, **종결됨**, **위양성** 중 하나입니다. 그런 다음 추가로 분석할 워크로드를 클릭하고 표시되는 팝업에서 관련 고객을 선택하면 위젯 설정에 따라 인시던트 목록이 새로 고쳐집니다.

인시던트 MTTR

이 위젯에는 보안 인시던트의 평균 해결 시간이 표시됩니다. MTTR은 인시던트 조사 및 해결 속도를 나타냅니다.

원하는 열을 클릭하면 심각도(**심각**, **높음**, **보통**)에 따른 인시던트 세부 정보, 그리고 각 심각도 수준의 인시던트를 해결하는 데 걸린 시간을 확인할 수 있습니다. 괄호 안에 표시되는 비율 값은 이전 기간과 비교한 증감률을 나타냅니다.

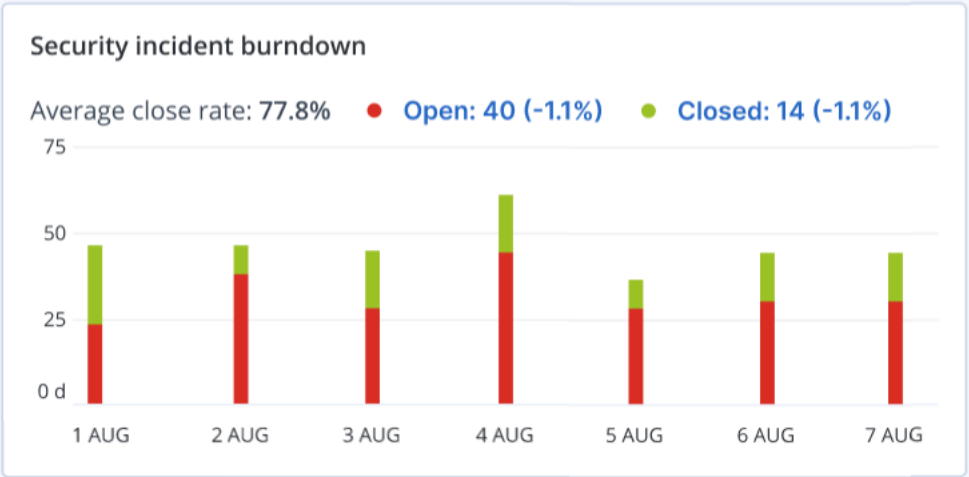


보안 인시던트 번다운(Burndown)

이 위젯에는 인시던트 종료 효율이 표시됩니다. 즉, 일정 기간 동안 종료된 인시던트 수를 기준으로 하여 측정된 미해결 인시던트 수가 표시됩니다.

원하는 열을 마우스로 가리키면 선택한 날짜의 종료된 인시던트와 미해결 인시던트 세부 정보를 확인할 수 있습니다. 미해결 값을 클릭하면 표시되는 팝업에서 관련 테넌트를 선택합니다. 그러면 선택한 테넌트의 필터링된 인시던트 목록이 나타나고 현재 미해결 상태인 인시던트(**조사 중** 또는 **시작되지 않음** 상태의 인시던트)가 표시됩니다. 종결됨 값을 클릭하면 선택한 테넌트의 인시던트 목록이 표시되며, 해당 목록이 필터링되어 더 이상 미해결 상태가 아닌 인시던트(**종결됨** 또는 **위양성** 상태의 인시던트)가 표시됩니다.

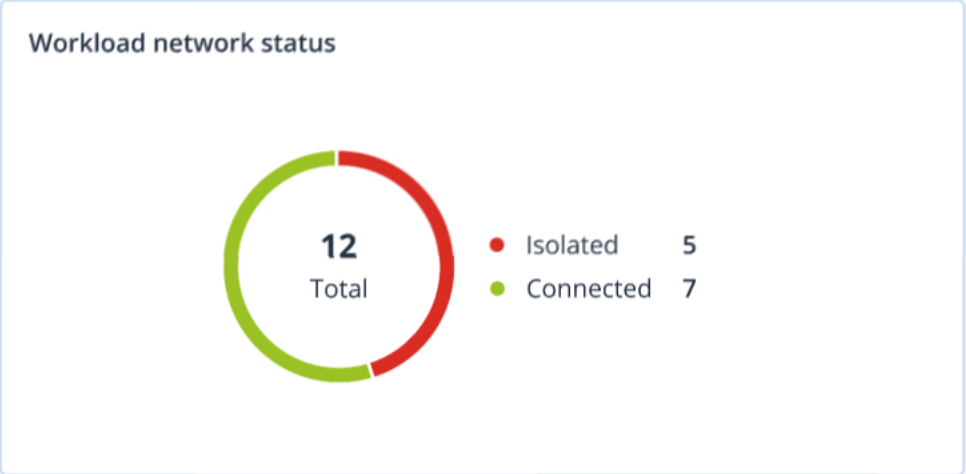
괄호 안에 표시되는 비율 값은 이전 기간과 비교한 증감률을 나타냅니다.



워크로드 네트워크 상태

이 위젯에는 워크로드의 현재 네트워크 상태, 그리고 분리된/연결된 워크로드 수가 표시됩니다.

분리됨 값을 클릭하면 표시되는 팝업에서 관련 테넌트를 선택합니다. 그러면 표시된 워크로드 보기가 필터링되어 분리된 워크로드가 표시됩니다. 연결됨 값을 클릭하면 선택한 테넌트의 연결된 워크로드가 표시되도록 에이전트 목록이 필터링된 워크로드를 확인할 수 있습니다.



디스크 상태 모니터링

디스크 상태 모니터링에서는 현재 디스크 상태 관련 정보 및 상태 예측 정보를 제공합니다. 따라서 디스크 오류와 관련하여 발생할 수 있는 데이터 손실을 방지할 수 있습니다. HDD 및 SSD 디스크가 모두 지원됩니다.

제한 사항

- 디스크 상태 예측은 Windows를 실행하는 머신에 대해서만 지원됩니다.
- 실제 머신의 디스크만 모니터링됩니다. 가상 머신의 디스크는 모니터링할 수 없으며 디스크 상태 위젯에 표시되지 않습니다.

- RAID 구성은 지원되지 않습니다. 디스크 상태 위젯에는 RAID가 구현된 머신 관련 정보가 표시되지 않습니다.
- VNMe SSD는 지원되지 않습니다.

디스크 상태는 다음 중 하나로 표시됩니다.

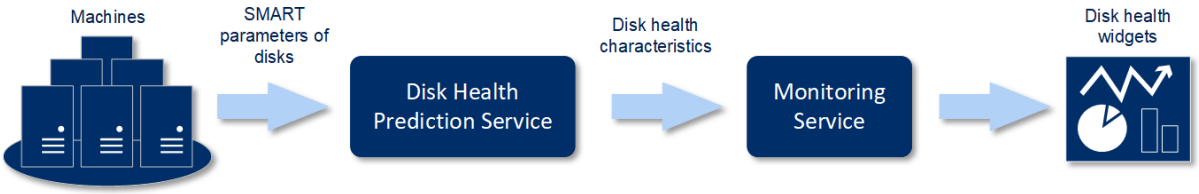
- **정상**
  디스크 상태가 70~100% 사이입니다.
- **경고**
  디스크 상태가 30~70% 사이입니다.
- **심각**
  디스크 상태가 0~30% 사이입니다.
- **디스크 데이터 계산**
  – 현재 및 예측 디스크 상태를 계산하는 중입니다.

작동법

디스크 상태 예측 서비스는 AI 기반 예측 모델을 사용합니다.

1. 보호 에이전트는 디스크의 SMART 매개변수를 수집해 해당 데이터를 디스크 상태 예측 서비스로 전달합니다.
   - SMART 5 – 재할당된 섹터 수입니다.
   - SMART 9 – 가동 시간입니다.
   - SMART 187 – 수정할 수 없는 오류가 보고되었습니다.
   - SMART 188 – 명령 시간이 초과되었습니다.
   - SMART 197 – 현재 보류 중인 섹터 수입니다.
   - SMART 198 – 수정할 수 없는 오프라인 섹터 수입니다.
   - SMART 200 – 쓰기 오류 비율입니다.
2. 디스크 상태 예측 서비스는 수신한 SMART 매개변수를 처리하고, 예측하며, 다음과 같은 디스크 상태 특성을 제공합니다.
   - 디스크 현재 상태: 정상, 경고, 심각.
   - 디스크 상태 예측: 부정적, 안정적, 긍정적
   - 디스크 상태 예측 가능성을 백분율로 표시합니다.

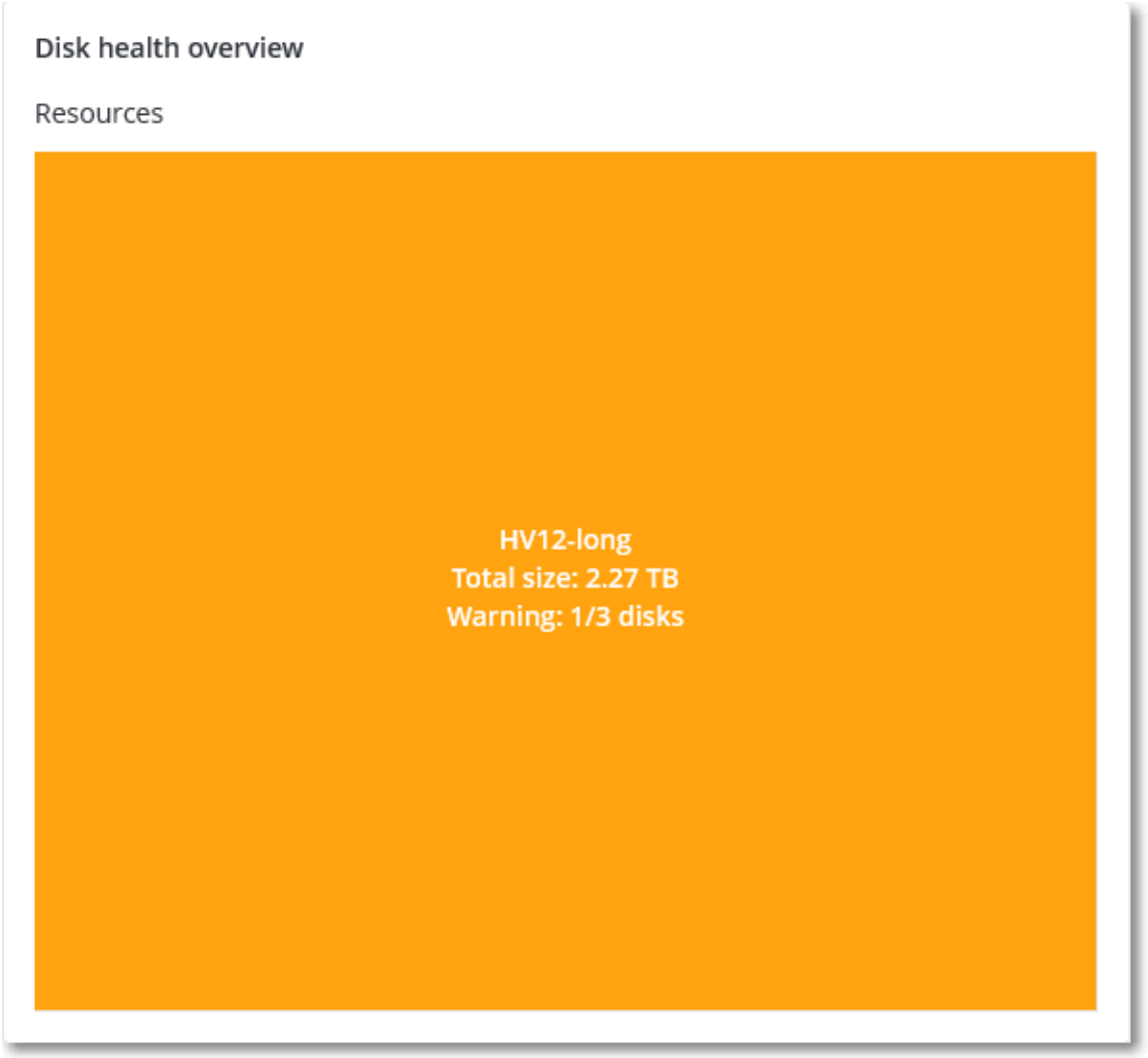
   예측 기간은 1개월입니다.
3. 모니터링 서비스는 이러한 특성을 수신한 다음 Cyber Protect 콘솔의 디스크 상태 위젯에 관련 정보를 표시합니다.



디스크 상태 위젯

디스크 상태 모니터링의 결과는 Cyber Protect 콘솔에서 사용 가능한 다음 위젯에 표시됩니다.

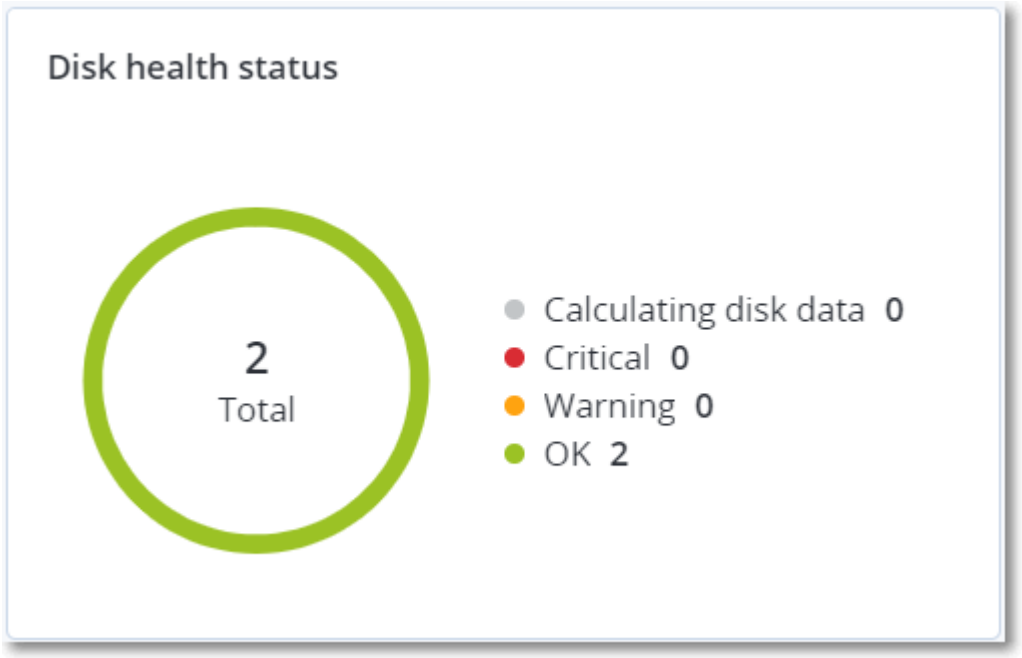
- **디스크 상태 개요** – 트리맵 구조의 위젯으로, 드릴다운을 통해 두 수준의 세부 정보를 전환하며 확인할 수 있습니다.
  - 머신 수준
    선택한 고객 머신별로 디스크 상태에 대한 요약 정보를 표시합니다. 가장 심각한 디스크 상태만 표시됩니다. 다른 상태는 특정 블록을 마우스로 가리켰을 때 도구 설명으로 표시됩니다. 머신 블록 크기는 머신의 총 디스크 크기에 따라 달라집니다. 머신 블록 색상은 발견된 중요 디스크 상태가 무엇인지에 따라 달라집니다.



  - 디스크 수준
    선택한 머신에 있는 모든 디스크의 현재 상태를 표시합니다. 각 디스크 블록에는 다음 디스크 상태 예측 항목 중 하나와 해당 상태가 표시될 확률(비율)이 표시됩니다.
    - 열화될 것으로 예측
    - 안정적으로 유지될 것으로 예측

- 개선될 것으로 예측

- **디스크 상태** – 각 상태에 해당하는 디스크의 수를 원 그래프에 표시한 위젯입니다.



디스크 상태 경보

디스크 상태 확인은 30분마다 실행되고 해당 경보는 하루에 한 번 생성됩니다. 디스크 상태가 **경고**에서 **심각**으로 변경되면 항상 경보가 생성됩니다.

경보 이름	심각도	디스크 상태	설명
잠재적인 디스크 장애	경고	(30 – 70)	나중에 이 머신의 <디스크 이름> 디스크에 장애가 발생할 가능성이 높습니다. 가능한 한 빨리 이 디스크에 대한 전체 이미지 백업을 실행하고 디스크를 교체한 후, 새로운 디스크에 이미지를 복구하십시오.
디스크 장애 임박	심각	(0 – 30)	이 머신의 <디스크 이름> 디스크가 심각한 상태이며, 곧 장애가 발생할 가능성이 매우 높습니다. 추가적인 부담은 디스크 장애를 유발할 수 있으므로 현재 시점에서는 이 디스크의 이미지 백업을 수행하지 않는 것이 좋습니다. 즉시 이 디스크에서 가장 중요한 파일들을 백업한 후 디스크를 교체하십시오.

데이터 보호 맵

사용자는 데이터 보호 맵 기능을 통해 자신에게 중요한 모든 정보를 조사하고 모든 중요 파일의 수, 크기, 위치, 보호 상태와 같은 자세한 정보를 확장 가능한 트리맵 보기로 확인할 수 있습니다.

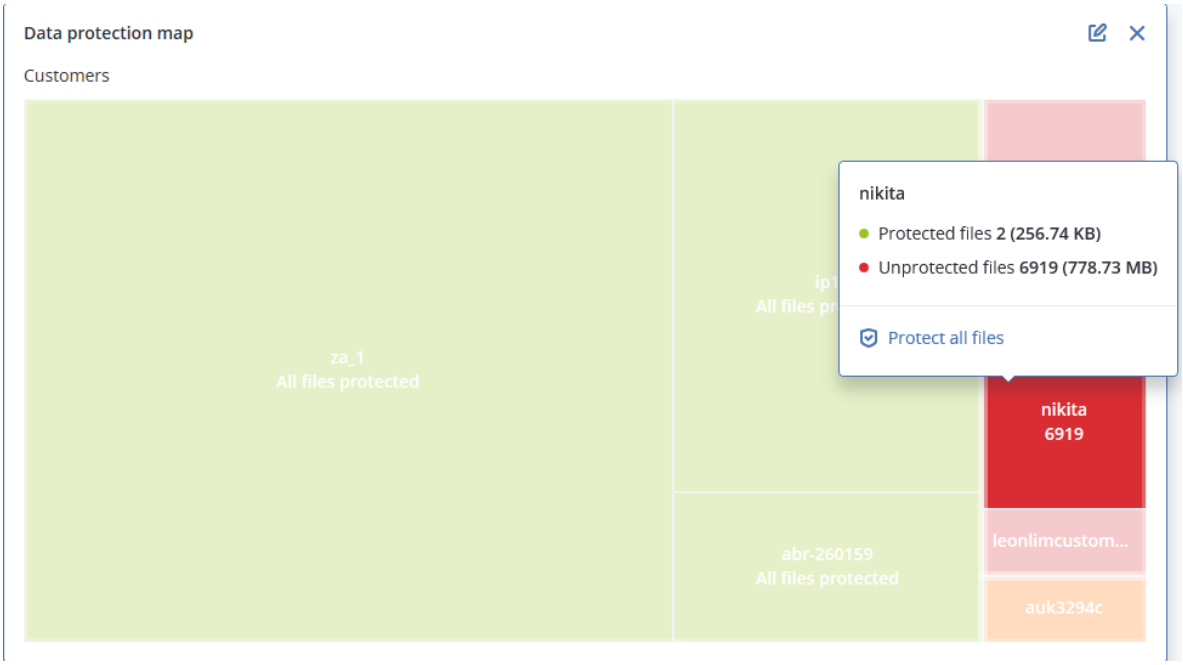
각 블록 크기는 고객/머신에 속한 모든 중요 파일의 총 수/크기에 따라 달라집니다.

파일의 보호 상태는 다음 중 하나로 표시됩니다.

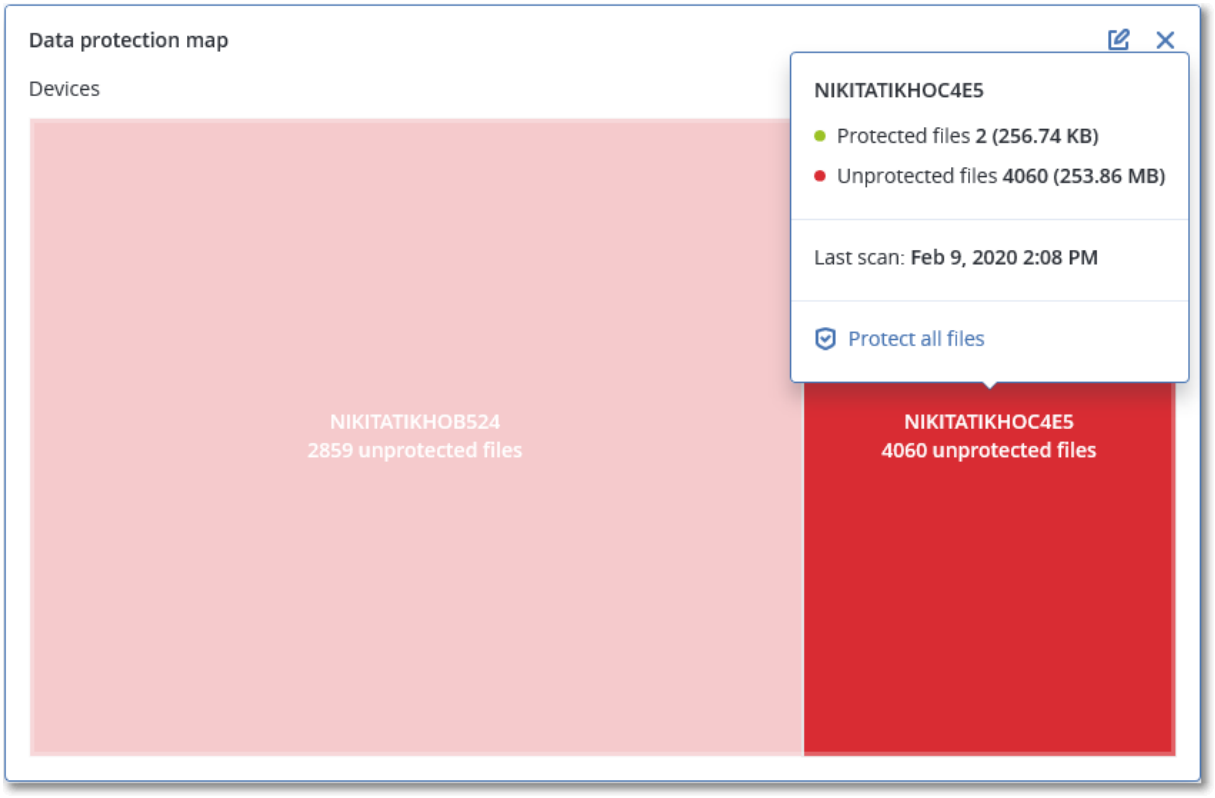
- **심각** – 선택한 고객 테넌트/머신/위치에 대해 백업되지 않도록 사용자가 지정한 확장자를 가진 파일 중 보호되지 않는 파일이 51~100%인 경우
- **낮음** – 선택한 고객 테넌트/머신/위치에 대해 백업되지 않도록 사용자가 지정한 확장자를 가진 파일 중 보호되지 않는 파일이 21~50%인 경우
- **중간** – 선택한 고객 테넌트/머신/위치에 대해 백업되지 않도록 사용자가 지정한 확장자를 가진 파일 중 보호되지 않는 파일이 1~20%인 경우
- **높음** – 선택한 고객 테넌트/머신/위치에 대해 백업되지 않도록 사용자가 지정한 확장자를 가진 모든 파일이 보호되고 있는 경우

데이터 보호 조사 결과는 트리맵 구조로 이루어져 있으며 드릴다운을 통해 2가지 세부 정보를 전환하며 확인할 수 있는 데이터 보호 맵 위젯에서 확인할 수 있습니다.

- 고객 테넌트 수준 – 선택한 고객별로 중요한 파일의 보호 상태에 대한 요약 정보를 표시합니다.



- 머신 수준 – 선택한 고객의 머신별로 중요한 파일의 보호 상태에 대한 요약 정보를 표시합니다.



보호되지 않는 파일을 보호하려면 블록을 마우스로 가리킨 다음 **모든 파일 보호**를 클릭합니다. 대화창에서 보호되지 않는 파일의 수와 해당 파일의 위치와 같은 정보를 확인할 수 있습니다. 이러한 파일을 보호하려면 **모든 파일 보호**를 클릭합니다.

상세 보고서를 CSV 형식으로 다운로드할 수도 있습니다.

취약성 평가 위젯

취약한 머신

이 위젯은 취약한 머신을 취약성 심각도에 따라 표시합니다.

CVSS(일반 취약성 점수 시스템) v3.0에 따라 취약성의 심각도 수준은 다음으로 나누어집니다.

- 보안됨: 발견된 취약성 없음
- 심각: 9.0 - 10.0 CVSS
- 높음: 7.0 - 8.9 CVSS
- 중간: 4.0 - 6.9 CVSS
- 낮음: 0.1 - 3.9 CVSS
- 없음: 0.0 CVSS

기존 취약성

이 위젯은 머신에 현재 존재하는 취약성을 표시합니다. **기존 취약성** 위젯에는 타임 스탬프를 보여주는 두 개의 열이 있습니다.

- **첫 번째로 감지됨** – 머신에서 처음으로 취약성이 감지된 날짜와 시간입니다.
- **마지막으로 감지됨** – 머신에서 마지막으로 취약성이 감지된 날짜와 시간입니다.

Existing vulnerabilities

Machine name	Vendor	Product	Vulnerability name/ID	Severity	Last detected	First detected
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-7096	Critical	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0856	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0688	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0739	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0752	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0753	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0806	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0810	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0812	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0829	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM

More

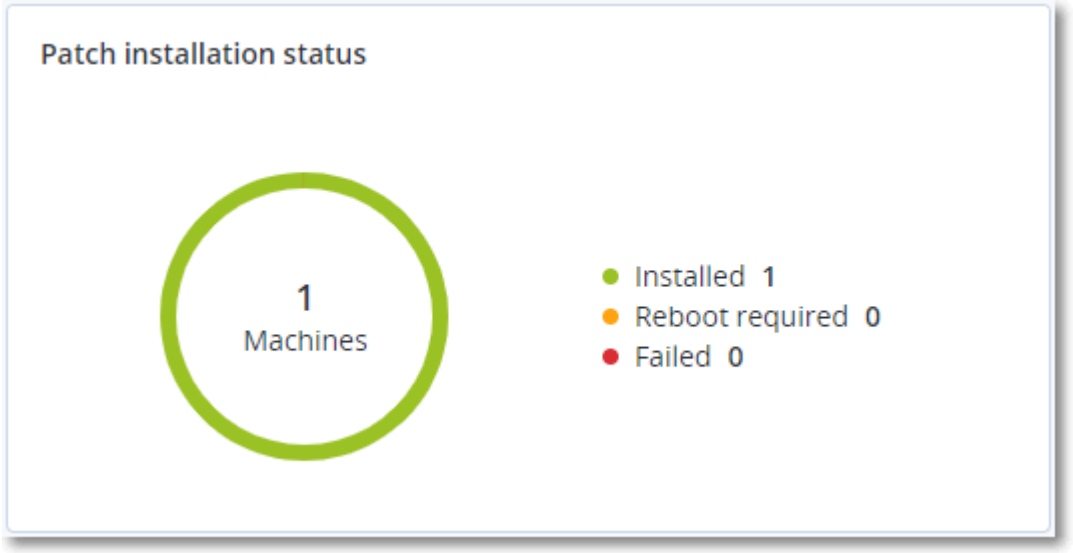
패치 설치 위젯

패치 설치 기능과 관련된 위젯은 4개입니다.

패치 설치 상태

이 위젯은 패치 설치 상태별로 그룹화된 머신 수를 표시합니다.

- **설치됨** – 사용 가능한 모든 패치가 머신에 설치되어 있음
- **재부팅 필요** – 패치 설치 후 재부팅이 필요한 머신
- **실패** – 머신에 패치 설치 실패



패치 설치 요약

이 위젯은 머신의 패치 내역을 패치 설치 상태로 요약하여 표시합니다.

Patch installation summary

Installation status	Total number of machines	Total number of updates	Microsoft updates	Application updates	Critical severity	High severity	Medium severity
Installed	1	2	1	1	2	0	0

패치 설치 내역

이 위젯은 머신의 패치에 대한 자세한 정보를 표시합니다.

Patch installation history

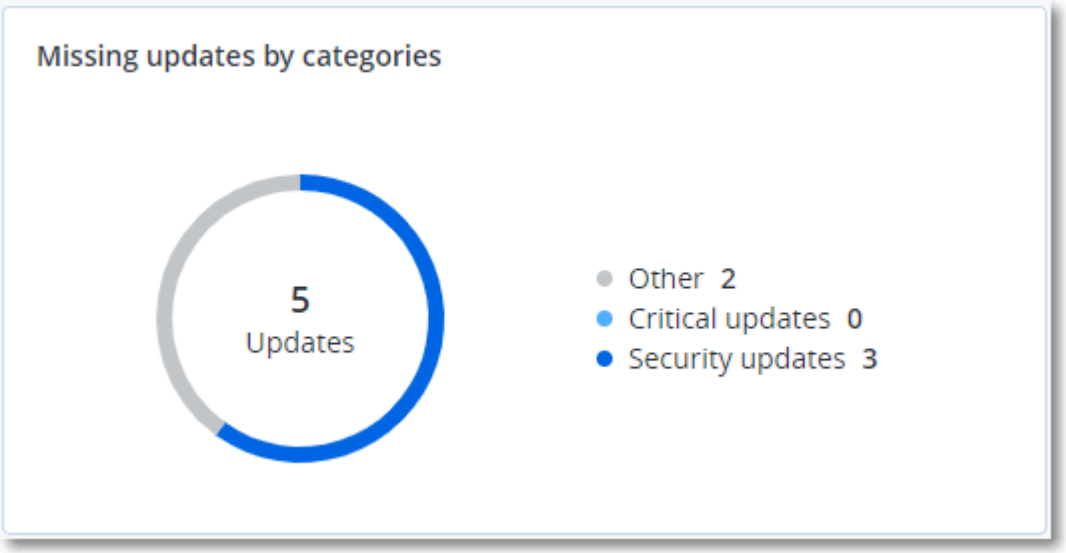
Machine name	Update name	Version	Severity	Approval status	Installation status	Installation date
NIKITATIKHOC4E5	FastStone Soft FastStone I...	5.9	Medium	New	Installed	02/05/2020
NIKITATIKHOB524	Mozilla Firefox	72.0.1	Critical	Approved	Failed	02/04/2020
NIKITATIKHOB524	Mozilla Firefox	72.0.1	Critical	Approved	Installed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Failed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Installed	02/04/2020
NIKITATIKHOC4E5	Oracle Java Runtime Envir...	8.0.2410.7	High	New	Failed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Installed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Installed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Failed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Failed	02/04/2020

More

카테고리별 누락 업데이트

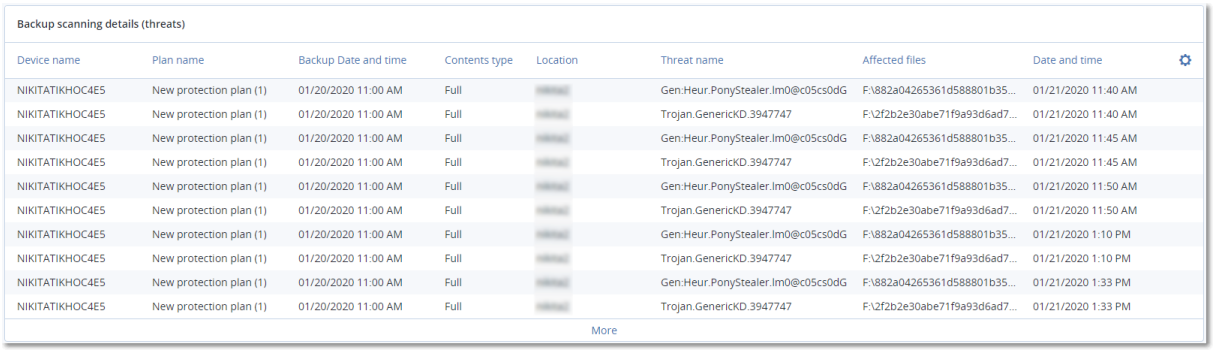
이 위젯은 카테고리별 누락 업데이트의 수를 표시합니다. 다음과 같은 카테고리가 표시됩니다.

- 보안 업데이트
- 중요 업데이트
- 기타



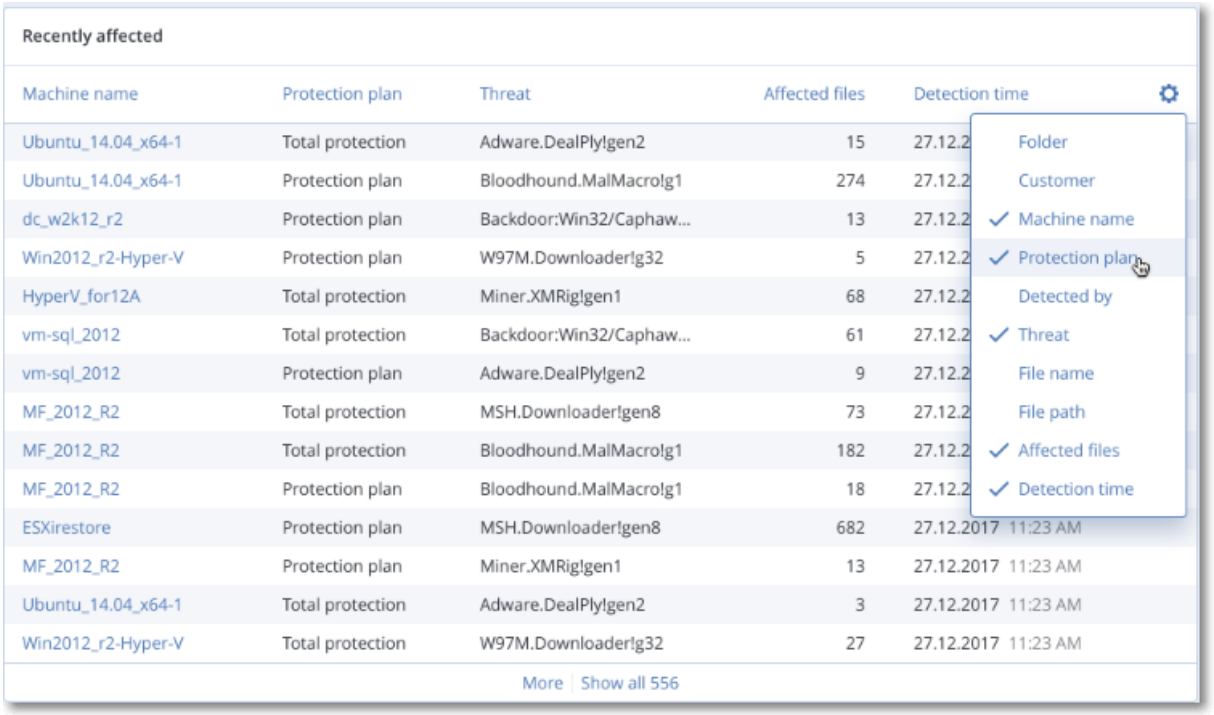
백업 스캔 세부 정보

이 위젯은 백업에서 감지된 위협에 대한 자세한 정보를 표시합니다.



최근 영향 받은 항목

이 위젯에는 바이러스, 맬웨어 및 랜섬웨어 같은 위협으로부터 영향을 받은 워크로드에 대한 자세한 정보가 표시됩니다. 여기서 감지된 위협, 위협이 감지된 시기 그리고 감염된 파일 수에 대한 정보를 확인할 수 있습니다.



최근 영향 받은 워크로드 관련 데이터 다운로드

최근 영향 받은 워크로드 관련 데이터를 다운로드하고, CSV 파일을 생성하고, 지정한 받는 사람에게 보낼 수 있습니다.

최근 영향 받은 워크로드 관련 데이터를 다운로드하려면

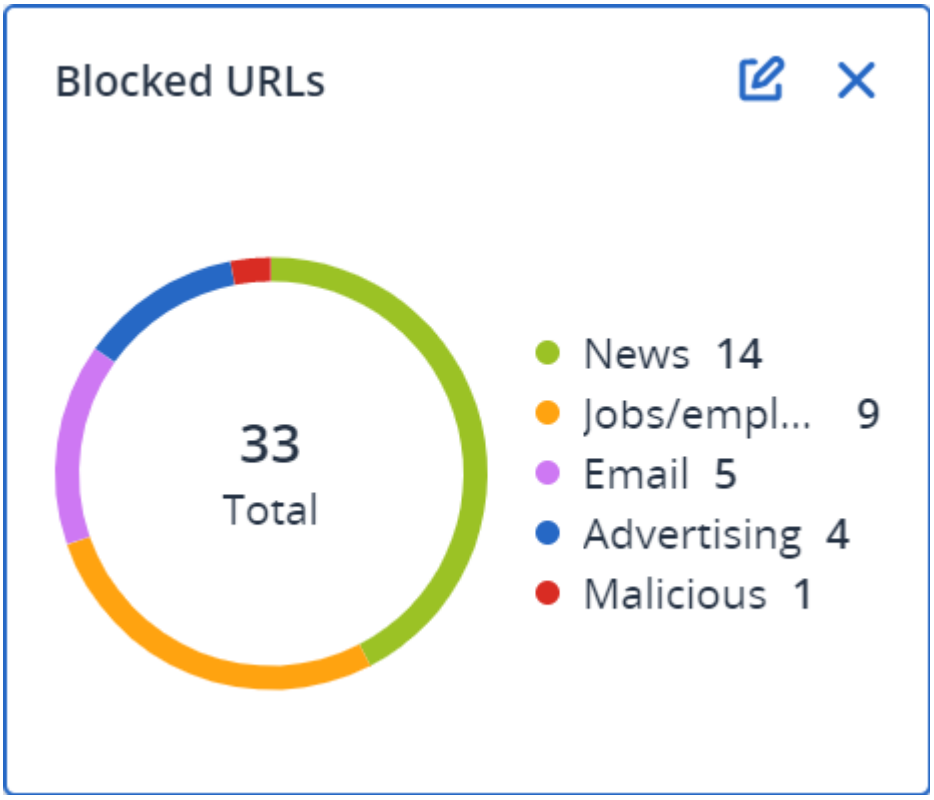
1. **최근 영향 받은 항목** 위젯에서 **데이터 다운로드**를 클릭합니다.
2. **기간** 필드에 데이터를 다운로드하려는 일수를 입력합니다. 입력할 수 있는 최대 일수는 200일입니다.
3. **받는 사람** 필드에 CSV 파일 다운로드 링크가 포함된 이메일을 받을 모든 사람의 이메일 주소를 입력합니다.

4. **다운로드**를 클릭합니다.

   시스템에서 지정한 기간 동안 영향을 받은 워크로드 관련 데이터가 포함된 CSV 파일을 생성하기 시작합니다. CSV 파일이 완성되면 시스템에서는 받는 사람에게 이메일을 보냅니다. 그러면 각각의 받는 사람이 CSV 파일을 다운로드할 수 있습니다.

차단된 URL

위젯에 차단된 URL의 통계가 카테고리별로 나타납니다. URL 필터링 및 분류에 대한 추가 정보는 사이버 보호 사용자 안내서를 참조하십시오.



소프트웨어 인벤토리 위젯

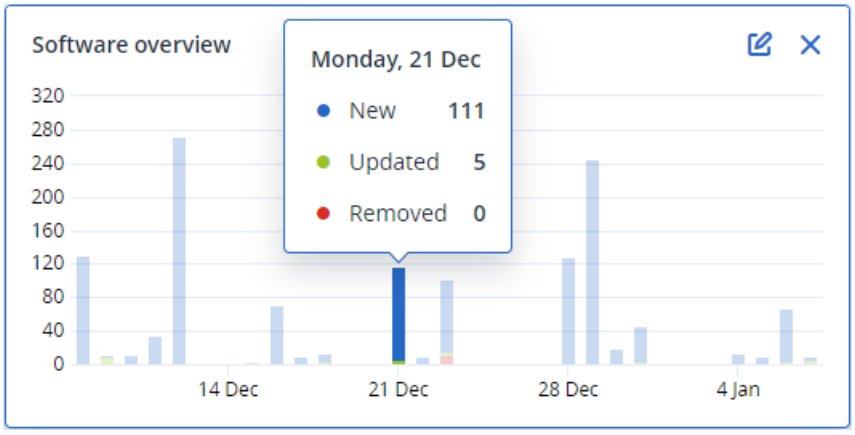
소프트웨어 인벤토리 표 위젯은 클라이언트 조직의 Windows 및 macOS 장치에 설치된 모든 소프트웨어에 대한 자세한 정보를 표시합니다.

Software inventory

Folder name	Customer name	Machine name	Software name	Software version	Vendor name	Status	Date installed	Last run	Scan time	Location	User	System type
ACP-QAZ03-A01												
ACP-QAZ03-A01												
ACP-QAZ03-A03												
folder1	rbarf4	ACP-QAZ03-A03	Microsoft Visual C...	9.0.30729.6161	Microsoft Corpora...	New	-	-	11/28/2020, 11:39 ...	-	System	X86
folder1	rbarf4	ACP-QAZ03-A03	Cyber Protect Agent	15.0.25965	Acronis	New	-	-	11/28/2020, 11:39 ...	-	System	X64
folder1	rbarf4	ACP-QAZ03-A03	Cyber Protect Agent	15.0.25965	Acronis	New	-	-	11/28/2020, 11:39 ...	C:\Program Files\B...	System	X64
folder1	rbarf4	ACP-QAZ03-A03	Mozilla Firefox	45.0.1	Mozilla	New	-	-	11/28/2020, 11:39 ...	C:\Program Files\...	System	X64
folder1	rbarf4	ACP-QAZ03-A03	Mozilla Maintenan...	45.0.1	Mozilla	New	-	-	11/28/2020, 11:39 ...	-	System	X86
folder1	rbarf4	ACP-QAZ03-A03	VMware Tools	10.0.6.3560309	VMware, Inc.	New	-	-	11/28/2020, 11:39 ...	C:\Program Files\V...	System	X64
ACP-QAZ03-A04												
folder1	rbarf4	ACP-QAZ03-A04	Google Chrome	79.0.3945.130	Google LLC	New	-	-	11/28/2020, 2:49 PM	C:\Program Files (x...	System	X86
folder1	rbarf4	ACP-QAZ03-A04	Google Update He...	1.3.36.31	Google LLC	New	-	-	11/28/2020, 2:49 PM	-	System	X86
folder1	rbarf4	ACP-QAZ03-A04	Microsoft Visual C...	9.0.30729.6161	Microsoft Corpora...	New	-	-	11/28/2020, 2:49 PM	-	System	X86
folder1	rbarf4	ACP-QAZ03-A04	Cyber Protect Agent	15.0.25965	Acronis	New	-	-	11/28/2020, 2:49 PM	-	System	X64
folder1	rbarf4	ACP-QAZ03-A04	Cyber Protect Agent	15.0.25965	Acronis	New	-	-	11/28/2020, 2:49 PM	C:\Program Files\B...	System	X64
folder1	rbarf4	ACP-QAZ03-A04	Notepad++	6.7.4	Notepad++ Team	New	-	-	11/28/2020, 2:49 PM	-	System	X86
folder1	rbarf4	ACP-QAZ03-A04	Microsoft OneDrive	20.201.1005.0009	Microsoft Corpora...	New	-	-	11/28/2020, 2:49 PM	-	System	X86
folder1	rbarf4	ACP-QAZ03-A04	Mozilla Firefox	45.0.1	Mozilla	New	-	-	11/28/2020, 2:49 PM	C:\Program Files\...	System	X64
folder1	rbarf4	ACP-QAZ03-A04	Mozilla Maintenan...	45.0.1	Mozilla	New	-	-	11/28/2020, 2:49 PM	-	System	X86
folder1	rbarf4	ACP-QAZ03-A04	Microsoft Update ...	2.68.0.0	Microsoft Corpora...	New	-	-	11/28/2020, 2:49 PM	-	System	X64
folder1	rbarf4	ACP-QAZ03-A04	VMware Tools	10.0.6.3560309	VMware, Inc.	New	-	-	11/28/2020, 2:49 PM	C:\Program Files\V...	System	X64

More | Less | Show 1000+

소프트웨어 개요 위젯은 클라이언트 조직의 Windows 및 macOS 장치에서 지정된 기간(7일, 30일 또는 현재 월) 동안 새로 설치, 업데이트 및 삭제된 애플리케이션의 수를 표시합니다.



차트의 특정 막대를 마우스로 가리키면 다음 정보가 포함된 툴팁이 표시됩니다.

신규 - 새로 설치된 애플리케이션의 수입니다.

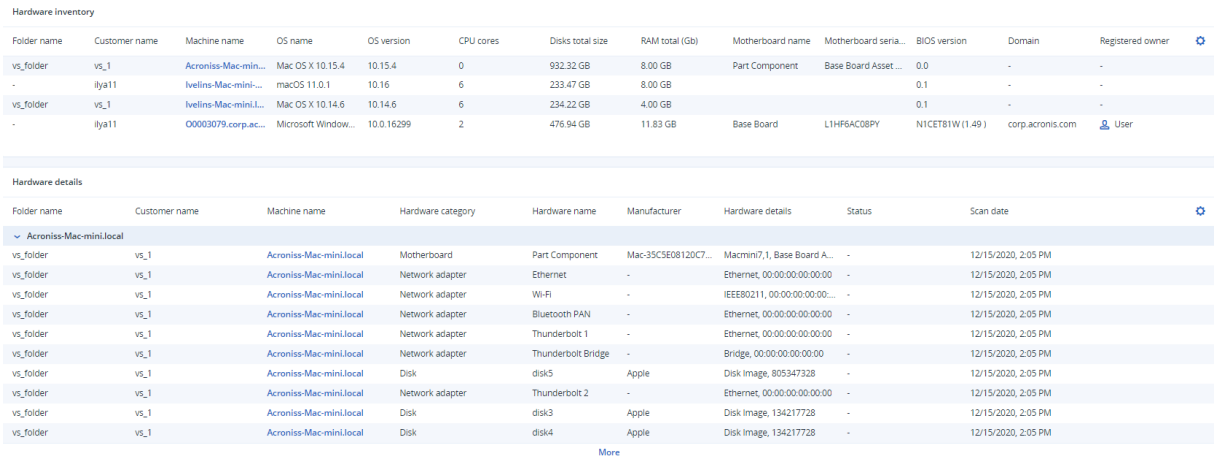
업데이트됨 - 업데이트된 애플리케이션의 수입니다.

제거됨 - 제거된 애플리케이션의 수입니다.

특정 상태에 해당하는 막대의 일부를 클릭하면 팝업 창이 로드됩니다. 이 창에는 선택한 날짜에 선택한 상태의 애플리케이션이 설치되어 있는 장치를 보유한 모든 고객이 나열됩니다. 목록에서 고객을 선택하고 **고객으로 이동**을 클릭하면 고객 콘솔의 **소프트웨어 관리** -> **소프트웨어 인벤토리** 페이지로 리디렉션됩니다. 페이지의 정보는 해당하는 날짜 및 상태에 따라 필터링됩니다.

하드웨어 인벤토리 위젯

하드웨어 인벤토리 및 **하드웨어 상세 정보** 표 위젯은 클라이언트 조직의 물리적 및 가상 Windows 및 macOS 장치에 설치된 모든 하드웨어에 대한 정보를 표시합니다.



Hardware inventory

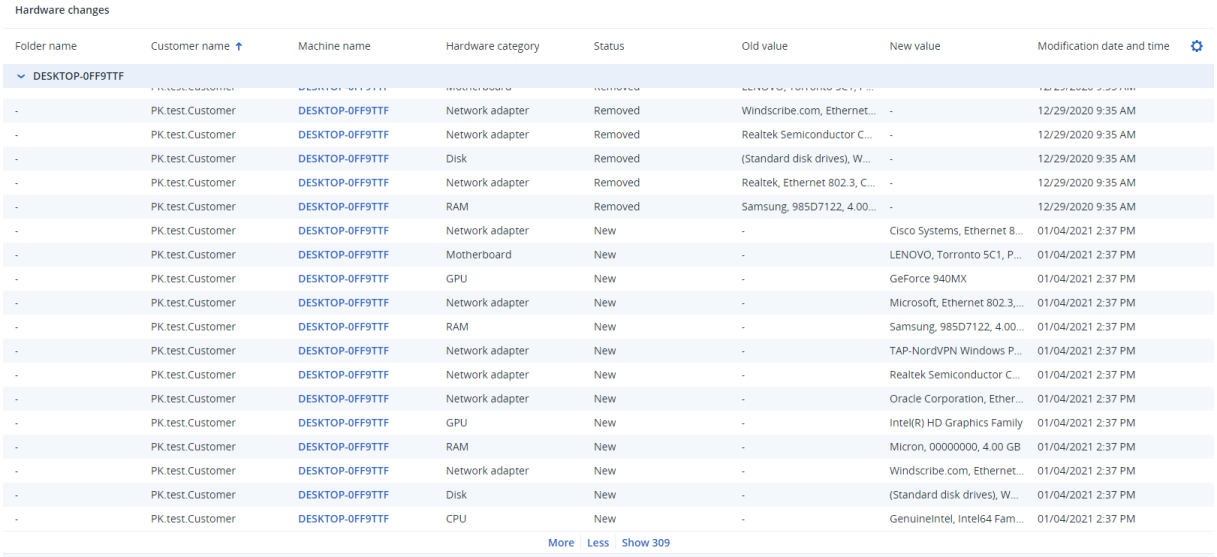
Folder name	Customer name	Machine name	OS name	OS version	CPU cores	Disks total size	RAM total (Gb)	Motherboard name	Motherboard seria...	BIOS version	Domain	Registered owner
vs_folder	vs_1	Acroniss-Mac-min...	Mac OS X 10.15.4	10.15.4	0	932.32 GB	8.00 GB	Part Component	Base Board Asset ...	0.0	-	-
-	ilya11	Ivelins-Mac-mini-...	macOS 11.0.1	10.16	6	233.47 GB	8.00 GB			0.1	-	-
vs_folder	vs_1	Ivelins-Mac-mini.l...	Mac OS X 10.14.6	10.14.6	6	234.22 GB	4.00 GB			0.1	-	-
-	ilya11	O0003079.corp.ac...	Microsoft Window...	10.0.16299	2	476.94 GB	11.83 GB	Base Board	L1HF6AC08PY	N1CET81W (1.49)	corp.acronis.com	User

Hardware details

Folder name	Customer name	Machine name	Hardware category	Hardware name	Manufacturer	Hardware details	Status	Scan date
Acroniss-Mac-mini.local								
vs_folder	vs_1	Acroniss-Mac-mini.local	Motherboard	Part Component	Mac-35C5E08120C7...	Macmini7,1, Base Board A...	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Network adapter	Ethernet	-	Ethernet, 00:00:00:00:00:00	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Network adapter	Wi-Fi	-	IEEE80211, 00:00:00:00:00:...	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Network adapter	Bluetooth PAN	-	Ethernet, 00:00:00:00:00:00	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Network adapter	Thunderbolt 1	-	Ethernet, 00:00:00:00:00:00	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Network adapter	Thunderbolt Bridge	-	Bridge, 00:00:00:00:00:00	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Disk	disk5	Apple	Disk Image, 805347328	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Network adapter	Thunderbolt 2	-	Ethernet, 00:00:00:00:00:00	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Disk	disk3	Apple	Disk Image, 134217728	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Disk	disk4	Apple	Disk Image, 134217728	-	12/15/2020, 2:05 PM

More

하드웨어 변경 표 위젯은 클라이언트 조직의 물리적 및 가상 Windows 및 macOS 장치에서 지정된 기간(7일, 30일 또는 현재 월) 동안 추가, 제거 및 변경된 하드웨어에 대한 정보를 표시합니다.



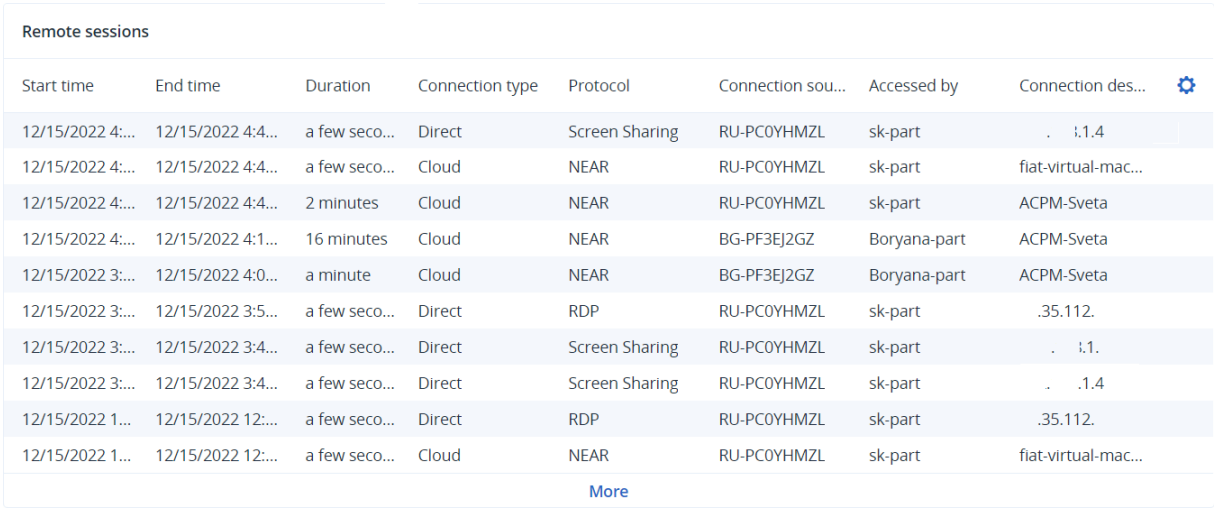
Hardware changes

Folder name	Customer name	Machine name	Hardware category	Status	Old value	New value	Modification date and time
DESKTOP-0FF9TTF							
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	Removed	Windscribe.com, Ethernet...	-	12/29/2020 9:35 AM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	Removed	Realtek Semiconductor C...	-	12/29/2020 9:35 AM
-	PK.test.Customer	DESKTOP-0FF9TTF	Disk	Removed	(Standard disk drives), W...	-	12/29/2020 9:35 AM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	Removed	Realtek, Ethernet 802.3, C...	-	12/29/2020 9:35 AM
-	PK.test.Customer	DESKTOP-0FF9TTF	RAM	Removed	Samsung, 985D7122, 4.00...	-	12/29/2020 9:35 AM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	New	-	Cisco Systems, Ethernet 8...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	Motherboard	New	-	LENOVO, Torronto 5C1, P...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	GPU	New	-	GeForce 940MX	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	New	-	Microsoft, Ethernet 802.3,...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	RAM	New	-	Samsung, 985D7122, 4.00...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	New	-	TAP-NordVPN Windows P...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	New	-	Realtek Semiconductor C...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	New	-	Oracle Corporation, Ether...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	GPU	New	-	Intel(R) HD Graphics Family	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	RAM	New	-	Micron, 00000000, 4.00 GB	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	New	-	Windscribe.com, Ethernet...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	Disk	New	-	(Standard disk drives), W...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	CPU	New	-	GenuineIntel, Intel64 Fam...	01/04/2021 2:37 PM

More | Less | Show 309

세션 내역

이 위젯에는 지정된 기간 동안 클라이언트 조직에서 수행한 원격 데스크탑 및 파일 전송 세션의 자세한 정보가 표시됩니다.



감사 로그

감사 로그는 다음 이벤트에 대한 기록을 시간 순서대로 제공합니다.

- 관리 포털에서 사용자가 수행한 작업
- Cyber Protect 콘솔에서 사용자가 수행한 클라우드 간 리소스 작업
- Cyber Protect 콘솔에서 사용자가 수행한 Cyber Scripting 작업
- 도달한 할당량 및 할당량 사용에 대한 시스템 메시지

이 로그는 사용자가 현재 작업 중인 테넌트 및 하위 테넌트의 이벤트를 보여줍니다. 이벤트를 클릭하면 자세한 내용을 볼 수 있습니다.

감사 로그는 데이터 센터에 저장되며 로그의 가용성은 최종 사용자 머신의 문제로 인해 영향 받지 않습니다.

로그는 일일 기준으로 정리됩니다. 이벤트는 180일 후 제거됩니다.

감사 로그 필드

각 이벤트에서 로그는 다음을 보여줍니다.

- **이벤트**
  이벤트에 대한 간단한 설명입니다. 예: **테넌트가 생성됨**, **테넌트가 삭제됨**, **사용자가 생성됨**, **사용자가 삭제됨**, **할당량에 도달함**, **백업 내용이 검색됨**, **스크립트가 변경됨**.
- **심각도**
  다음 중 하나일 수 있습니다.
  - **오류**
    오류를 나타냅니다.
  - **경고**
    잠재적으로 부정적인 동작을 나타냅니다. 예를 들어, **테넌트가 삭제됨**, **사용자가 삭제됨**, **할당량에 도달함**.
  - **고지 사항**

주의가 필요할 수 있는 이벤트를 나타냅니다. 예를 들어, **테넌트가 업데이트됨**, **사용자가 업데이트됨**.

  - **정보**

    참고로 알려주는 변경 또는 동작을 나타냅니다. 예: **테넌트가 생성됨**, **사용자가 생성됨**, **할당량이 업데이트됨**, **스크립팅 계획이 삭제됨**.

- **날짜**

  이벤트가 발생한 날짜 및 시간.

- **객체 이름**

  작업 수행에 함께 사용된 객체입니다. 예를 들어, **사용자가 업데이트됨** 이벤트의 객체는 속성이 변경된 사용자입니다. 할당량과 관련된 이벤트의 경우 할당량이 객체입니다.

- **테넌트**

  객체가 속한 테넌트의 이름입니다.

- **시작자**

  이벤트를 시작하는 사용자의 로그인입니다. 상위 레벨 관리자가 시작한 시스템 메시지 및 이벤트의 경우 시작자가 **시스템**으로 표시됩니다.

- **시작자 테넌트**

  시작자가 속한 테넌트의 이름입니다. 상위 레벨 관리자가 시작한 시스템 메시지 및 이벤트의 경우 이 필드가 비어있습니다.

- **방법**

  이벤트가 웹 인터페이스나 API를 통해 시작되었는지 표시합니다.

- **IP**

  이벤트가 시작된 머신의 IP 주소

필터링 및 검색

유형, 심각도 또는 날짜를 기준으로 이벤트를 필터링할 수 있습니다. 이름, 객체, 테넌트, 시작자 및 시작자 테넌트로 이벤트를 검색할 수도 있습니다.

보고 중

서비스 사용 및 작업에 대한 보고서를 생성하려면 **보고서**를 클릭합니다.

사용

사용 보고서는 서비스 사용에 대한 기록 데이터를 제공합니다. 사용 보고서는 CSV 및 HTML 형식으로 제공됩니다.

보고서 유형

다음 보고서 유형 중 하나를 선택합니다.

- **현재 사용량**

  보고서에 현재 서비스 사용 메트릭이 포함됩니다.

사용 메트릭은 각 하위 테넌트의 청구 기간 내에서 계산됩니다. 보고서에 포함된 여러 테넌트의 청구 기간이 서로 다른 경우 상위 테넌트 사용량은 하위 테넌트 사용량의 합과 다를 수 있습니다.

- **현재 사용량 분포**
  이 보고서는 외부 프로비저닝 시스템에서 관리하는 상위 테넌트에 대해서만 사용할 수 있습니다. 이 보고서는 자식 테넌트의 청구 기간이 부모 테넌트의 청구 기간과 일치하지 않는 경우 유용합니다. 보고서에 부모 테넌트의 현재 청구 기간 내에 계산된 자식 테넌트의 서비스 사용 메트릭이 포함됩니다. 부모 테넌트의 사용량은 자식 테넌트의 사용량을 합한 것과 동일합니다.
- **기간 동안 요약**
  보고서에 지정된 기간 종료 시점의 서비스 사용 메트릭, 그리고 지정된 기간의 시작 시점과 종료 시점 간 메트릭 차이가 포함됩니다.
- **기간 동안 매일**
  보고서에 지정된 기간 동안의 서비스 사용 메트릭, 그리고 각 날짜별 변경 정보가 포함됩니다.

리포트 범위

다음 값에서 리포트의 범위를 선택할 수 있습니다.

- **직접 고객 및 파트너**
  보고서에 현재 운영 중인 테넌트의 직속 하위 테넌트에 대한 서비스 사용 메트릭만 포함됩니다.
- **모든 고객 및 파트너**
  보고서에 현재 운영 중인 테넌트의 모든 하위 테넌트에 대한 서비스 사용 메트릭이 포함됩니다.
- **모든 고객 및 파트너(사용자 세부정보 포함)**
  보고서에 현재 운영 중인 테넌트의 모든 하위 테넌트를 비롯하여 테넌트 내 모든 사용자에 대한 서비스 사용 메트릭이 포함됩니다.

사용량이 0인 메트릭

사용량이 0이 아닌 메트릭 관련 정보는 표시하고 사용량이 0인 메트릭 관련 정보는 숨기면 보고서의 행 수를 줄일 수 있습니다.

예약된 사용 보고서 구성

예약된 보고서는 지난 달 전체에 대한 서비스 사용 메트릭을 보고합니다. 보고서는 해당 월의 첫 번째 날 23:59:59(UTC)에 생성되어 해당 월의 두 번째 날 전송됩니다.보고서는 사용자 설정에서 선택한 **예약된 사용 보고서**확인란이 있는 테넌트의 모든 관리자에게 전송됩니다.

참고
날짜별 필터링은 작업 시작 또는 완료 시간이 아닌 클라우드에 이벤트가 제출된 타임 스탬프를 기준으로 수행됩니다. 그러므로 서버 연결이 중단된 경우 일일 보고서에 여러 날짜의 데이터가 포함될 수 있습니다.

예약된 보고서를 활성화하거나 비활성화하려면

1. 관리 포털에 로그인합니다.
2. 사용 가능한 최상위 테넌트에서 운영하는지 확인하십시오.
3. **보고서** > **사용법**을 클릭합니다.
4. **예약됨**을 클릭합니다.
5. **월별 요약 보고서 전송** 확인란을 선택하거나 선택 취소합니다.
6. **세부정보 수준**에서 보고서 범위를 선택합니다.
7. [선택 사항] 보고서에서 사용량이 0인 메트릭은 제외하려면 **사용량이 0인 메트릭 숨기기**를 선택합니다.

사용자 정의 사용 보고서 구성

이 유형의 리포트는 요청 시 생성할 수 있으며 예약할 수 없습니다. 이 리포트는 사용자의 이메일 주소로 전송됩니다.

사용자 정의 보고서를 생성하려면

1. 관리 포털에 로그인합니다.
2. 보고서를 생성하려는 테넌트로 이동합니다.
3. **보고서** > **사용법**을 클릭합니다.
4. **사용자 정의** 탭을 선택합니다.
5. **유형**에서 위에 설명된 대로 보고서 유형을 선택합니다.
6. [**현재 사용량** 보고서 유형에 사용할 수 없음] **기간**에서 보고 기간을 선택합니다.
   - **현재 월(달력 기준)**
   - **지난 월(달력 기준)**
   - **사용자 정의**
7. [**현재 사용량** 보고서 유형에 사용할 수 없음] 사용자 정의 보고 기간을 지정하고 싶다면 시작 및 종료 날짜를 선택합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
8. **세부정보 수준**에서 위에 설명된 대로 보고서 범위를 선택합니다.
9. [선택 사항] 보고서에서 사용량이 0인 메트릭은 제외하려면 **사용량이 0인 메트릭 숨기기**를 선택합니다.
10. 보고서를 생성하려면 **생성 및 보내기**를 클릭합니다.

동작 보고서

작업 보고서에는 **작업** 대시보드 위젯 집합이 포함될 수 있습니다. 기본적으로 모든 위젯에는 사용자가 운영 중인 테넌트에 대한 요약 정보가 표시됩니다. 해당 위젯을 편집하여 각 위젯에 대해 개별적으로 변경하거나 보고서 설정의 모든 위젯에 대해 변경할 수 있습니다.

위젯 유형에 따라 보고서에는 특정 시간 범위의 데이터가 포함될 수도 있고, 보고서 찾아보기 또는 생성 시점의 데이터가 포함될 수도 있습니다. "위젯 유형에 따라 보고된 데이터"(113페이지)을(를) 참조하십시오.

모든 이력 위젯에는 같은 시간 범위의 데이터가 표시됩니다. 보고서 설정에서 이 범위를 변경할 수 있습니다.

기본 보고서를 사용하거나 사용자 정의 보고서를 생성할 수 있습니다.

XLSX(Excel) 또는 PDF 형식 보고서를 다운로드하거나 이메일로 전송할 수 있습니다.

기본 보고서에 포함되어 있는 항목:

보고서 이름	설명
머신별 #CyberFit Score	각 머신의 보안 메트릭 평가 및 구성에 기반한 #CyberFit Score와 개선을 위한 권장 사항을 보여줍니다.
경보	지정된 기간 동안 발생한 경보를 표시합니다.
백업 스캔 세부 정보	백업에서 감지된 위협에 대한 자세한 정보를 표시합니다.
일일 작업	지정된 기간 동안 수행된 작업에 대한 요약 정보를 표시합니다.
데이터 보호 맵	머신에 있는 모든 중요 파일의 수, 크기, 위치, 보호 상태에 대한 자세한 정보를 표시합니다.
감지된 위협	차단된 위협, 양호한 머신 및 취약한 머신의 수를 통해 감염된 머신에 대한 자세한 정보를 표시합니다.
검색된 머신	조직 네트워크에서 발견된 모든 머신의 목록을 표시합니다.
디스크 상태 예측	HDD/SDD가 고장나게 되는 예상 시기와 현재 디스크 상태를 표시합니다.
기존 취약성	조직 OS 및 애플리케이션에 이미 존재하는 취약성의 목록을 보여줍니다. 이 보고서는 나열된 모든 제품과 관련하여 네트워크 내에서 영향을 받는 머신에 대한 상세 정보도 표시합니다.
패치 관리 요약	누락된 패치, 설치된 패치, 적용 가능한 패치의 수를 목록으로 보여줍니다. 이 보고서를 자세히 살펴보면 모든 시스템의 상세 정보 및 누락/설치된 패치 정보를 확인할 수 있습니다.
요약	지정된 기간 동안 보호되는 장치에 대한 요약 정보를 표시합니다.
주간 작업	지정된 기간 동안 수행된 작업에 대한 요약 정보를 표시합니다.
소프트웨어 인벤토리	클라이언트 조직의 Windows 및 macOS 머신에 설치된 모든 소프트웨어에 대한 자세한 정보를 표시합니다.
하드웨어 인벤토리	클라이언트 조직의 물리적 및 가상 Windows 및 macOS 머신에서 사용할 수 있는 모든 하드웨어에 대한 자세한 정보를 표시합니다.
원격 세션	지정된 기간 동안 클라이언트 조직에서 수행한 원격 데스크탑 및 파일 전송 세션의 자세한 정보를 표시합니다.

보고서 관련 작업

보고서를 보려면 보고서 이름을 클릭합니다.

새 보고서를 추가하려면

1. Cyber Protect 콘솔에서 **보고서**로 이동합니다.
2. 사용 가능한 보고서 목록에서 **보고서 추가**를 클릭합니다.
3. [사전 정의된 보고서를 추가하려는 경우] 사전 정의된 보고서 이름을 클릭합니다.
4. [사용자 정의 보고서를 추가하려는 경우] **사용자 정의**를 클릭하고 보고서에 위젯을 추가합니다.
5. [선택 사항] 위젯을 끌어서 놓아 재정렬합니다.

보고서를 편집하는 방법

1. Cyber Protect 콘솔에서 **보고서**로 이동합니다.
2. 보고서 목록에서 편집할 보고서를 선택합니다.
   수행할 수 있는 작업은 다음과 같습니다.
   - 보고서 이름 변경
   - 보고서 내 모든 위젯의 시간 범위 변경
   - 보고서 수신인 및 수신인에게 보고서를 전송할 시간 지정 사용 가능한 형식은 PDF와 XLSX입니다.

보고서를 삭제하려면

1. Cyber Protect 콘솔에서 **보고서**로 이동합니다.
2. 보고서 목록에서 삭제할 보고서를 선택합니다.
3. 말줄임표 아이콘(...)을 클릭한 후에 **삭제**를 클릭합니다.
4. **삭제**를 클릭하여 선택을 확인합니다.

보고서를 예약하는 방법

1. Cyber Protect 콘솔에서 **보고서**로 이동합니다.
2. 보고서 목록에서 예약할 보고서를 선택하고 **설정**을 클릭합니다.
3. **예약된** 스위치를 활성화합니다.
   - 수신인의 이메일 주소를 지정합니다.
   - 보고서의 형식을 선택합니다.

     참고
     PDF 파일 하나에서는 항목을 1,000개까지, XLSX 파일 하나에서는 항목을 10,000개까지 내보낼 수 있습니다. PDF 및 XLSX 파일의 타임 스탬프에는 머신의 로컬 시간이 사용됩니다.

   - 보고서의 언어를 선택합니다.
   - 일정을 구성합니다.
4. **저장**을 클릭합니다.

보고서를 다운로드하려면

1. Cyber Protect 콘솔에서 **보고서**로 이동합니다.
2. 보고서 목록에서 보고서를 선택하고 **다운로드**를 클릭합니다.
3. 보고서의 형식을 선택합니다.

보고서를 전송하려면

1. Cyber Protect 콘솔에서 **보고서**로 이동합니다.
2. 보고서 목록에서 보고서를 선택하고 **전송**을 클릭합니다.
3. 수신인의 이메일 주소를 지정합니다.
4. 보고서의 형식을 선택합니다.
5. **보내기**를 클릭합니다.

보고서 구조를 내보내려면

1. Cyber Protect 콘솔에서 **보고서**로 이동합니다.
2. 보고서 목록에서 보고서를 선택합니다.
3. 말줄임표 아이콘(...)을 클릭한 후에 **내보내기**를 클릭합니다.

그러면 보고서 구조가 머신에 JSON 파일로 저장됩니다.

보고서 데이터를 덤프하려면

이 옵션을 사용하면 사용자 정의 기간 동안의 모든 데이터를 필터링하지 않고 CSV 파일로 내보낸 다음 이메일 수신인에게 해당 CSV 파일을 전송할 수 있습니다.

참고
CSV 파일 하나에서 항목을 150,000개까지 내보낼 수 있습니다. CSV 파일의 타임 스탬프에는 UTC (Coordinated Universal Time)가 사용됩니다.

1. Cyber Protect 콘솔에서 **보고서**로 이동합니다.
2. 보고서 목록에서 데이터를 덤프할 보고서를 선택합니다.
3. 말줄임표 아이콘(...)을 클릭한 후에 **데이터 덤프**를 클릭합니다.
4. 수신인의 이메일 주소를 지정합니다.
5. **시간 범위**에서 데이터를 덤프할 사용자 정의 기간을 지정합니다.

   참고
   CSV 파일을 준비하는 기간이 길수록 소요 시간도 길어집니다.

6. **보내기**를 클릭합니다.

총괄 요약

총괄 요약 보고서는 특정 시간 범위에서 고객 환경의 보호 상태와 보호되는 장치에 대한 개괄을 제공합니다.

총괄 요약 보고서에는 능동적 위젯 섹션이 있어 다음과 같은 클라우드 서비스의 고객 사용과 관련된 주요 성능 메트릭을 제공합니다. 백업, 안티맬웨어 보호, 취약성 평가, 패치 관리, 데이터 손실 방지, 공증, 재해 복구, 파일 동기화 및 공유.

보고서는 다양한 방법으로 사용자 정의할 수 있습니다.

- 섹션을 추가하거나 삭제합니다.
- 섹션의 순서를 변경합니다.
- 섹션 이름을 변경합니다.

- 위젯을 한 섹션에서 다른 섹션으로 이동합니다.
- 각 섹션 내 위젯의 순서 변경.
- 위젯 추가 또는 제거.
- 위젯 사용자 정의.

총괄 요약 보고서는 PDF 혹은 엑셀 형식으로 생성한 다음 고객 조직의 소유자 혹은 이해관계인에게 송부하여 제공된 서비스의 기술적, 사업적 가치를 쉽게 확인하도록 할 수 있습니다.

파트너 관리자는 직접 고객에 대해서만 총괄 요약 보고서를 생성 및 전송할 수 있습니다. 서브 파트너가 있는 복잡한 테넌트 계층 구조인 경우에는 서브 파트너가 보고서를 생성해야 합니다.

총괄 요약 위젯

총괄 요약 보고서에 섹션이나 위젯을 추가하거나 제거하여 포함할 정보를 제어할 수 있습니다.

워크로드 개요 위젯

다음 표는 **워크로드 개요** 섹션의 위젯에 대한 자세한 정보를 제공합니다.

위젯	설명
클라우드 워크로드 보호 상태	이 위젯에는 보고서 생성 시점에 보호되는/보호되지 않는 클라우드 워크로드 수가 유형별로 표시됩니다. 보호된 클라우드 워크로드는 하나 이상의 보호 또는 백업 계획이 적용되는 클라우드 워크로드입니다. 보호되지 않는 클라우드 워크로드는 하나 이상의 보호 또는 백업 계획이 적용되지 않는 클라우드 워크로드입니다. 다음의 클라우드 워크로드 유형이 차트에 표시됩니다(A부터 Z까지 알파벳 순서). • Google Workspace Drive • Google Workspace Gmail • Google Workspace Shared Drive • Hosted Exchange 사서함 • Microsoft 365 사서함 • Microsoft 365 OneDrive • Microsoft 365 SharePoint Online • Microsoft Teams • 웹사이트 일부 워크로드 유형의 경우 다음 워크로드 그룹이 사용됩니다. • Microsoft 365: 사용자, 그룹, 공용 폴더, 팀, 사이트 모음 • Google Workspace: 사용자, 공유 드라이브 • Hosted Exchange: 사용자 하나의 워크로드 그룹에 10,000개 이상의 워크로드가 있는 경우 위젯은 해당 워크로드에 대해서는 데이터를 표시하지 않습니다. 예를 들어 고객의 Microsoft 365 계정 사서함이 10,000개이고 OneDrive 서비스의 사용자 수는 500명이라면 모든 사용자는 사용자 워크로드 그룹에 속하게 됩니다. 이 워크로드의 총 합은 10,500으로 워크로드 그룹 제한 요건인 10,000을 초과합니다. 따라서 위젯은 다음 워크로드 유형을 숨기게 됩니다. Microsoft 365 사서함, Microsoft 365

위젯	설명
	OneDrive.
사이버 보호 요약	이 위젯은 특정 기간 범위에서 사이버 보호 성능에 대한 주요 메트릭을 표시합니다. **백업된 데이터** - 클라우드 및 로컬 스토리지에 생성된 아카이브의 총 크기. **완화된 위협** - 모든 장치에서 차단된 맬웨어의 총 수. **차단된 악의적 URL** - 모든 장치에서 차단된 URL의 총 수. **패치된 취약성** - 모든 장치에서 소프트웨어 패치를 설치하여 수정한 취약점의 총 수. **설치된 패치** - 모든 장치에서 설치한 패치의 총 수입니다. **DR이 보호하는 서버** - 재해 복구가 보호하는 서버의 총 수. **File Sync & Share 사용자** - 사이버 파일을 사용하는 최종 및 게스트 사용자의 총 수. **공증된 파일** - 공증된 파일의 총 수. **전자 서명 문서** - 전자 서명된 서류의 총 수. **차단된 주변 장치** - 차단된 주변 장치의 총 수.
워크로드 네트워크 상태	이 위젯에는 분리된 워크로드 및 연결된 워크로드(워크로드의 정상 상태) 수가 표시됩니다. 관련 고객을 선택하면 표시된 워크로드 보기가 필터링되어 분리된 워크로드가 표시됩니다. 연결됨 값을 클릭하면 선택한 고객의 연결된 워크로드가 표시되도록 에이전트 목록이 필터링된 워크로드를 확인할 수 있습니다.
워크로드 보호 상태	이 위젯은 보고서 생성 시점의 유형별 보호 및 보호되지 않는 워크로드 수를 표시합니다. 보호된 워크로드는 하나 이상의 보호 또는 백업 계획이 적용된 워크로드입니다. 보호되지 않는 워크로드는 하나 이상의 보호 또는 백업 계획이 적용되지 않는 워크로드입니다. 다음 워크로드를 포함합니다. **서버** -실제 서버, 도메인 컨트롤러 서버. **워크스테이션** - 실제 워크스테이션. **가상 머신** - 에이전트 기반 및 비에이전트 가상 머신. **웹 호스팅 서버** - cPanel이나 Plesk가 설치된 가상 혹은 실제 서버. **모바일 장치** - 실제 모바일 장치. 하나의 워크로드는 하나 이상의 카테고리에 속할 수 있습니다. 예를 들어 웹 호스팅 서버는 **서버** 및 **웹 호스팅 서버** 라는 두 개의 카테고리에 해당합니다.

안티맬웨어 보호 기능 위젯

다음 표는 위협 방어 **섹션의 위젯에 대한 자세한 정보를 제공합니다.**

위젯	설명
파일의 맬웨	이 위젯은 특정한 날짜 범위에서 요청에 따른 장치의 맬웨어 방지 스캔 결과

위젯	설명
어 방지 스캔	를 보여줍니다. **파일** - 스캔한 총 파일 수 **문제 없음** - 문제가 발견되지 않은 총 파일 수 **감지됨, 격리됨** - 감염되고 격리된 총 파일 수 **감지됨, 격리되지 않음** - 감염되었지만 격리되지 않은 총 파일 수 **보호되는 장치** - 안티맬웨어 보호 정책이 적용되는 총 장치 수 **총 등록 장치 수** - 보고서 생성 시의 총 등록 장치 수
백업의 맬웨어 방지 스캔	이 위젯은 다음 메트릭을 사용하여 백업에 대한 특정한 날짜 범위의 맬웨어 방지 스캔 결과를 나타냅니다. • 스캔한 복구 지점의 총 수 • 문제 없는 복구 지점의 수 • 비지원 파티션이 있는 문제 없는 복구 지점의 수 • 감염된 복구 지점의 수. 이 메트릭은 비지원 파티션이 있는 감염된 복구 지점의 수를 포함합니다.
차단된 URL	이 위젯은 특정 날짜 범위에서 차단된 URL의 수를 웹 사이트 카테고리별로 그룹화하여 보여줍니다. 이 위젯은 차단 URL 수가 가장 많은 일곱 개의 웹 사이트 카테고리를 나열하고, 나머지 웹 사이트 카테고리는 **기타**로 통합합니다. 웹 사이트 카테고리에 대한 자세한 내용은 Cyber Protection 에 있는 URL 필터링 주제를 참조하십시오.
보안 인시던트 번다운 (Burndown)	이 위젯에는 선택한 회사의 인시던트 종료 효율이 표시됩니다. 즉, 일정 기간 동안 종료된 인시던트 수를 기준으로 하여 측정된 미해결 인시던트 수가 표시됩니다. 원하는 열을 마우스로 가리키면 선택한 날짜의 종료된 인시던트와 미해결 인시던트 세부 정보를 확인할 수 있습니다. 괄호 안에 표시되는 비율 값은 이전 기간과 비교한 증감률을 나타냅니다.
인시던트 MTTR	이 위젯에는 보안 인시던트의 평균 해결 시간이 표시됩니다. MTTR은 인시던트 조사 및 해결 속도를 나타냅니다. 원하는 열을 클릭하면 심각도(**심각**, **높음**, **보통**)에 따른 인시던트 세부 정보, 그리고 각 심각도 수준의 인시던트를 해결하는 데 걸린 시간을 확인할 수 있습니다. 괄호 안에 표시되는 비율 값은 이전 기간과 비교한 증감률을 나타냅니다.
위협 상태	이 위젯에는 회사 워크로드 수에 관계없이 워크로드의 현재 위협 상태가 표시됩니다. 그리고 완화되지 않아 조사가 필요한 인시던트의 현재 수가 강조 표시됩니다. 그리고 수동으로 및/또는 시스템에서 자동으로 완화된 인시던트의 수도 표시됩니다.
보호 기술로	이 위젯은 특정 날짜 범위에서 감지된 위협의 수를 웹 사이트 카테고리별로

위젯	설명
탐지한 위협	그룹화하여 보여줍니다. • 맬웨어 방지 스캐닝 • 동작 엔진 • 크립토마이닝(cryptomining) 예방 • 악용 방지 • 랜섬웨어 활성 보호 • 실시간 보호 • URL 필터링

백업 위젯

다음 표는 **백업** 섹션에 있는 위젯에 대한 자세한 내용입니다.

위젯	설명
백업된 워크로드	이 위젯은 등록된 워크로드의 총 수를 백업 상태별로 보여줍니다. **백업됨** - 보고 날짜 범위 내에 백업된 워크로드의 수(성공적인 백업이 1회 이상 수행된 경우). **백업되지 않음** - 보고 날짜 범위 내에 백업되지 않은 워크로드의 수(성공적인 백업이 수행되지 않은 경우).
실제 장치별 디스크 상태	이 위젯은 장치의 디스크 상태에 기반한 실제 장치의 총 상태를 보여줍니다. **OK** - 이 디스크 상태는 [70-100] 값과 관련됩니다. 모든 디스크의 상태가 **OK**일 경우 장치의 상태는 **OK**입니다. **경고** - 이 디스크 상태는 [30-70] 값과 관련됩니다. 한 개 이상의 장치 디스크 상태가 **경고**이고 **오류** 상태인 디스크가 없는 경우 장치의 상태는 **경고**입니다. **오류** - 이 디스크 상태는 [0-30] 값과 관련됩니다. 한 개 이상의 디스크 상태가 **오류**일 경우 장치의 상태는 **오류**입니다. **디스크 데이터 계산 중** - 디스크 상태가 아직 계산 중인 경우 장치 상태는 **디스크 데이터 계산 중**입니다.
백업 스토리지 사용량	이 위젯은 특정한 시간 범위에서 클라우드 및 로컬 스토리지 내 백업의 총 수와 총 크기를 표시합니다.

취약성 평가 및 패치 관리 위젯

다음 표는 **취약성 평가 및 패치 관리** 섹션의 위젯에 대한 자세한 정보를 제공합니다.

위젯	설명
패치된 취약성	이 위젯은 특정 날짜 범위에서 취약성 평가 성능 결과를 보여줍니다. **합계** - 패치된 취약성의 총 수.

위젯	설명
	Microsoft 소프트웨어 취약성 - 모든 Windows 장치에서 수정된 Microsoft 취약성의 총 수. **Windows 서드 파티 소프트웨어 취약성** - 모든 Windows 장치에서 수정된 Windows 서드 파티 취약성의 총 수. **스캔된 워크로드** - 특정 날짜 범위에서 한 번 이상 성공적으로 취약성 스캔이 이루어진 장치의 총 수입니다.
설치된 패치	이 위젯은 특정 날짜 범위에서 패치 관리 성능 결과를 보여줍니다. **설치됨** - 모든 장치에 성공적으로 설치된 패치의 총 수. **Microsoft 소프트웨어 패치** - 모든 Windows 장치에 설치된 Microsoft 소프트웨어 패치의 총 수. **Windows 서드 파티 소프트웨어 패치** - 모든 Windows 장치에 설치된 Windows 서드 파티 패치의 총 수. **패치된 워크로드** - 성공적으로 패치된 장치의 총 수(특정한 날짜 범위에서 한 번 이상 성공적으로 패치가 이루어진 경우).

재해 복구 위젯

다음 표는 **재해 복구** 섹션의 위젯에 대한 자세한 정보를 제공합니다.

위젯	설명
재해 복구 통계	이 위젯은 특정 날짜 범위에서 재해 복구 주요 성능 메트릭을 보여줍니다. **프로덕션 장애 조치** - 특정 날짜 범위에서 프로덕션 장애 조치 작업의 수. **시험 장애 조치** - 특정 날짜 범위에서 시험 장애 조치 작업의 총 수. **기본 서버** - 보고서 생성 시점에서 기본 서버의 총 수. **복구 서버** - 보고서 생성 시점에서 복구 서버의 총 수. **공용 IP** - 공용 IP 주소의 총 수(보고서 생성 시점). **사용한 총 컴퓨팅 포인트** - 특정 날짜 범위에서 사용한 컴퓨팅 포인트의 총 수.
테스트된 재해 복구 서버	이 위젯은 재해 복구로 보호되고 시험 장애 조치로 테스트된 서버에 대한 정보를 표시합니다. 이 위젯은 다음 메트릭을 나타냅니다. **보호 중인 서버** - 보고서 생성 시점에서 재해 복구에 의해 보호된 서버의 수(최소 한 개 이상의 복구 서버를 가지고 있는 경우). **테스트됨** - 재해 복구로 보호된 모든 서버 중 특정 시간 범위 내에서 시험 장애 조치로 테스트된 서버의 수. **테스트되지 않음** - 재해 복구로 보호되는 모든 서버 중 특정 시간 범위 내에서 시험 장애 조치로 검사되지 않은 서버의 수.

위젯	설명
	이 위젯은 또한 보고서 생성 시점에서 재해 복구 스토리지의 크기(GB 단위)도 표시합니다. 클라우드 서버 백업 크기의 총 합계입니다.
재해 복구로 보호되는 서버	이 위젯은 재해 복구로 보호되거나 보호되지 않는 서버에 대한 정보를 표시합니다. 이 위젯은 다음 메트릭을 나타냅니다. 보고서 생성 시점에서 고객 테넌트에 등록된 서버의 총 수. **보호됨** - 보고서 생성 시점에서 등록된 모든 서버 중 재해 복구에 의해 보호된 서버의 수(최소 한 개 이상의 복구 서버 및 전체 서버 백업을 가지고 있는 경우). **보호되지 않음** - 보고서 생성 시점에서 등록된 모든 서버 중 보호되지 않는 서버의 총 수.

데이터 손실 방지 위젯

다음 항목에서는 **데이터 손실 방지** 섹션의 차단된 주변 장치에 대한 자세한 정보를 제공합니다.

이 위젯은 특정 날짜 범위에서 차단된 장치의 총 수와 장치 유형별로 차단된 장치의 총 수를 보여줍니다.

- 이동식 스토리지
- 암호화된 이동식
- 프린터
- 클립보드- 클립보드 및 스크린샷 캡처 장치 유형을 포함합니다.
- 모바일 장치
- Bluetooth
- 광학 드라이브
- 플로피 드라이브
- USB - USB 포트 및 리디렉션 USB 포트 장치 유형을 포함합니다.
- FireWire
- 매핑된 드라이브
- 리디렉션 클립보드- 들어온 리디렉션 클립보드 및 나가는 클립보드 유형을 포함합니다.

이 위젯은 차단된 장치의 수가 가장 많은 일곱 개의 장치 유형을 보여주고, 나머지 장치 유형은 **기타** 장치 유형으로 통합합니다.

File Sync & Share 위젯

다음 표는 **File Sync & Share** 섹션의 위젯에 대한 자세한 정보를 제공합니다.

위젯	설명
File Sync & Share 통계	이 위젯은 다음 메트릭을 나타냅니다.

위젯	설명
	사용한 총 클라우드 스토리지 - 모든 사용자가 사용한 총 스토리지. **최종 사용자** - 최종 사용자의 총 수. **최종 사용자당 평균 스토리지 사용량** - 최종 사용자 별 평균 스토리지 사용량. **게스트 사용자** - 게스트 사용자의 총 수.
최종 사용자별 File Sync & Share 스토리지 사용량	이 위젯은 다음 범위에서 스토리지 사용량이 있는 File Sync & Share 최종 사용자의 총 수를 나타냅니다. • 0 – 1GB • 1 - 5GB • 5 - 10GB • 10 - 50GB • 50 - 100GB • 100 – 500GB • 500 - 1TB • 1+ TB

공증 위젯

다음 표는 **공증** 섹션의 위젯에 대한 자세한 정보를 제공합니다.

위젯	설명
사이버 공증 통계	이 위젯은 다음 공증 메트릭을 나타냅니다. **사용된 공증 클라우드 스토리지** - 공증 서비스에 사용된 스토리지의 총 크기. **공증된 파일** - 공증된 파일의 총 수. **전자 서명 문서** - 전자 서명된 문서 및 파일의 총 수.
최종 사용자 전반의 공증된 파일	모든 최종 사용자의 공증한 파일의 총 수를 보여줍니다. 사용자는 보유한 공증된 파일의 수에 따라 그룹화됩니다. • 최대 10개 파일 • 11 - 100개 파일 • 101 - 500개 파일 • 501 - 1000개 파일 • 1000+ 파일
최종 사용자의 전자 서명 문서	이 위젯은 모든 최종 사용자의 전자 서명된 문서의 총 수와 해당 파일을 보여줍니다. 사용자는 보유한 전자 서명된 문서와 파일의 수에 따라 그룹화됩니다. • 최대 10개 파일

위젯	설명
	• 11 - 100개 파일 • 101 - 500개 파일 • 501 - 1000개 파일 • 1000+ 파일

총괄 요약 보고서 설정 구성

총괄 요약 보고서가 생성된 시점에 구성된 보고서 설정을 업데이트할 수 있습니다.

총괄 요약 보고서 설정 업데이트하는 방법

1. 관리 콘솔에서 **보고서>총괄 요약**으로 이동합니다.
2. 업데이트하고자 하는 총괄 요약 보고서 이름을 클릭합니다.
3. **설정**을 클릭합니다.
4. 필요한 경우 필드 값을 변경합니다.
5. **저장**을 클릭합니다.

총괄 요약 보고서 생성

총괄 요약 보고서를 생성하고, 내용을 검토하고, 보고서 수령자를 구성하고, 자동으로 전송하는 시점을 예약할 수 있습니다.

총괄 요약 보고서 생성 방법

1. 관리 콘솔에서 **보고서>총괄 요약**으로 이동합니다.
2. **총괄 요약 보고서 생성**을 클릭합니다.
3. **보고서 이름**에 보고서 이름을 입력합니다.
4. 보고서 수령자를 선택합니다.
   - 모든 직접 고객에게 보고서를 보내려면 **모든 직접 고객에 전송**을 선택합니다.
   - 특정 고객에게 보고서를 보내려면
     a. **모든 직접 고객에게 전송**을 선택 취소합니다.
     b. **연락처 선택**을 클릭합니다.
     c. 특정 고객을 선택하십시오. 검색을 통해 특정 연락처를 쉽게 찾을 수 있습니다.
     d. **선택**을 클릭합니다.
5. 범위를 선택합니다. **30일** 또는 **이번 달**
6. 파일 형식을 선택합니다. **PDF**, **Excel**, 또는 **Excel 및 PDF**.
7. 예약 설정을 구성합니다.
   - 특정 날짜와 시간에 보고서를 수령자에게 보내는 방법:
     a. **예약됨** 옵션을 활성화합니다.
     b. **날짜** 필드를 클릭한 다음 마지막 날짜 필드를 지우고, 원하는 날짜를 선택합니다.

c. **시간** 필드에서는 설정하고자 하는 시간으로 입력합니다.
d. **적용**을 클릭합니다.
   - 보고서를 전송하지 않고 보고서를 생성하고자 하는 경우에는 **예약됨** 옵션을 비활성화 하십시오.
8. **저장**을 클릭합니다.

총괄 요약 보고서 사용자 정의

요약 보고서에 포함할 정보를 결정할 수 있습니다. 섹션을 추가 또는 삭제하고, 위젯을 추가 또는 삭제하고, 섹션 이름을 변경하고, 위젯을 사용자 정의하고, 위젯과 섹션을 끌어서 놓아 보고서의 정보가 표시되는 순서를 변경할 수 있습니다.

섹션을 추가하려면

1. **항목 추가** > **섹션 추가**를 클릭합니다.
2. **섹션 추가** 창에서 섹션 이름을 입력하거나 기본 섹션 이름을 사용합니다.
3. **보고서에 추가**를 클릭합니다.

섹션 이름을 변경하려면

1. 이름 변경할 섹션에서 **편집**을 클릭합니다.
2. **섹션 수정** 창에서 새 이름을 입력합니다.
3. **저장**을 클릭합니다.

섹션을 삭제하려면

1. 삭제할 섹션에서 **섹션 삭제**를 클릭합니다.
2. **섹션 삭제** 확인 창에서 **삭제**를 클릭합니다.

섹션에 기본 설정으로 위젯 추가하는 방법

1. 위젯을 추가할 섹션에서 **위젯 추가**를 클릭합니다.
2. **위젯 추가** 창에서 추가할 위젯을 선택합니다.

섹션에 사용자 정의된 위젯을 추가하려면

1. 위젯을 추가할 섹션에서 **위젯 추가**를 클릭합니다.
2. **위젯 추가** 창에서 추가할 위젯을 선택한 다음 **사용자 정의**를 클릭합니다.
3. 필요한 경우 필드를 구성합니다.
4. **위젯 추가**를 클릭합니다.

보고서에 기본 설정으로 위젯 추가하는 방법

1. **항목 추가** > **위젯 추가**를 클릭합니다.
2. **위젯 추가** 창에서 추가할 위젯을 선택합니다.

보고서에 사용자 정의된 위젯을 추가하려면

1. **위젯 추가**를 클릭합니다.
2. **위젯 추가** 창에서 추가할 위젯을 선택한 다음 **사용자 정의**를 클릭합니다.
3. 필요한 경우 필드를 구성합니다.
4. **위젯 추가**를 클릭합니다.

위젯 기본 설정 초기화하는 방법

1. 사용자 정의할 위젯에서 **편집**을 클릭합니다.
2. **기본값으로 복구**를 클릭합니다.
3. **완료**를 클릭합니다.

위젯을 사용자 정의하는 방법

1. 사용자 정의할 위젯에서 **편집**을 클릭합니다.
2. 필요한 경우 필드를 편집합니다.
3. **완료**를 클릭합니다.

총괄 요약 보고서 전송

필요에 따라 총괄 요약 보고서를 전송할 수 있습니다. 이 경우 **예약됨** 설정은 무시되고 보고서가 즉시 보내집니다. 보고서를 전송할 때는 시스템은 **설정**에서 구성한 수령인, 범위, 파일 형식 값을 사용합니다. 보고서를 전송하기 전에 수동으로 이 설정을 바꿀 수 있습니다. 자세한 내용은 "총괄 요약 보고서 설정 구성"(110페이지)을(를) 참조하십시오.

총괄 요약 보고서 전송 방법

1. 관리 포털에서 **보고서>총괄 요약서**로 이동합니다.
2. 보내고자 하는 총괄 요약 보고서 이름을 클릭합니다.
3. **지금 보내기**를 클릭합니다.
   시스템이 선택된 수령인에게 총괄 요약 보고서를 보내게 됩니다.

보고서의 시간대

보고서에서 사용되는 시간대는 보고서 유형에 따라 다릅니다. 다음 표에는 참조를 위한 정보가 포함되어 있습니다.

보고서 위치 및 유형	보고서에서 사용되는 시간대
관리 포털> 개요 > 작업 (위젯)	보고서 생성 시간은 브라우저가 실행되는 머신의 시간대로 표시됩니다.
관리 포털> 개요 > 작업 (PDF 또는 xslx로 내보냄)	• 내보낸 보고서의 타임 스탬프는 보고서를 내보내는 데 사용된 머신의 시간대로 표시됩니다. • 보고서에 표시되는 활동의 시간대는 UTC로 표시됩니다.
관리 포털> 보고서 > 사용 > 예약된 보고서	• 보고서는 해당 월의 첫 번째 날 23:59:59(UTC)에 생성됩니다. • 보고서는 해당 월의 두 번째 날 전송됩니다.

관리 포털> 보고서 > 사용 > 사용자 정의 보고서	보고서의 시간대와 날짜는 UTC로 표시됩니다.
관리 포털> 보고서 > 작업 (위젯)	• 보고서 생성 시간은 브라우저가 실행되는 머신의 시간대로 표시됩니다. • 보고서에 표시되는 활동의 시간대는 UTC로 표시됩니다.
관리 포털> 보고서 > 작업 (PDF 또는 xslx로 내보냄)	• 내보낸 보고서의 타임 스탬프는 보고서를 내보내는 데 사용된 머신의 시간대로 표시됩니다. • 보고서에 표시되는 활동의 시간대는 UTC로 표시됩니다.
관리 포털> 보고서 > 작업 (예약된 전송)	• 보고서 전송 시간대는 UTC로 표시됩니다. • 보고서에 표시되는 활동의 시간대는 UTC로 표시됩니다.
관리 포털> 사용자 > 활성 경보에 대한 일일 확인	• 이 보고서는 하루에 한 번 10:00와 23:59 UTC 사이에 전송됩니다.보고서가 전송되는 시간은 데이터센터의 워크로드에 따라 다릅니다. • 보고서에 표시되는 활동의 시간대는 UTC로 표시됩니다.
관리 포털> 사용자 > 사이버 보호 상태 알림	• 이 보고서는 작업이 완료될 때 전송됩니다. **참고** 데이터센터의 워크로드에 따라 일부 보고서의 전송이 지연될 수 있습니다. • 보고서의 활동 시간대는 UTC로 표시됩니다.

위젯 유형에 따라 보고된 데이터

대시보드의 위젯은 표시하는 데이터 범위에 따라 두 가지 유형으로 구분할 수 있습니다.

- 찾아보기 또는 보고서 생성 시점의 실제 데이터를 표시하는 위젯
- 내역 데이터를 표시하는 위젯

특정 기간의 데이터를 덤프하기 위해 보고서 설정에서 날짜 범위를 구성하면 선택한 시간 범위는 내역 데이터를 표시하는 위젯에만 적용됩니다.찾아보기 시점의 실제 데이터를 표시하는 위젯에는 시간 범위 매개변수가 적용되지 않습니다.

다음 표에는 사용 가능한 위젯과 해당 데이터 범위가 나와 있습니다.

위젯 이름	위젯과 보고서에 표시되는 데이터
머신별 #CyberFit Score	실제
최신 경보 5개	실제
활성 경보 세부 정보	실제
활성 경보 요약	실제
작업	내역

활동 목록	내역
경보 내역	내역
백업 맬웨어 방지 스캔	내역
파일의 맬웨어 방지 스캔	내역
백업 스캔 세부 정보(위협)	내역
백업 상태	내역 - **총 실행 수** 및 **성공한 실행 수** 열 실제 - 기타 모든 열
백업 스토리지 사용량	내역
차단된 주변 장치	내역
차단된 URL	실제
클라우드 애플리케이션	실제
클라우드 워크로드 보호 상태	실제
Cyber protection	실제
사이버 보호 요약	내역
데이터 보호 맵	내역
장치	실제
테스트된 재해 복구 서버	내역
재해 복구 통계	내역
검색된 머신	실제
디스크 상태 개요	실제
디스크 상태	실제
실제 장치별 디스크 상태	실제
최종 사용자의 전자 서명 문서	실제
기존 취약성	내역
File Sync & Share 통계	실제
최종 사용자별 File Sync & Share 스토리지 사용량	실제
하드웨어 변경	내역
하드웨어 상세 정보	실제
하드웨어 인벤토리	실제

경보 내역 요약	내역
위치 요약	실제
카테고리별 누락 업데이트	실제
보호되지 않음	실제
최종 사용자 전반의 공증된 파일	실제
공증 통계	실제
패치 설치 내역	내역
패치 설치 상태	내역
패치 설치 요약	내역
패치된 취약성	내역
설치된 패치	내역
보호 상태	실제
최근 영향 받은 항목	내역
원격 세션	내역
보안 인시던트 번다운(Burndown)	내역
보안 인시던트 MTTR	내역
재해 복구로 보호되는 서버	실제
소프트웨어 인벤토리	실제
소프트웨어 개요	내역
위협 상태	실제
보호 기술로 탐지한 위협	내역
워크로드별 상위 인시던트 분산	실제
취약한 머신	실제
워크로드 네트워크 상태	실제
백업된 워크로드	내역
워크로드 보호 상태	실제

계산기로 Cyber Protect Cloud 예상 비용 계산

Cyber Protect Cloud 평가판 버전을 사용 중이라면 계산기를 사용하여 예상 비용을 계산할 수 있습니다.

참고

평가판을 사용 중인 파트너만 관리 포털에서 Cyber Protect Cloud 계산기에 액세스할 수 있으며 고객이나 평가판을 사용 중이지 않은 파트너는 계산기에 액세스할 수 없습니다.

계산기를 사용하여 Cyber Protect Cloud 예상 비용을 계산하려면

1. 관리 포털 왼쪽 아래에서 **월간 비용 계산**을 클릭합니다.
2. 계획한 로드에 대해 다음 상세 정보를 지정합니다.
   - 워크로드 유형별 워크로드 수. 예를 들어 가상 머신, 워크스테이션, 호스팅 서버, Google Workspace 시트, 모바일 장치, Microsoft 365 시트 등을 지정합니다.
   - 데이터 센터 위치와 스토리지 용량 등의 데이터 스토리지 상세 정보.
3. [선택 사항] 사용하려는 고급 백업, 보안 또는 관리 옵션 및 각 옵션의 워크로드 수를 지정합니다.
4. 라이선스 모델(워크로드 단위 또는 GB 단위)을 선택합니다.

그러면 오른쪽에 예상 월간 비용이 표시됩니다.

계산기 페이지에서 해당 버튼을 클릭하거나, 전문가와 채팅을 진행하거나, 클라우드 상담사의 직접 연락을 요청하면 파트너 등록을 할 수 있습니다.

관리 포털 왼쪽 아래에서 **영업 담당자 문의**를 클릭하여 영업 부서 문의를 시작할 수도 있습니다.

파트너 포털 사용

파트너 포털은 #CyberFit 파트너 프로그램에 참여하는 서비스 제공업체, 총판업체 및 리셀러용 웹 사이트입니다.

파트너 포털에서는 관련 콘텐츠, 도구 및 교육에 액세스할 수 있습니다.

파트너 포털 사용을 시작하려면

1. 다음 방법 중 하나로 파트너 포털에 액세스합니다.
   - 관리 포털 왼쪽 아래에서 **파트너 가입**을 클릭합니다.
   - 파트너 포털 웹 사이트를 방문합니다.
2. 파트너 프로그램에 회사를 등록합니다.
3. 이메일을 통해 액세스 상세 정보를 수신합니다.

파트너 포털 역할

파트너 포털에는 필요에 따라 사용자에게 할당할 수 있는 여러 역할이 포함되어 있습니다.

아래 표는 각각의 사용 가능한 역할과 파트너 포털 내에서 각 역할에 할당된 권한을 설명합니다.

역할	설명
기본	모든 사용자에게 적용되는 기본 역할입니다. 이 역할은 파트너 포털의 필수 기능에 대한 액세스 권한을 부여합니다. 여기에는 대시보드, 파트너 프로그램, 콘텐츠 허브, 교육 및 지원 등이 있습니다.
교육	이 역할을 가진 사용자는 교육 자료에 액세스할 수 있습니다. 파트너 포털의 다른 기능은 이러한 사용자에게 사용할 수 없습니다.
마케팅	이 역할은 마케팅 전문가에게 필요한 파트너 포털의 기능에 대한 액세스 권한을 부여합니다. 여기에는 대시보드, 파트너 프로그램, 마케팅, 콘텐츠 허브, 교육, 지원, 데이터 센터 상태, 데이터베이스 관리 등이 있습니다.
영업	이 역할을 가진 사용자는 영업 전문가에게 필요한 파트너 포털의 기능에 액세스할 수 있습니다. 여기에는 대시보드, 파트너 프로그램, 영업, 콘텐츠 허브, 교육, 지원, 데이터 센터 상태, 데이터베이스 관리 등이 있습니다.
영업 및 마케팅	이 역할은 영업 및 마케팅 통합 전문가에게 필요한 파트너 포털의 기능에 대한 액세스 권한을 부여합니다. 여기에는 대시보드, 파트너 프로그램, 영업, 마케팅, 콘텐츠 허브, 교육, 지원, 데이터 센터 상태, 데이터베이스 관리 등이 있습니다.
관리자	관리자는 대시보드, 파트너 프로그램, 영업, 마케팅, 콘텐츠 허브, 교육, 지원, 데이터 센터 상태, 데이터베이스 관리 등 파트너 포털의 모든 기능에 액세스할 수 있습니다. 또한 관리자는 파트너 사용자의 권한을 관리하고 회사 정보를 수정할 수 있습니다.

공급 업체 포털 사용

공급 업체 포털(CyberApp Standard)은 서드 파티 소프트웨어 공급 업체가 자사 제품과 서비스를 Cyber Protect Cloud에 통합할 수 있는 플랫폼입니다.

공급 업체 포털에서는 다음 작업을 수행할 수 있습니다.

- 개발 및 테스트용 아크로니스 샌드박스 환경 액세스.
- 아크로니스 애플리케이션 카탈로그에 솔루션 추가.
- Cyber Protect Cloud 콘솔에 워크로드, 경보, 위젯, 보고서 통합.
- 업계 표준 조치를 활용하여 데이터 보안 강화.

공급 업체 포털 사용을 시작하려면

1. 아크로니스 Technology Ecosystem 웹 사이트에서 등록 진행.
2. 계정을 활성화합니다.

Advanced Protection 팩

Advanced Protection 팩은 보호 서비스와 별도로 활성화할 수 있으며, 활성화 시에는 추가 요금이 부과됩니다. Advanced Protection 팩에서는 표준 기능 세트 및 기타 Advanced 팩에는 포함되지 않은 고유한 기능이 제공됩니다. 고객은 Advanced 팩을 하나 또는 여러 개 사용하거나 모든 Advanced 팩을 사용하여 워크로드를 보호할 수 있습니다. Advanced Protection 팩은 보호 서비스의 두 가지 요금 청구 모드(워크로드당, 기가바이트당)에 모두 사용 가능합니다.

File Sync & Share 서비스를 사용하여 Advanced File Sync & Share 기능을 활성화할 수 있습니다. 이 기능은 사용자당 청구 모드와 기가바이트당 청구 모드에서 모두 사용 가능합니다.

활성화할 수 있는 Advanced Protection 팩은 다음과 같습니다.

- Advanced Backup

  Advanced Backup 팩에는 워크스테이션, 서버, 가상 머신, 웹 호스팅 서버, Google Workspace 시트 및 Microsoft 365 시트용으로 다수의 개별 라이선스와 할당량이 포함되어 있습니다.
- Advanced Management
- Advanced Security + EDR(엔드포인트 탐지 및 응답)
- Advanced Data Loss Prevention
- Advanced Disaster Recovery
- Advanced Email Security
- Advanced File Sync & Share

참고
Advanced 팩은 확장 대상 기능이 활성화되어 있어야 사용할 수 있습니다. 표준 서비스 기능이 비활성화되어 있으면 사용자는 고급 기능을 사용할 수 없습니다. 예를 들어 보호 기능이 비활성화되어 있으면 사용자는 Advanced Backup 팩 기능을 사용할 수 없습니다.

고급 보호 팩이 활성화된 경우 해당 기능이 보호 계획에 나타나고 고급 기능 아이콘( )으로 표시됩니다. 사용자가 기능 활성화를 시도하면 추가 요금이 청구된다는 메시지가 표시됩니다.

Advanced Protection 팩이 활성화되어 있지 않지만 업셀이 켜져 있는 경우 Advanced Protection 기능이 보호 계획에 표시되지만 액세스하여 사용할 수 없습니다. 그리고 관리자에게 필요한 고급 기능 세트 활성화를 요청하라는 메시지가 사용자에게 표시됩니다.

고급 보호 팩이 활성화되어 있지 않고 업셀도 꺼져 있으면 고객의 보호 계획에 고급 기능이 표시되지 않습니다.

Cyber Protect 서비스에 포함된 기능 및 Advanced 팩

Cyber Protect에서 서비스 또는 기능 세트를 활성화하면 기본적으로 포함되어 있으며 사용 가능한 여러 기능이 활성화됩니다. 또한 Advanced Protection 팩도 활성화할 수 있습니다.

아래 섹션에는 Cyber Protect 서비스 기능 및 Advanced 팩의 대략적인 개요가 나와 있습니다. 제공 항목의 전체 목록은 Cyber Protect 라이선스 안내서를 참조하십시오.

보호 서비스에 포함된 기능 및 고급 기능

보호 서비스에 포함된 기능 및 고급 기능

기능 그룹	포함된 표준 기능	고급 기능
Security + EDR	• #CyberFit Score • 취약성 평가 • 안티 랜섬웨어 예방: Active Protection • 안티바이러스 및 안티맬웨어 보호: 클라우드 서명 기반 파일 감지(실시간 보호 기능은 제공되지 않으며 예약된 스캔만 가능)* • 안티바이러스 및 안티맬웨어 보호: 사전 실행 AI 기반 파일 분석기, 동작 기반 Cyber Engine • Microsoft Defender 관리 *Cyber Protect는 제로 데이 공격 감지를 위해 추정 스캔 규칙과 알고리즘을 사용하여 악성 명령을 찾습니다.	Advanced Security + EDR 팩에는 다음이 포함됩니다. • 중앙 집중식 인시던트 페이지에서 인시던트 관리 • 인시던트의 범위와 영향 시각화 • 권장 사항 및 수정 단계 • 위협 피드를 사용하여 워크로드와 관련해 공개된 공격 확인 • 180일 동안 보안 이벤트 저장 • 관리형 탐지 및 대응(MDR) • 로컬 서명 기반 감지 기능이 포함된 안티바이러스 및 안티맬웨어 보호(실시간 보호 기능 제공) • 악용 방지 • URL 필터링 • 엔드포인트 방화벽 관리 • 포렌식 백업, 맬웨어 대비 백업 스캔, 안전 복구, 기업 허용 목록 • 스마트 보호 계획(CPOC 경보와의 통합) • 중앙 집중식 맬웨어 스캔 • 원격 지우기 • Windows Defender 안티바이러스 • Microsoft Security Essentials Advanced Security + EDR을 활성화하는 방법에 대한 정보는 "Advanced Security + EDR 활성화"(124페이지)을(를) 참조하십시오.
데이터 손실 방지	• 장치 제어	• 주변 장치 및 네트워크 통신을 통한 워크로드의 데이터 손실 콘텐츠 인식 방지 • PII(개인 식별 정보), PHI(개인 건강 정보), PCI DSS(결제 카드 산업 데이터 보안 표준) 데이터 및 "기밀로 표시됨" 카테고리의 문서에 대한 사전 구축된 자동 탐지 • 선택적 최종 사용자 지원을 통한 자동 데이터 손실 방지 정책 생성

기능 그룹	포함된 표준 기능	고급 기능
		• 자동 학습 기반 정책 조정을 통한 적응형 데이터 손실 방지 적용 • 클라우드 기반 중앙 집중식 감사 로깅, 경보 및 최종 사용자 알림
관리	• 워크로드의 그룹 관리 • 중앙 관리식 보호 계획 관리 • 하드웨어 인벤토리 • 원격 제어 • 원격 작업 • 기술 담당자당 동시 연결 수 • 원격 연결 프로토콜: RDP • 모니터 4개 • 임계값 기반 모니터링	• 패치 관리 • 디스크 상태 • 소프트웨어 인벤토리 • 유사시 대기 패칭 • Cyber Scripting • 원격 지원 • 파일 전송 및 공유 • 연결할 세션 선택 • 다중 보기에서 워크로드 관찰 • 연결 모드: 제어, 보기 전용 및 커튼 • 빠른 지원 애플리케이션을 통한 연결 • 원격 연결 프로토콜: NEAR 및 Apple 화면 공유 • NEAR 연결을 위한 세션 녹화 • 스크린샷 전송 • 세션 내역 보고서 • 모니터 24개 • 임계값 기반 모니터링 • 이상 현상 기반 모니터링
이메일 보안	없음	Microsoft 365 및 Gmail 사서함의 실시간 보호: • 맬웨어 방지 스팸 방지 • 이메일에서 URL 검색 • DMARC 분석 • 피싱 방지 • 가장 보호 • 첨부 파일 검사 • 컨텐츠 무해화 및 재구성 • 신뢰 그래프 구성 가이드를 참조하십시오.
Cyber Disaster Recovery Cloud	Disaster Recovery 표준 기능을 사용하여 워크로드에 적용되는 Disaster Recovery 시나리오를 테스트할 수 있습니다. 제공되는 Disaster Recovery 표준 기능 및 각 기능의 제한은 다음과 같습니다.	Advanced Disaster Recovery 팩을 활성화할 수 있으며 전체 Disaster Recovery 기능을 사용하여 워크로드를 보호할 수 있습니다. 제공되는 Disaster Recovery 고급 기능은

기능 그룹	포함된 표준 기능	고급 기능
	• 격리된 네트워크에서의 테스트 장애 조치. 매월 컴퓨팅 포인트 32개의 장애 조치를 테스트할 수 있으며 테스트 장애 조치 작업을 5개까지 동시에 실행할 수 있습니다. • 복구 서버 구성: CPU 1개와 2GB RAM, CPU 1개와 4GB RAM, CPU 2개와 8GB RAM. • 장애 조치에 사용 가능한 복구 지점 수: 백업 직후에 제공되는 마지막 복구 지점만 사용 가능합니다. • 제공되는 연결 모드: 클라우드 전용, 지점 및 사이트 간. • VPN 게이트웨이 가용성: VPN 게이트웨이는 마지막 테스트 장애 조치 완료 후 4시간 동안 비활성 상태로 유지되면 일시 중지되며 테스트 장애 조치를 시작하면 다시 디플로이됩니다. • 클라우드 네트워크 수: 1. • 인터넷 액세스 • 실행서 관련 작업: 생성 및 편집.	다음과 같습니다. • 프로덕션 장애 조치 • 격리된 네트워크에서의 테스트 장애 조치. • 장애 조치에 사용 가능한 복구 지점 수: 복구 서버 생성 후 제공되는 모든 복구 지점을 사용할 수 있습니다. • 기본 서버 • 복구/기본 서버 구성: 제한 없음 • 제공되는 연결 모드: 클라우드 전용, 지점 및 사이트 간, 사이트 간 OpenVPN, 다중 사이트 IPsec VPN. • VPN 게이트웨이 가용성: 항상 사용 가능합니다. • 클라우드 네트워크 수: 23. • 공용 IP 주소 • 인터넷 액세스 • 실행서 관련 작업: 생성, 편집 및 실행.

보호 서비스의 고급 기능 및 종량과금제

보호 서비스의 고급 기능 및 종량과금제

기능 그룹	종량제 기능	고급 기능
백업	• 파일 백업 • 이미지 백업 • 애플리케이션 백업 • 네트워크 공유 백업 • 클라우드 스토리지에 백업 • 로컬 스토리지에 백업 **참고** 클라우드 스토리지 사용 요금이 적용됩니다.	• 원클릭 복구 • 지속적인 데이터 보호 • Microsoft SQL Server 클러스터 및 Microsoft Exchange 클러스터의 백업 지원 - Always On 가용성 그룹(AAG) 및 데이터베이스 가용성 그룹(DAG) • MariaDB, MySQL, Oracle DB 및 SAP HANA의 백업 지원 • 데이터 보호 맵 및 규제 준수 보고 • 오프호스트 데이터 처리 • Microsoft 365 및 Google Workspace 워크로드의 백업 빈도 • 부트 가능한 미디어를 사용한 원격 작업 • Microsoft Azure 퍼블릭 클라우드 스토리지에 직접 백업

기능 그룹	종량제 기능	고급 기능
File Sync & Share	• 암호화된 파일 기반 컨텐츠 저장 • 지정된 장치에서 파일 동기화 • 지정된 사용자 및 시스템과 폴더 및 파일 공유	• 공증 및 전자 서명 • 문서 템플릿* *동기화 및 공유 파일 백업
실제 데이터 전달	실제 데이터 전달 기능	해당 없음
공증	• 파일 공증 • 파일 전자 서명 • 문서 템플릿	해당 없음

참고
확장 대상 표준 보호 기능을 활성화해야 Advanced Protection 팩을 활성화할 수 있습니다. 기능을 비활성화하면 해당 Advanced 팩이 자동으로 비활성화되며, Advanced 팩을 사용하는 보호 계획이 자동으로 철회됩니다. 예를 들어 보호 기능을 비활성화하면 해당 Advanced 팩이 자동으로 비활성화되며 이러한 Advanced 팩을 사용하는 모든 계획이 철회됩니다.

표준 보호를 사용하지 않는 사용자는 Advanced Protection 팩을 사용할 수 없습니다. 특정 워크로드에서 표준 보호에 포함된 기능과 Advanced 팩을 함께 사용할 수는 있습니다. 이 경우에는 사용하는 Advanced 팩의 요금만 부과됩니다.

요금 청구에 대한 정보는 "Cyber Protect의 청구 모드"(8페이지)의 내용을 참조하십시오.

Advanced Data Loss Prevention

Advanced Data Loss Prevention 모듈은 로컬 및 네트워크 채널을 통해 전송되는 데이터의 내용을 검사하고 조직별 데이터 플로우 정책 규칙을 적용하여 워크스테이션, 서버, 가상 머신에서 민감한 정보가 유출되는 것을 방지합니다.

Advanced Data Loss Prevention 모듈을 사용하기 전에 기본 가이드에 설명된 Advanced Data Loss Prevention 관리의 기본 개념과 논리를 읽고 이해했는지 확인해야 합니다.

기술 사양 문서를 검토할 수도 있습니다.

Advanced Data Loss Prevention 활성화

기본적으로 Advanced Data Loss Prevention은 새 테넌트에 대한 구성에서 실행됩니다. 테넌트 생성 프로세스 중에 이 기능을 사용하지 않도록 설정한 경우, 파트너 관리자가 나중에 사용하도록 설정할 수 있습니다.

Advanced Data Loss Prevention을 활성화하려면

1. Cyber Protect Cloud 관리 콘솔에서 **클라이언트**로 이동합니다.
2. 편집할 테넌트를 선택합니다.
3. **서비스 선택** 섹션에서 **보호**로 스크롤하고 적용하는 요금 청구 모드에서 **Advanced Data Loss Prevention**을 선택합니다.

4. 서비스 구성에서 **Advanced Data Loss Prevention**으로 스크롤하고 할당량을 구성합니다.
   할당량은 무제한으로 기본 설정됩니다.
5. 설정을 저장합니다.

Advanced Security + EDR

EDR(Endpoint Detection and Response)은 워크로드에서 감지되지 않은 공격을 비롯한 의심스러운 활동을 감지하며 인시던트를 생성합니다. 이러한 인시던트에서는 각 공격의 단계별 개요를 제공하므로 공격이 발생한 방식 및 해당 공격의 재발 방지 방법을 파악할 수 있습니다. 공격의 각 단계를 쉽게 이해할 수 있는 해석 정보가 제공되므로 공격 조사에 소요되는 시간을 몇 분으로 단축할 수 있습니다.

Advanced Security + EDR 활성화

파트너 관리자는 Advanced Security + EDR Protection 팩을 활성화하여 클라이언트 보호 계획에서 EDR(Endpoint Detection and Response) 기능을 제공할 수 있습니다.

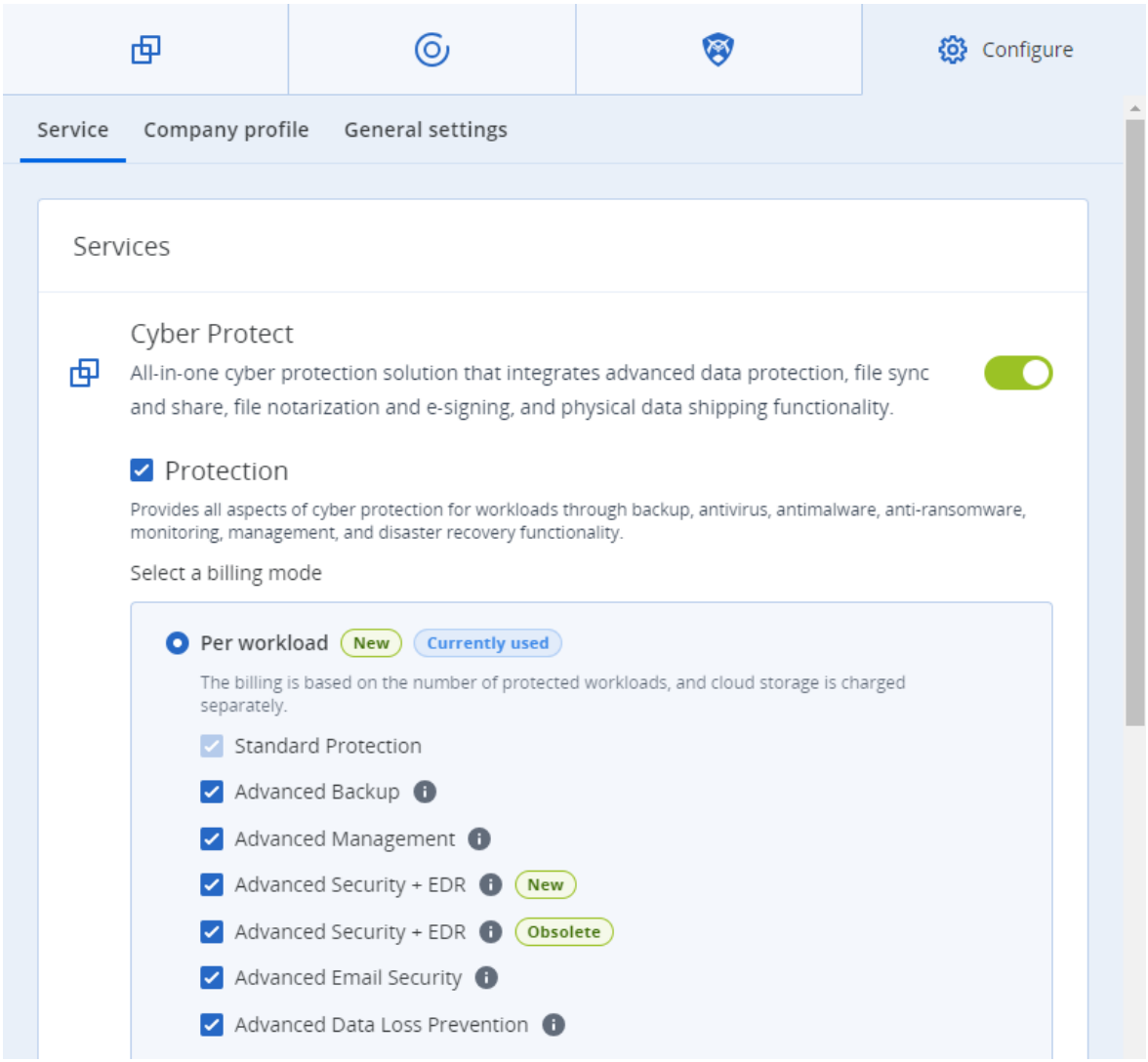
Advanced Security + EDR 팩을 활성화하려면

1. 관리 포털에 로그인합니다.

   참고
   메시지가 표시되면 Advanced Security + EDR Protection 팩을 활성화할 클라이언트를 선택하고 **활성화**를 클릭합니다.

2. 왼쪽 네비게이션 창에서 **클라이언트**를 클릭합니다.
3. Cyber Protect 아래에서 **보호** 탭을 클릭합니다.
   Protection 서비스에 가입한 기존 클라이언트 목록이 표시됩니다.
4. Advanced Security + EDR 팩을 추가할 관련 클라이언트를 선택합니다.

구성 탭의 **보호** 섹션에서 **Advanced Security + EDR** 확인란이 선택되어 있는지 확인합니다.



관리형 탐지 및 대응(MDR)

MDR에서는 엔드포인트 탐지 및 대응(EDR)에서 탐지된 보안 인시던트 조사 및 대응을 위한 추가 지원을 받아야 하거나 사내에 보안 전문가가 없는 MSP를 위한 연중 무휴 서비스를 제공합니다.

관리 포털의 Advanced Security + EDR 팩에서 MDR 기능을 활성화할 수 있습니다. MDR 서비스는 외부 MDR 공급업체가 제공합니다. 특정 고객을 대상으로 MDR을 활성화하면 해당 고객의 보호 계획에서 EDR이 활성화되어 있는 워크로드에 대해 아크로니스가 전송하는 EDR 인시던트 데이터가 MDR 공급업체에 수신됩니다. 그러면 MDR 공급업체가 다양한 수준의 서비스를 수행해 사용 가능한 대응 조치에 따라 인시던트를 분류합니다. 자세한 내용은 "관리형 탐지 및 대응(MDR) 소개"(126 페이지) 항목을 참조하십시오.

EDR 사용 방법에 대한 자세한 내용은 엔드포인트 탐지 및 대응(EDR)을 참조하십시오.

관리형 탐지 및 대응(MDR) 소개

서드 파티 벤더에서 제공하는 서비스인 MDR에서는 숙련된 분석가가 제공하는 분석 정보, 통합형 도구, 위협 인텔리전스, 해당 공급업체와 아크로니스의 기술 등을 활용하여 보안 위협 및 위반 발생 가능성을 모니터링하고 관련 대응 조치를 수행합니다.

관리 포털에서 고객을 대상으로 MDR을 활성화하면 MDR 공급업체가 인시던트 관련 조사와 대응 활동을 수행할 수 있도록 아크로니스가 공급업체에 인시던트 원격 측정 정보를 전달합니다. 이때 EDR을 통해 자동으로 완화되지 않는 인시던트만 MDR 공급업체로 전달됩니다.

MDR의 주요 컴포넌트

MDR의 세 가지 주 컴포넌트는 다음과 같습니다.

- 모니터링
- 분리
- 대응 및 해결

모니터링

MDR 공급업체는 고객 엔드포인트에서 EDR이 탐지한 보안 경보와 알림을 모니터링합니다. 모니터링 후에는 분석, 보안 오케스트레이션 및 대응 기능을 사용하여 이러한 경보와 일반적인 위협/위협 인텔리전스/서드 파티 위협 인텔리전스 간의 상관 관계를 설정하고 경보의 우선 순위를 지정합니다. 그리고 최종적으로는 경보나 알림이 보안 위반이나 손상에 해당하는지 여부를 결정합니다.

MDR 공급업체가 보안 위협 가능성이 있는 것으로 판단하는 보안 이벤트는 고객 관련 보안 인시던트로 에스컬레이션되며, 그러면 Cyber Protect 콘솔에서 해당 이벤트를 확인할 수 있게 됩니다. 공급업체는 보안 심각도 관련 상황 정보와 권장 해결 방법(이미 진행된 조치 포함)을 제공합니다.

분리

MDR 공급업체의 분석가가 사전 정의된 플레이북을 활용해 엔드포인트 분리를 위한 대응 조치를 시작합니다. MDR 공급업체가 수행하는 대응 조치는 관련 보안 인시던트에 반영됩니다. 엔드포인트의 데이터, 그리고 위협 인텔리전스 및 위협 조사 결과에서 제공되는 추가 입력을 검토하여 엔드포인트 분리 여부를 결정하게 됩니다.

대응 및 해결

초기 모니터링 및 분리 활동이 완료되면 대응 및 해결 활동이 진행됩니다. 보안 인시던트가 탐지되면 MDR 공급업체가 보안 인시던트에 따라 대응을 시작합니다. 구체적으로는 다음과 같은 대응 및 해결 활동이 진행됩니다.

- 제공된 데이터, 인텔리전스 및 권고를 토대로 보안 인시던트를 완화, 중지 또는 방지하는 방법과 관련된 지침 제시
- 보안 이벤트를 분석 및 조사하여 보안 손상의 근본 원인과 범위 확인
- MDR 공급업체의 대응 플레이북에 정의되어 있는 승인된 워크플로를 수행하여 워크로드 분리, 위협 격리 또는 위협 완전 해결

- 서비스 제공업체에 고객 관련 보안 인시던트, 위협 인텔리전스 및 권고 정보가 명시된 더욱 상세한 보안 에스컬레이션 과정 제공
- 다양한 채널을 통해 인시던트 에스컬레이션(보안 인시던트 생성, 고객이 제공한 연락처 상세 정보를 사용한 이메일 알림 및 전화 통화 포함)
- 위협이 완전히 해결될 때까지 고객과 지속적으로 연락하면서 새로운 정보가 확인되면 제때 업데이트 제공
- MDR 서비스 범위에 포함되지 않는 대응 조치를 수행해야 하는 경우에는 MDR 공급업체가 해당 조치를 중점적으로 진행해야 하는 영역 관련 권장 사항을 제공합니다. 가령 인시던트 대응 등의 추가 서비스 관련 권장 사항이 제공될 수 있습니다.

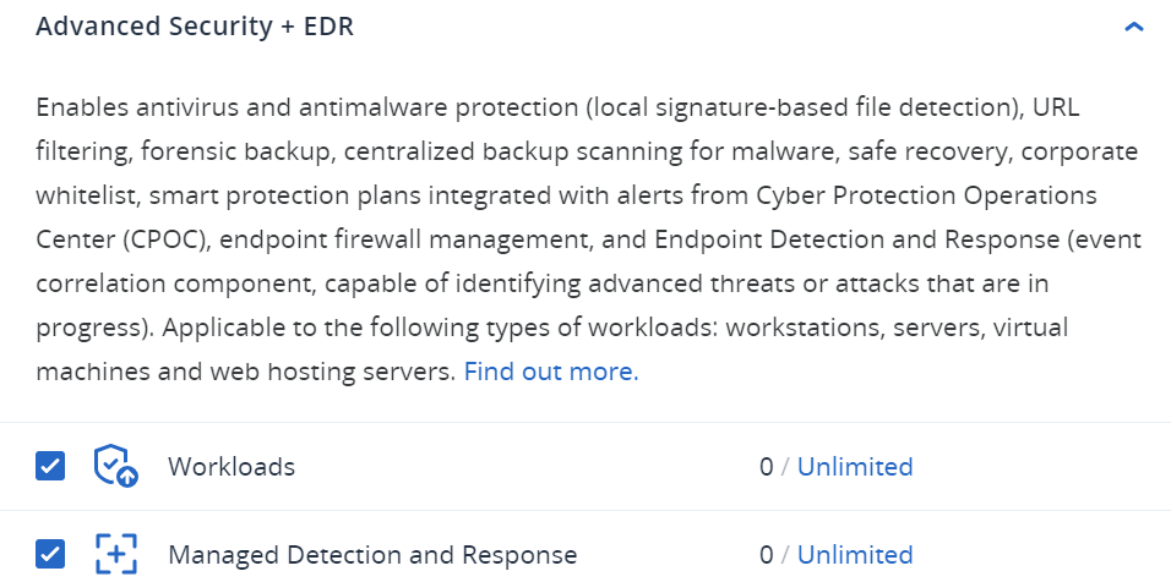
관리형 탐지 및 대응(MDR) 활성화

다음 2단계를 수행하면 선택한 고객을 대상으로 MDR을 활성화할 수 있습니다.

- 1단계: 고객의 MDR 제공 항목 활성화
- 2단계: MDR 공급업체 앱과의 통합 구성

선택한 고객을 대상으로 MDR을 활성화하려면

1. 관리 포털에서 **클라이언트**로 이동합니다.
2. 관련 고객 옆에 있는 말줄임표 아이콘(...)을 클릭하고 **구성**을 선택합니다.
3. **보호** 탭에서 **편집**을 클릭합니다.
4. **Advanced Security + EDR** 섹션에서 **워크로드**와 **관리형 탐지 및 대응** 확인란이 선택되어 있는지 확인한 후 **저장**을 클릭하여 변경 사항을 적용합니다.

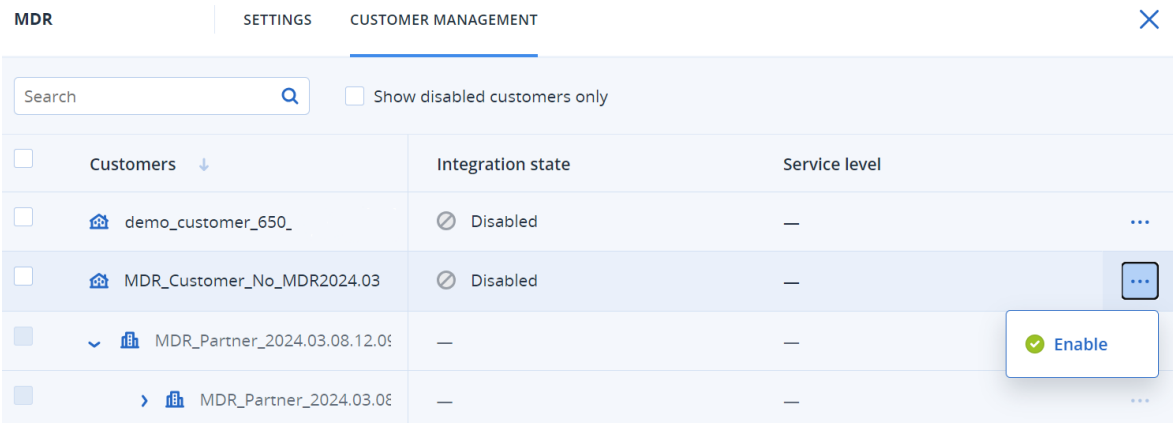


MDR 공급업체 앱과의 통합을 구성하려면

1. 관리 포털에서 **통합**으로 이동합니다.
2. 검색 창에서 MDR 공급업체 앱을 찾습니다.
3. 표시되는 MDR 카탈로그 카드에서 **구성**을 클릭합니다.

4. **설정** 탭에서 연필 아이콘을 클릭하고 파트너 연락처 1명 이상의 연락처 상세 정보를 입력합니다. 보안 이벤트가 탐지되면 MDR 공급업체가 해당 연락처에게 연락을 합니다. 연락처 최대 3명의 상세 정보를 추가할 수 있습니다. 입력을 완료한 후 **활성화**를 클릭합니다.

   보안 이벤트가 탐지되면 공급업체는 각 연락처에게 6번 전화를 한 후 연락이 되지 않으면 다음 연락처에게 연락을 합니다. 연락처와 통화를 마쳤거나 어떤 연락처와도 연락이 되지 않으면 공급업체는 에스컬레이션 및 인시던트 개요 정보가 포함된 이메일을 모든 연락처에게 전송합니다.
5. **고객 관리** 탭에서 관련 고객 정보의 맨 오른쪽 열에 표시된 말줄임표 아이콘(...)을 클릭한 후 **활성화**를 클릭합니다.



   여러 고객을 활성화하려면 관련 고객 옆의 확인란을 선택한 후 **고객 관리** 탭 왼쪽 위의 **활성화**를 클릭합니다.
6. 표시되는 대화 상자의 **서비스 수준** 드롭다운 목록에서 선택한 고객에게 적용하려는 MDR 서비스의 수준을 선택합니다.
   - **표준**: 공격 파악을 위한 연중 무휴 24시간 고객 엔드포인트 모니터링 서비스, AI 기반 이벤트 분류 및 우선 순위 지정, 위협 억제 및 영향 받는 엔드포인트 분리, 콘솔 내에서 우선 순위가 지정된 인시던트 목록을 실시간으로 확인하는 기능 등이 제공됩니다.
   - **고급**: **표준**에 포함된 기능과 함께 공격 롤백, 복구, 보안 격차 해소 등의 모든 문제 해결 기능도 제공됩니다.
7. **활성화**를 클릭하여 MDR 통합을 완료합니다.

   IP 허용 목록 기능이 활성화되어 있으면("웹 인터페이스에 대한 액세스 제한"(28페이지) 항목 참조) MDR 공급업체의 IP를 허용 목록에 추가하라는 메시지가 표시됩니다. IP를 허용 목록에 추가하면 공급업체가 관련 워크로드를 모니터링할 수 있습니다. 추가를 확인하려면 **활성화**를 클릭합니다.

   이제 MDR이 활성화되며, MDR 공급업체가 조사 및 대응 활동을 수행할 수 있도록 EDR 보안 인시던트가 공급업체에 전달됩니다. MDR 서비스에 대한 자세한 내용은 "관리형 탐지 및 대응(MDR) 소개"(126페이지) 항목을 참조하십시오.

관리형 탐지 및 대응(MDR) 비활성화

제공 항목 수준에서 MDR을 비활성화할 수 있으며 MDR 공급업체의 통합 앱에서 개별 고객을 대상으로 MDR을 비활성화할 수도 있습니다.

MDR 제공 항목을 비활성화하려면

1. 관리 포털에서 **클라이언트**로 이동합니다.
2. 관련 고객 옆에 있는 말줄임표 아이콘(...)을 클릭하고 **구성**을 선택합니다.
3. **보호** 탭에서 **편집**을 클릭합니다.
4. **Advanced Security + EDR** 섹션에서 **워크로드**와 **관리형 탐지 및 대응** 확인란이 선택되어 있지 않은지 확인한 후 **저장**을 클릭하여 변경 사항을 적용합니다.

   구성 탭에서 **Advanced Security + EDR** 서비스를 비활성화할 수도 있습니다. 그러면 MDR이 자동으로 비활성화됩니다.

MDR 공급업체의 통합 앱에서 개별 고객을 대상으로 MDR을 비활성화하려면

1. 관리 포털에서 **통합**으로 이동합니다.
2. 관련 MDR 공급업체 앱을 검색합니다.
3. 표시되는 MDR 카탈로그 카드에서 **구성**을 클릭합니다.
4. **고객 관리** 탭에서 관련 고객 정보의 맨 오른쪽 열에 표시된 말줄임표 아이콘(...)을 클릭한 후 **비활성화**를 선택합니다.

   여러 고객을 비활성화하려면 각 고객 왼쪽의 확인란을 선택한 후 **고객 관리** 탭 왼쪽 위의 **비활성화**를 클릭합니다.

관리형 탐지 및 대응(MDR)에서 사용 가능한 대응 조치

MDR에는 인시던트 수준에서 적용할 수 있는 다양한 대응 조치가 포함되어 있습니다.

MDR 보안 분석가가 대응 조치를 수행한 후 Cyber Protect 콘솔에 액세스하거나 API 호출을 실행하여 관련 조치를 적용합니다. 이러한 분석가는 **보안 분석가** 역할로 Cyber Protect콘솔에 로그인합니다.

모든 대응 조치는 **활동** 목록에 기록됩니다. 고객은 수행된 대응 조치 및 이러한 활동의 상태(진행중/성공/실패) 목록을 확인할 수 있습니다. **시작한 사람** 열에는 조치를 시작한 사용자(파트너 사용자, 고객 사용자, MDR 보안 분석가)가 표시됩니다. 자세한 내용은 엔드포인트 탐지 및 대응(EDR) 사용 방법을 참조하십시오.

참고

대응 조치 목록, 그리고 엔드포인트 탐지 및 대응(EDR) 설명서에서 해당 조치의 설명이 포함된 관련 섹션에 대한 참조가 아래 표에 나와 있습니다.

대응 조치	추가 정보
조사 상태 변경	상태는 다음 중 하나로 설정할 수 있습니다. • **조사 중** • **닫힘** • **위양성** 조사 상태를 변경하는 방법에 대한 자세한 내용은 사이버 킬 체인에서 인시던트를 조사하는 방법을 참조하십시오.

대응 조치	추가 정보
네트워크 분리	MDR 보안 분석가는 다음 작업을 수행할 수 있습니다. • 워크로드 분리 • 워크로드 분리 해제 • 분리 상태 확인 워크로드 분리에 대한 자세한 내용은 워크로드의 네트워크 분리 관리를 참조하십시오.
주석 추가	MDR 보안 분석가는 인시던트 관련 사이버 킬 체인에서 **주석 게시**를 클릭하여 인시던트에 주석을 추가할 수 있습니다. 이러한 주석은 특정 인시던트의 **활동** 탭에 표시됩니다. 자세한 내용은 인시던트를 완화하기 위해 수행된 조치 파악을 참조하십시오.
프로세스/프로세스 트리 중지	이 조치는 전체 인시던트에 적용될 수 있습니다. 인시던트가 발생했던 프로세스가 이미 중지되었더라도 대응 조치를 트리거할 수 있습니다. 대응 조치가 처리되고 나면 비동기 응답이 전송됩니다. 다음 응답 중 하나가 전송될 수 있습니다. • 성공: 모든 프로세스가 정상적으로 중지되었습니다. • 경고와 함께 성공: 일부 프로세스가 정상적으로 중지되었거나, 중지할 프로세스가 없거나, MDR 외부에서 프로세스가 중지되었습니다. • 오류: 프로세스가 중지되지 않았습니다. 프로세스 또는 프로세스 트리를 중지하는 방법에 대한 자세한 내용은 의심스러운 프로세스에 대한 대응 조치 정의를 참조하십시오.
격리	이 조치는 전체 인시던트에 적용될 수 있습니다. 파일이나 프로세스가 이미 격리되었더라도 대응 조치를 트리거할 수 있습니다. 대응 조치가 처리되고 나면 비동기 응답이 전송됩니다. 다음 응답 중 하나가 전송될 수 있습니다. • 성공: 모든 파일과 프로세스가 정상적으로 격리되었습니다.

대응 조치	추가 정보
	• 경고와 함께 성공: 일부 파일과 프로세스가 정상적으로 격리되었거나, 격리할 파일이나 프로세스가 없거나, MDR 외부에서 파일이나 프로세스가 격리되었습니다. • 오류: 파일이나 프로세스가 격리되지 않았습니다. 프로세스를 격리하는 방법에 대한 자세한 내용은 의심스러운 프로세스에 대한 대응 조치 정의를 참조하십시오. 파일을 격리하는 방법에 대한 자세한 내용은 의심스러운 파일에 대한 대응 조치 정의를 참조하십시오.
파일 삭제	이 조치는 전체 인시던트에 적용될 수 있습니다. 파일이 이미 삭제되었더라도 대응 조치를 트리거할 수 있습니다. 대응 조치가 처리되고 나면 비동기 응답이 전송됩니다. 다음 응답 중 하나가 전송될 수 있습니다. • 성공: 모든 파일이 정상적으로 삭제되었습니다. • 경고와 함께 성공: 일부 파일이 정상적으로 삭제되었거나, 삭제할 파일이 없거나, MDR 외부에서 파일이 삭제되었습니다. • 오류: 파일이 삭제되지 않았습니다. 파일을 삭제하는 방법에 대한 자세한 내용은 의심스러운 파일에 대한 대응 조치 정의를 참조하십시오.
워크로드 다시 시작	워크로드를 다시 시작할 때까지의 시간 간격을 설정하거나 워크로드를 즉시 다시 시작할 수 있습니다. 워크로드를 다시 시작하는 방법에 대한 자세한 내용은 워크로드 다시 시작을 참조하십시오.
허용 목록/차단 목록에 URL, 파일 또는 프로세스 추가	기본 계획(워크로드에 현재 할당되어 있는 계획)의 허용 목록/차단 목록에 URL, 파일 또는 프로세스를 추가합니다. 대응 조치가 처리되고 나면 비동기 응답이 전송됩니다. 다음 응답 중 하나가 전송될 수 있습니다.

대응 조치	추가 정보
	• 성공: 모든 URL, 파일 및 프로세스가 정상적으로 추가되었습니다. • 경고와 함께 성공: 일부 URL, 파일, 및 프로세스만 정상적으로 추가되었으며 허용 목록에 이미 포함되어 있는 항목 등의 일부 항목은 추가되지 않았습니다. • 오류: 작업이 실패했습니다. 허용 목록과 차단 목록에 URL, 파일, 또는 프로세스를 추가하는 방법에 대한 자세한 내용은 보호 계획 차단 목록 또는 허용 목록에 프로세스, 파일 또는 네트워크 추가를 참조하십시오.

Advanced Disaster Recovery

Advanced Disaster Recovery 팩을 활성화할 수 있으며 전체 Disaster Recovery 기능을 사용하여 워크로드를 보호할 수 있습니다.

다음과 같은 고급 재해 복구 기능을 사용할 수 있습니다.

- 운영 장애 조치
- 격리된 네트워크에서의 테스트 장애 조치.
- 장애 조치에 사용 가능한 복구 지점 수: 복구 서버 생성 후 제공되는 모든 복구 지점을 사용할 수 있습니다.
- 기본 서버
- 복구/기본 서버 구성: 제한 없음
- 제공되는 연결 모드: 클라우드 전용, 지점 및 사이트 간, 사이트 간 OpenVPN, 다중 사이트 IPsec VPN.
- VPN 게이트웨이 가용성: 항상 사용 가능합니다.
- 클라우드 네트워크 수: 23.
- 공용 IP 주소
- 인터넷 액세스
- 실행서 관련 작업: 생성, 편집 및 실행.

Advanced Email Security

Advanced Email Security 팩은 Microsoft 365, Google Workspace 또는 Open-Xchange 사서함에 대한 실시간 보호 기능을 제공합니다.

- 안티맬웨어 및 안티스팸
- 이메일에서 URL 검색
- DMARC 분석

- 피싱 방지
- 가장 보호
- 첨부 파일 검사
- 컨텐츠 무해화 및 재구성
- 신뢰 그래프

Microsoft 365 협업 앱 시트도 활성화할 수 있습니다. 그러면 콘텐츠 기반 보안 위협으로부터 Microsoft 365 클라우드 협업 애플리케이션을 보호할 수 있습니다. 이러한 애플리케이션으로는 OneDrive, SharePoint, Teams 등이 있습니다.

Advanced Email Security는 워크로드나 용량(기가바이트) 단위로 활성화할 수 있으며, 활성화 단위에 따라 라이선스 모델이 달라집니다.

Advanced Email Security 데이터시트에서 Advanced Email Security에 대해 자세히 알 수 있습니다.

구성 지침은 Perception Point가 포함된 Advanced Email Security를 참조하십시오.

Advanced Backup

Advanced Backup 팩을 활성화하여 고급 백업 및 복구 기능으로 워크로드를 보호할 수 있습니다.

사용 가능한 기능은 다음과 같습니다.

- 원클릭 복구
- 지속적인 데이터 보호
- Microsoft SQL Server 클러스터 및 Microsoft Exchange 클러스터의 백업 지원 - Always On 가용성 그룹(AAG) 및 데이터베이스 가용성 그룹(DAG)
- MariaDB, MySQL, Oracle DB 및 SAP HANA의 백업 지원
- 데이터 보호 맵 및 규제 준수 보고
- 오프호스트 데이터 처리
- Microsoft 365 및 Google Workspace 워크로드의 백업 빈도
- 부트 가능한 미디어를 사용한 원격 작업
- Microsoft Azure 퍼블릭 클라우드 스토리지에 직접 백업

Advanced Management

Advanced Management를 사용하면 속도와 반응성이 우수하며 대다수 문제를 사전에 방지해 주는 관리 인프라를 빌드할 수 있습니다.

Advanced Management 팩에는 다음 기능이 포함되어 있습니다.

- **소프트웨어 인벤토리** - 클라이언트가 사용하는 전체 소프트웨어 목록을 확인할 수 있으므로 업데이트 준비, 계획 또는 추적 시간을 단축하고 작업량을 줄일 수 있습니다.
- **패치 자동 관리** - 취약성을 익스플로잇 전에 수정할 수 있습니다.
- **페일세이프 패치** - 패칭 전에 자동 시스템 백업을 수행하여 결함이 있는 패치가 적용된 워크로드를 빠르고 쉽게 복구할 수 있습니다.

- **머신 러닝 기반 모니터링 및 스마트 경보 생성** - 예측 모니터링을 수행하고 경보를 생성하여 모니터링 작업을 최적화하고 운영상의 위험을 완화할 수 있습니다.
- **즉시 사용 가능한 Cyber Scripting 기능** - 일상적인 작업을 자동으로 간편하게 처리할 수 있습니다.
- **드라이브 상태 모니터링** - 예측 모니터링 기능과 경보를 활용하여 드라이브 고장으로 인해 발생하는 다운타임을 사전에 완화할 수 있습니다.
- **원격 데스크탑 및 원격 지원** - 원격 워크로드에 액세스하여 기술적인 문제를 빠르게 해결할 수 있습니다. 대역폭이 제한되는 상황에서도 우수한 성능이 보장되므로 안정적인 지원을 받을 수 있으며 작업 시간도 절약할 수 있습니다. Windows, macOS, Linux 등의 더욱 다양한 플랫폼이 지원될 뿐 아니라 세션 녹화, 원격 작업, 파일 전송, 모니터링, 보고, 여러 보기에서 워크로드 관찰 등을 위한 확장 기능도 제공됩니다.

통합

서드 파티 시스템과의 통합

서비스 제공자는 Cyber Protect Cloud와 타사 시스템을 다음과 같이 통합할 수 있습니다.

- 이 시스템에 플랫폼 확장자 설정.

  관리 포털의 **통합** 페이지에는 가장 널리 사용되는 PSA(Professional Services Automations) 및 RMM(Remote Monitoring and Management) 시스템에 대해 사용할 수 있는 확장자가 나열됩니다.

  이는 권장되는 플랫폼 통합 방법입니다.
- 시스템에 대한 API 클라이언트를 생성하고 시스템이 플랫폼과 그 서비스의 API(애플리케이션 프로그래밍 인터페이스)에 액세스하도록 허용. API 클라이언트는 플랫폼의 OAuth 2.0 인증 프레임워크의 일부입니다.OAuth 2.0에 대한 자세한 내용은 https://tools.ietf.org/html/rfc6749를 참조하십시오.

  이는 프로그래밍 기술이 필요한 하위 수준의 플랫폼 통합 방법입니다. 시스템에 대한 플랫폼 확장자가 없거나, 시스템이 사용 가능한 확장자가 지원되지 않는 플랫폼 및 서비스를 관리하는 사례에 대해 사용자 정의된 경우 이 방법을 선택하는 것이 권장됩니다.

Cyber Protect Cloud용 통합 설정

1. 관리 포털에 로그인합니다.
2. 기본 네비게이션 메뉴에서 **통합**으로 이동합니다.
3. 통합을 활성화할 서드 파티 시스템 이름을 클릭합니다.
4. 화면에 나타나는 지침을 따릅니다.

https://solutions.acronis.com에서 타사 시스템을 통합할 때 사용 가능한 방법(단계별 설명서 포함)과 관련된 자세한 내용을 확인할 수 있습니다.

API 클라이언트 관리

타사 시스템은 API(애플리케이션 프로그래밍 인터페이스)를 사용하여 Cyber Protect Cloud에 통합될 수 있습니다. 이러한 API에 대한 액세스는 플랫폼의 OAuth 2.0 인증 프레임워크의 필수 부분인 API 클라이언트를 통해 활성화됩니다.

API 클라이언트란 무엇입니까?

API 클라이언트 플랫폼과 그 서비스의 API에 있는 데이터에 액세스할 수 있도록 인증하고 인증받기 위해 필요한 타사 시스템을 나타내기 위한 특별 플랫폼 계정입니다.

클라이언트의 액세스는 관리자가 클라이언트를 생성하는 테넌트와 하위 테넌트로 제한되어 있습니다.

클라이언트는 생성될 때 관리자 계정의 서비스 역할을 상속하며 그러한 역할은 이후에 변경될 수 없습니다. 관리자 계정의 역할을 변경하거나 관리자 계정을 비활성화해도 클라이언트는 영향을 받지 않습니다.

클라이언트 자격 증명은 고유 식별자(ID)와 암호 값으로 구성됩니다. 자격 증명은 만료되지 않고 관리 포털이나 서비스 콘솔에 로그인하는 데 사용될 수 없습니다. 암호 값은 재설정될 수 있습니다.

클라이언트에 대해 2단계 인증을 활성화할 수 없습니다.

일반적인 통합 절차

1. 관리자는 타사 시스템이 관리하는 테넌트에서 API 클라이언트를 생성합니다.
2. 관리자는 타사 시스템에서 OAuth 2.0 클라이언트 자격 증명 플로우를 활성화합니다.
   이 플로우에 따르면 API를 통해 테넌트와 그 서비스에 액세스하기 전에, 시스템은 먼저 인증 API를 사용하여 생성된 클라이언트의 자격 증명을 플랫폼으로 전송해야 합니다. 플랫폼은 이 특정 클라이언트에 할당된 고유 암호 문자열인 보안 토큰을 생성하여 되돌려 보냅니다. 그다음 시스템은 이 토큰을 모든 API 요청에 추가해야 합니다.
   보안 토큰을 사용하면 API 요청에 클라이언트 자격 증명을 전송할 필요가 없습니다. 추가적인 보안을 위해 토큰은 두 시간 내에 만료됩니다. 이후 토큰이 만료된 모든 API 요청은 실패하게 되며 시스템은 플랫폼에서 새로운 토큰을 요청해야 합니다.

인증 API 및 플랫폼 API 사용에 대한 자세한 내용은 개발자 안내서 https://developer.acronis.com/doc/account-management/v2/guide/index를 참조하십시오.

API 클라이언트 생성

1. 관리 포털에 로그인합니다.
2. **설정** > **API 클라이언트** > **API 클라이언트 생성**을 클릭합니다.
3. API 클라이언트의 이름을 입력합니다.
4. **다음**을 클릭합니다.
   기본적으로 API 클라이언트는 **활성** 상태로 생성됩니다.
5. 클라이언트의 ID와 암호 값, 데이터 센터 URL을 복사 및 저장합니다. 타사 시스템에서 OAuth 2.0 클라이언트 자격 증명 플로우를 활성화할 때 필요합니다.

   중요
   보안상의 이유로 암호 값은 한 번만 표시됩니다. 이 값을 잃어버리면 다시 가져올 수 없습니다. 재설정만 가능합니다.

6. **완료**를 클릭합니다.

API 클라이언트의 암호 값 재설정

1. 관리 포털에 로그인합니다.
2. **설정** > **API 클라이언트**를 클릭합니다.
3. 목록에서 필요한 클라이언트를 찾습니다.

4. 을 클릭한 다음, **암호 재설정**을 클릭합니다.
5. **다음**을 클릭하여 결정을 확인합니다.
   새 암호 값이 생성됩니다. 클라이언트 ID와 데이터 센터 URL은 변경되지 않습니다.
   이 클라이언트에 할당된 모든 보안 토큰은 즉시 만료되며 이러한 토큰이 있는 API 요청은 실패합니다.
6. 클라이언트의 새 암호 값을 복사 및 저장합니다.

   중요
   보안상의 이유로 암호 값은 한 번만 표시됩니다. 이 값을 잃어버리면 다시 가져올 수 없습니다. 재설정만 가능합니다.

7. **완료**를 클릭합니다.

API 클라이언트 비활성화

1. 관리 포털에 로그인합니다.
2. **설정** > **API 클라이언트**를 클릭합니다.
3. 목록에서 필요한 클라이언트를 찾습니다.
4. 을(를) 클릭한 다음 **비활성화**를 클릭합니다.
5. 결정을 확인합니다.
   클라이언트의 상태가 **비활성화됨**으로 변경됩니다.
   이 클라이언트에 할당된 보안 토큰이 있는 API 요청은 실패하지만, 토큰이 즉시 만료되지는 않습니다. 클라이언트를 비활성화해도 토큰의 만료 시간은 영향을 받지 않습니다.
   언제든 클라이언트를 다시 활성화할 수 있습니다.

비활성화된 API 클라이언트 활성화

1. 관리 포털에 로그인합니다.
2. **설정** > **API 클라이언트**를 클릭합니다.
3. 목록에서 필요한 클라이언트를 찾습니다.
4. 을(를) 클릭한 다음 **활성화**를 클릭합니다.
   클라이언트의 상태가 **활성**으로 변경됩니다.
   이 클라이언트에 할당된 보안 토큰이 만료되지 않으면 이러한 토큰이 있는 API 요청은 성공합니다.

API 클라이언트 삭제

1. 관리 포털에 로그인합니다.
2. **설정** > **API 클라이언트**를 클릭합니다.
3. 목록에서 필요한 클라이언트를 찾습니다.

4. 을(를) 클릭한 다음 **삭제**를 클릭합니다.
5. 결정을 확인합니다.
   이 클라이언트에 할당된 모든 보안 토큰은 즉시 만료되며 이러한 토큰이 있는 API 요청은 실패합니다.

중요
삭제된 클라이언트는 복구할 수 있는 방법이 없습니다.

통합 참조

통합 카탈로그에서 통합 설명서를 확인할 수 있습니다.

필요한 설명서를 찾으려면

1. https://solutions.acronis.com을 방문합니다.
2. 필요한 통합을 선택하고 **자세히 알아보기**를 클릭합니다.
   페이지 위쪽에 작업 방법 문서나 안내서의 링크가 있습니다.

https://www.acronis.com/support/documentation/의 **통합 참조**에서 아크로니스가 개발한 통합의 설명서를 확인할 수도 있습니다.

VMware Cloud Director 통합

서비스 공급자는 VMware Cloud Director(이전 명칭 VMware vCloud Director)을(를) Cyber Protect Cloud과(와) 통합할 수 있으며, 고객의 가상 머신용으로 즉시 사용 가능한 백업 솔루션을 제공할 수 있습니다.

통합 시에는 다음 단계를 수행합니다.

1. VMware Cloud Director 환경용으로 RabbitMQ 메시지 브로커를 구성합니다.
   RabbitMQ에서는 SSO(Single Sign-On) 기능을 제공하므로 VMware Cloud Director 자격 증명을 사용하여 Cyber Protect 콘솔에 로그인할 수 있습니다.
   Cyber Protect Cloud 23.05(2023년 5월 출시) 이하 버전에서는 VMware Cloud Director 환경의 변경 사항을 Cyber Protect Cloud에 동기화할 때도 RabbitMQ가 사용됩니다.
2. 관리 에이전트를 디플로이합니다.
   관리 에이전트 디플로이 중에는 VMware Cloud Director용 플러그인도 설치됩니다. 해당 플러그인이 설치되면 사용자 인터페이스에 Cyber Protection이(가) 추가됩니다.
   관리 에이전트는 Cyber Protect Cloud의 고객 테넌트에 VMware Cloud Director 조직을 매핑하며 고객 테넌트 관리자에 조직 관리자를 매핑합니다. 조직에 대한 자세한 내용은 VMware 지식 베이스에서 VMware Cloud Director에서 조직 생성을 참조하십시오.
   고객 테넌트는 VMware Cloud Director 통합 구성 대상 파트너 테넌트 내에 생성됩니다. 이러한 신규 고객 테넌트는 **잠김** 모드로 설정되므로 파트너 관리자가 Cyber Protect Cloud 내에서 관리할 수 없습니다.

참고
VMware Cloud Director에 고유한 이메일 주소가 있는 조직 관리자만 Cyber Protect Cloud에 매핑됩니다.

3. 백업 에이전트를 하나 이상 디플로이합니다.
   백업 에이전트는 VMware Cloud Director 환경의 가상 머신용 백업 및 복구 기능을 제공합니다.

VMware Cloud Director 및 Cyber Protect Cloud 간의 통합을 비활성화하려면 기술 지원에 문의하십시오.

제한 사항

- VMware Cloud Director과(와)의 통합은 **서비스 공급자가 관리함** 관리 모드 상태의 파트너 테넌트에서만 가능합니다. 이러한 파트너 테넌트의 상위 테넌트(있는 경우) 역시 **서비스 공급자가 관리함** 관리 모드를 사용해야 합니다. 테넌트 유형 및 테넌트의 관리 모드에 대한 자세한 내용은 "테넌트 생성"(33페이지)을(를) 참조하십시오.
  모든 기존 직접 파트너는 VMware Cloud Director과(와)의 통합을 구성할 수 있습니다. 파트너 관리자는 자식 테넌트를 대상으로 이 옵션을 활성화할 수도 있습니다. 이렇게 하려면 자식 파트너 테넌트를 생성할 때 **파트너 소유 VMware Cloud Director 인프라** 확인란을 선택하면 됩니다.
- VMware Cloud Director과(와)의 통합이 구성되어 있는 파트너 테넌트에서는 2단계 인증을 비활성화해야 합니다.
- 여러 VMware Cloud Director 조직에서 조직 관리자 역할이 할당되어 있는 관리자는 Cyber Protection에서 고객 테넌트 하나의 백업 및 복구만 관리할 수 있습니다.
- Cyber Protect 콘솔은 새 탭에서 열립니다.

소프트웨어 요구 사항

지원되는 VMware Cloud Director 버전

- VMware Cloud Director 10.4, 10.5

지원되는 웹 브라우저

- Google Chrome 29 이상 버전
- Mozilla Firefox 23 이상 버전
- Opera 16 이상 버전
- Microsoft Edge 25 이상 버전
- macOS 및 iOS 운영 체제에서 실행되는 Safari 8 이상

다른 웹 브라우저(다른 운영 체제에서 실행 중인 Safari 포함)에서는 사용자 인터페이스가 제대로 표시되지 않거나 일부 기능을 사용하지 못할 수 있습니다.

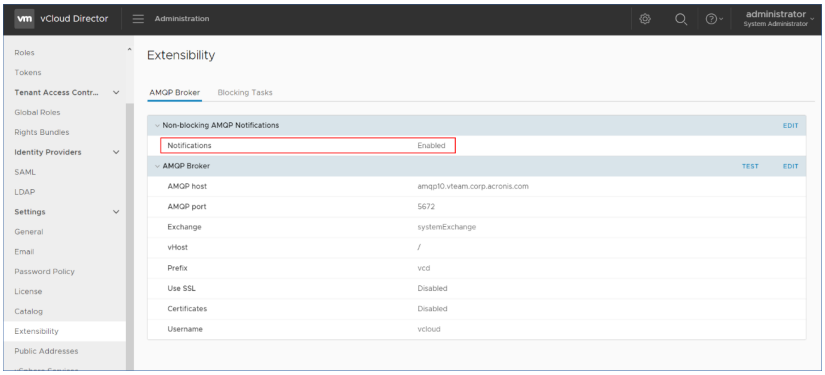
RabbitMQ 메시지 브로커 구성

이 절차는 Cyber Protect Cloud의 버전에 따라 달라집니다. 버전 23.06(2023년 6월 출시) 이상에는 간소화된 절차가 사용됩니다.

RabbitMQ 메시지 브로커 구성 방법

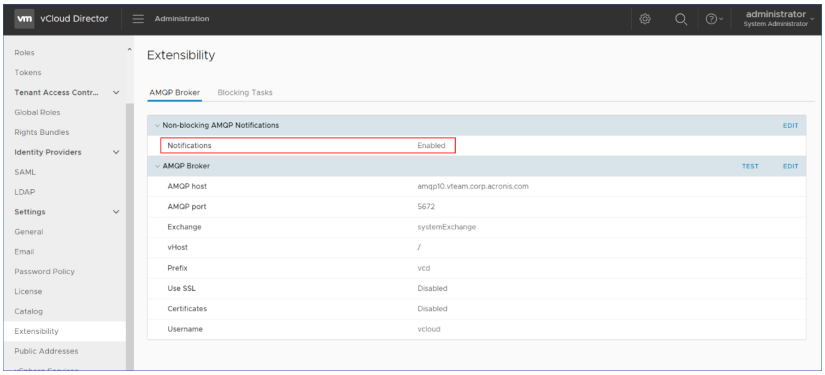
*버전 **23.06** 이상*

1. VMware Cloud Director 환경용 RabbitMQ AMQP 브로커를 설치합니다.
   RabbitMQ를 설치하는 방법에 대한 자세한 내용은 VMware 설명서의 RabbitMQ AMQP 브로커 설치 및 구성을 참조하십시오.
2. VMware Cloud Director 공급자 포털에 시스템 관리자로 로그인합니다.
3. **관리** > **확장성**으로 이동하여 **비차단 AMQP 알림** 아래에서 **알림**이 활성화되어 있는지 확인합니다.



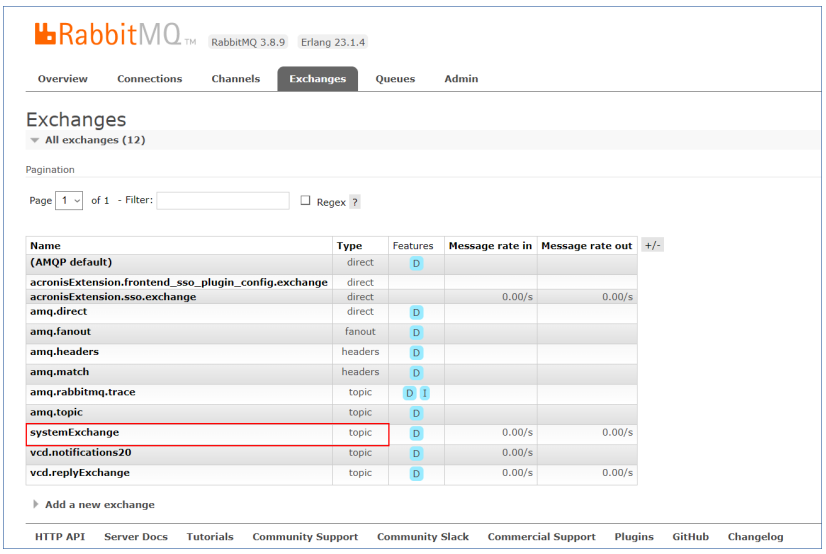
*버전 **23.05** 이하*

1. VMware Cloud Director 환경용 RabbitMQ AMQP 브로커를 설치합니다.
   RabbitMQ를 설치하는 방법에 대한 자세한 내용은 VMware 설명서의 RabbitMQ AMQP 브로커 설치 및 구성을 참조하십시오.
2. VMware Cloud Director 공급자 포털에 시스템 관리자로 로그인합니다.
3. **관리** > **확장성**으로 이동하여 **비차단 AMQP 알림** 아래에서 **알림**이 활성화되어 있는지 확인합니다.



4. RabbitMQ 관리 콘솔에 관리자로 로그인합니다.

5. **교환** 탭에서 교환(기본 이름은 **SystemExchange**)이 생성되었으며 교환 유형이 **항목**인지 확인합니다.



VMware Cloud Director용 플러그인 설치 및 게시

관리 에이전트를 설치하면 VMware Cloud Director용 플러그인이 자동으로 설치됩니다.

그러나 Cyber Protection을(를) 사용할 테넌트에 해당 플러그인을 수동으로 게시해야 합니다.

VMware Cloud Director용 플러그인을 게시하려면

1. VMware Cloud Director 공급자 포털에 시스템 관리자로 로그인합니다.
2. 탐색 메뉴에서 **포털 사용자 정의**를 선택합니다.
3. **플러그인** 탭에서 **Cyber Protection** 플러그인을 선택하고 **게시**를 클릭합니다.
4. 게시 범위를 구성합니다.
   a. **대상 범위** 섹션에서 **테넌트** 확인란만 선택합니다.
   b. **게시 대상** 섹션에서 **모든 테넌트**를 선택하여 모든 기존 테넌트와 향후 생성할 테넌트에 대해 플러그인을 활성화하거나, 플러그인을 활성화할 개별 테넌트를 선택합니다.
5. **저장**을 클릭합니다.
6. **신뢰**를 클릭합니다.

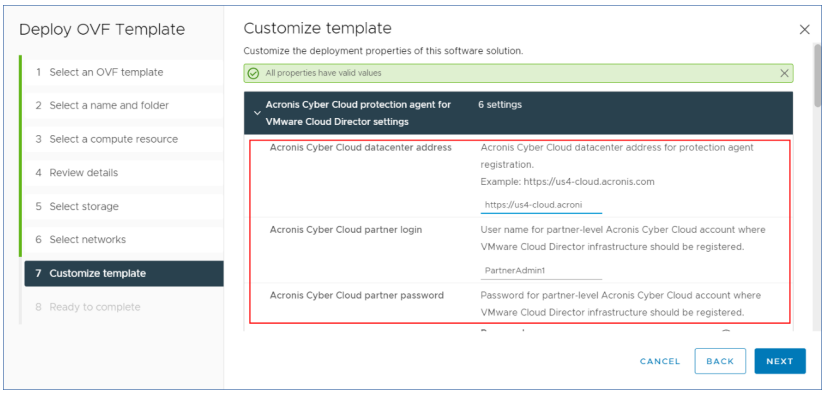
관리 에이전트 설치

1. Cyber Protect Cloud 관리 포털에 파트너 관리자로 로그인합니다.
2. **설정** > **위치**로 이동하여 **추가VMware Cloud Director**를 클릭합니다.
3. **릴리스 채널** 드롭다운 목록에서 에이전트 버전을 선택합니다. 다음 옵션을 사용할 수 있습니다.
   - **현재** - 최신 버전입니다.
   - **안정적** - 이전 릴리스의 버전입니다.
4. **관리 에이전트** 링크를 클릭하여 ZIP 파일을 다운로드합니다.

5. 관리 에이전트 템플릿 파일 `vCDManagementAgent.ovf` 및 가상 하드 디스크 파일 `vCDManagementAgent-disk1.vmdk`를 추출합니다.
6. vSphere Client에서 관리 에이전트 OVF 템플릿을 VMware Cloud Director에서 관리하는 vCenter 인스턴스 아래의 ESXi 호스트에 디플로이합니다.

중요
관리 에이전트는 VMware Cloud Director 환경당 하나만 설치합니다.

7. **OVF 템플릿 디플로이** 마법사에서 다음 항목을 설정하여 관리 에이전트를 구성합니다.



a. Cyber Protect Cloud 데이터 센터의 URL. 예를 들어 `https://us5-cloud.example.com` 등을 입력할 수 있습니다.
b. 파트너 관리자 로그인 및 비밀번호.
c. VMware Cloud Director 환경의 가상 머신용 백업 스토리지의 ID. 이 백업 스토리지로는 파트너 소유의 스토리지만 사용할 수 있습니다. 스토리지에 대한 자세한 내용은 "위치 및 스토리지 관리"(66페이지)을(를) 참조하십시오.
ID를 확인하려면 관리 포털에서 **설정** > **위치**로 이동하여 원하는 스토리지를 선택합니다. 스토리지 ID는 URL의 **uuid=** 부분 뒤에서 확인 가능합니다.
d. Cyber Protect Cloud 청구 모드: **기가바이트당** 또는 **워크로드당**.

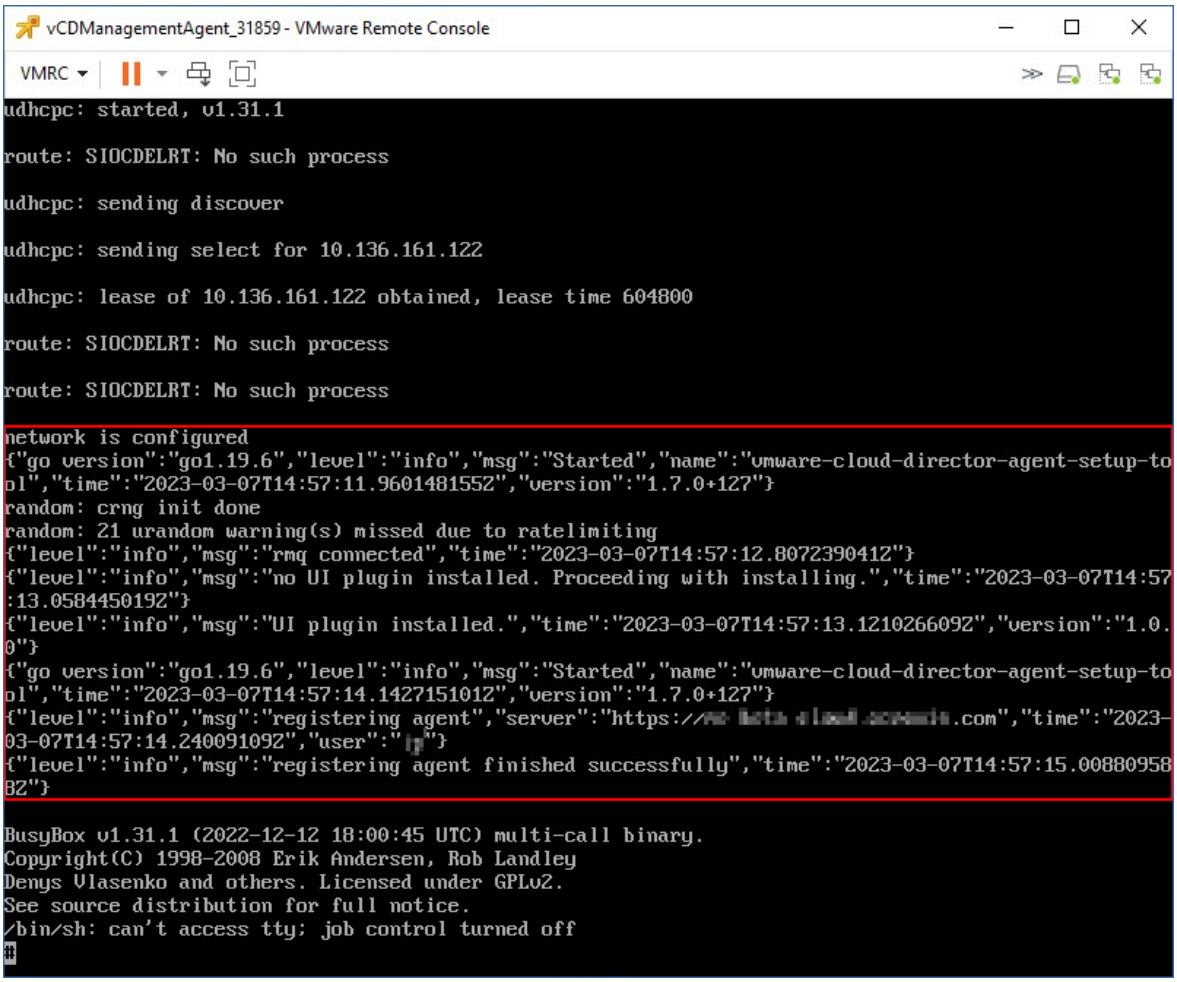
참고
선택한 청구 모드는 새로 생성하는 모든 고객 테넌트에 적용됩니다.

e. VMware Cloud Director 매개변수: 인프라 주소, 시스템 관리자 로그인 및 비밀번호.
f. RabbitMQ 매개변수: 관리자 로그인 및 암호.
g. 에이전트가 있는 가상 머신의 루트 사용자의 암호입니다.
h. 네트워크 매개변수: IP 주소, 서브넷 마스크, 기본 게이트웨이, DNS, DNS 접미부.
기본적으로는 네트워크 인터페이스 하나만 활성화됩니다. 두 번째 네트워크 인터페이스를 활성화하려면 **eth1 활성화** 옆의 확인란을 선택합니다.

참고
관리 에이전트가 VMware Cloud Director 환경과 Cyber Protect Cloud 데이터 센터에 모두 액세스할 수 있도록 네트워크 설정을 지정해야 합니다.

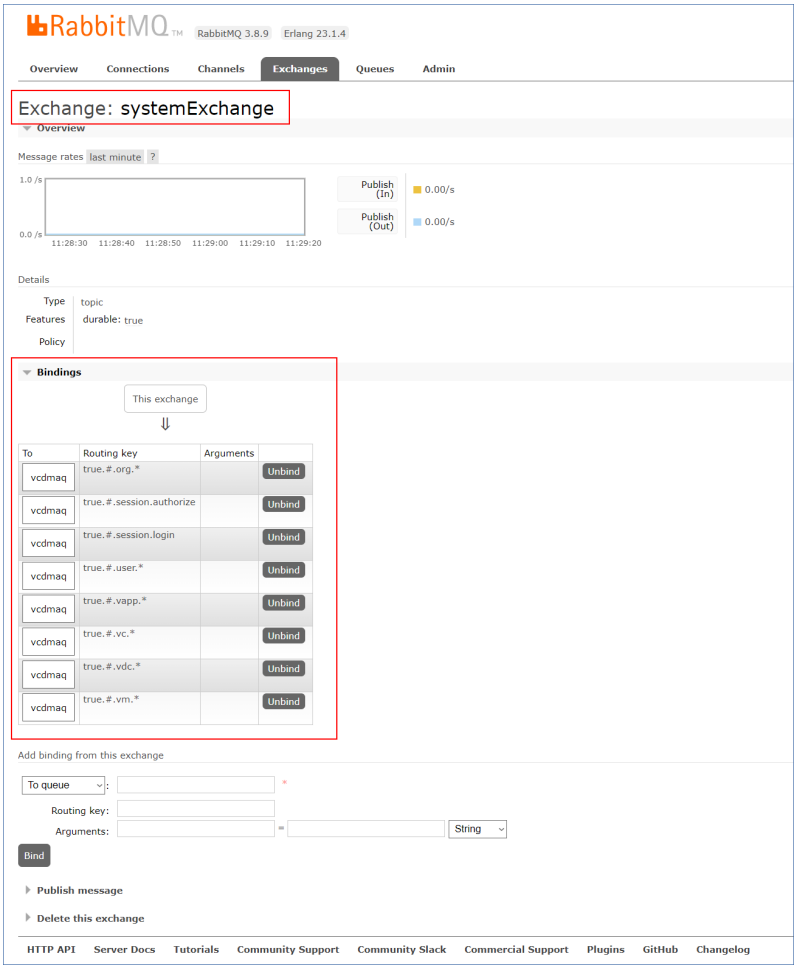
초기 디플로이 후에 관리 에이전트 설정을 구성할 수도 있습니다. vSphere Client에서 관리 에이전트가 설치된 가상 머신의 전원을 끈 다음 **구성** > **설정** > **vApp 옵션**을 클릭합니다. 원하는 설정을 적용한 후 관리 에이전트가 설치된 가상 머신의 전원을 켭니다.

8. [선택 사항] vSphere Client에서 관리 에이전트가 설치된 가상 머신의 콘솔을 열고 설정을 확인합니다.



9. RabbitMQ 연결을 확인합니다.
   a. RabbitMQ 관리 콘솔에 관리자로 로그인합니다.
   b. **교환** 탭에서 RabbitMQ 설치 중에 설정한 교환을 선택합니다. 해당 교환의 기본 이름은 **systemExchange**입니다.

c. **vcdmaq** 큐에 대한 바인딩을 확인합니다.



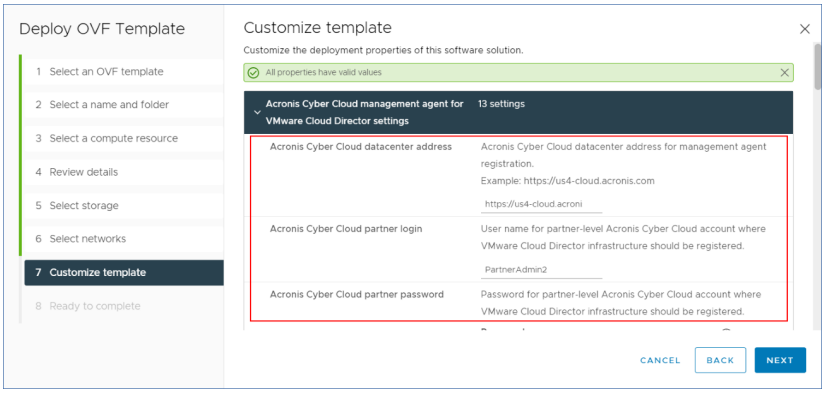
백업 에이전트 설치

1. 관리 포털에 파트너 관리자로 로그인합니다.
2. **설정** > **위치**로 이동하여 **추가VMware Cloud Director**를 클릭합니다.
3. **릴리스 채널** 드롭다운 목록에서 에이전트 버전을 선택합니다. 다음 옵션을 사용할 수 있습니다.
   - **현재** - 최신 버전입니다.
   - **안정적** - 이전 릴리스의 버전입니다.
4. **백업 에이전트** 링크를 클릭하여 ZIP 파일을 다운로드합니다.
5. 백업 에이전트 템플릿 파일 `vCDCyberProtectAgent.ovf` 및 가상 하드 디스크 파일 `vCDCyberProtectAgent-disk1.vmdk`를 추출합니다.
6. vSphere Client에서 백업 에이전트 템플릿을 원하는 ESXi 호스트에 디플로이합니다.
   호스트당 백업 에이전트 하나 이상이 필요합니다. 기본적으로 백업 에이전트에는 8GB RAM과 CPU 2개가 할당됩니다. 백업 에이전트는 백업 또는 복구 작업을 5개까지 동시에 처리할 수 있습니다.

더 많은 작업을 처리하거나 백업 및 복구 트래픽을 분산하려는 경우에는 같은 호스트에 에이전트를 추가로 디플로이하십시오. 그리고 메모리 부족으로 인한 오류를 방지하려는 경우에는 기존 에이전트에 16GB RAM과 vCPU 4개를 할당하는 것이 좋습니다.

참고
백업 에이전트가 설치되지 않은 ESXi 호스트의 가상 머신 백업은 "작업 시간 초과 만료" 오류가 발생하면서 실패합니다.

7. **OVF 템플릿 디플로이** 마법사에서 다음 항목을 설정하여 백업 에이전트를 구성합니다.



a. Cyber Protect Cloud 데이터 센터의 URL. 예를 들어 `https://us5-cloud.example.com` 등을 입력할 수 있습니다.
b. 파트너 관리자 로그인 및 비밀번호.
c. VMware vCenter 매개변수: 서버 주소, 로그인 및 비밀번호.
   에이전트는 이러한 자격 증명을 사용하여 vCenter Server에 연결합니다. **관리자** 역할이 할당된 계정을 사용하는 것이 좋습니다. 또는 vCenter Server에서 필수 권한이 있는 계정을 제공합니다.
d. 에이전트가 있는 가상 머신의 루트 사용자의 암호입니다.
e. 네트워크 매개변수: IP 주소, 서브넷 마스크, 기본 게이트웨이, DNS, DNS 접미부.
   기본적으로 하나의 네트워크 인터페이스만 활성화되어 있습니다. 두 번째 네트워크 인터페이스를 활성화하려면 **eth1 활성화** 옆의 확인란을 선택합니다.

   참고
   백업 에이전트가 vCenter Server와 Cyber Protect Cloud 데이터 센터에 모두 액세스할 수 있도록 네트워크 설정을 지정해야 합니다.

f. 다운로드 제한: 복구 작업 중에 백업 아카이브 읽기 속도를 정의하는 최대 다운로드 속도(Kbps)입니다. 기본값은 0(무제한)입니다.
g. 업로드 제한: 백업 작업 중에 백업 아카이브 쓰기 속도를 정의하는 최대 업로드 속도(Kbps)입니다. 기본값은 0(무제한)입니다.

초기 디플로이 후에 백업 에이전트 설정 매개변수를 구성할 수도 있습니다. vSphere Client에서 백업 에이전트가 설치된 가상 머신의 전원을 끈 다음 **구성** > **설정** > **vApp 옵션**을 클릭합니다. 원하는 설정을 적용한 후 백업 에이전트가 설치된 가상 머신의 전원을 켭니다.

8. vSphere Client에서 백업 에이전트가 설치된 가상 머신에 대해 **호스트** 및 **Storage vMotion**이 비활성화되어 있는지 확인합니다.

에이전트 업데이트

관리 에이전트를 업데이트하려면

1. Cyber Protect Cloud 관리 포털에 파트너 관리자로 로그인합니다.
2. **설정** > **위치**로 이동하여 **추가VMware Cloud Director**를 클릭합니다.
3. **관리 에이전트** 링크를 클릭하여 최신 에이전트가 포함된 ZIP 파일을 다운로드합니다.
4. 관리 에이전트 템플릿 파일 `vCDManagementAgent.ovf` 및 가상 하드 디스크 파일 `vCDManagementAgent-disk1.vmdk`를 추출합니다.
5. vSphere Client에서 현재 관리 에이전트가 설치된 가상 머신의 전원을 끕니다.
6. 최신 `vCDManagementAgent.ovf` 및 `vCDManagementAgent-disk1.vmdk` 파일을 사용하여 새 관리 에이전트가 포함된 가상 머신을 디플로이합니다.
7. 이전 에이전트와 같은 설정을 사용하여 관리 에이전트를 구성합니다.
8. [선택 사항] 이전 관리 에이전트가 설치된 가상 머신을 삭제합니다.

중요
관리 에이전트는 VMware Cloud Director 환경당 하나만 활성 상태여야 합니다.

백업 에이전트를 업데이트하려면

1. Cyber Protect Cloud 관리 포털에 파트너 관리자로 로그인합니다.
2. **설정** > **위치**로 이동하여 **추가VMware Cloud Director**를 클릭합니다.
3. **백업 에이전트** 링크를 클릭하여 최신 에이전트가 포함된 ZIP 파일을 다운로드합니다.
4. 관리 에이전트 템플릿 파일 `vCDCyberProtectAgent.ovf` 및 가상 하드 디스크 파일 `vCDCyberProtectAgent-disk1.vmdk`를 추출합니다.
5. vSphere Client에서 현재 백업 에이전트가 설치된 가상 머신의 전원을 끕니다.
   현재 실행 중일 수 있는 모든 백업 및 복구 작업은 실패합니다. vSphere Client에서 실행 중인 작업이 있는지 확인하려면 백업 에이전트가 설치된 가상 머신의 콘솔을 열고 `ps | grep esx_worker` 명령을 실행합니다. 활성 `esx_worker` 프로세스가 없는지 확인합니다.
6. 최신 `vCDCyberProtectAgent.ovf` 및 `vCDCyberProtectAgent-disk1.vmdk` 파일을 사용하여 새 백업 에이전트가 포함된 가상 머신을 디플로이합니다.
7. 이전 에이전트와 같은 설정을 사용하여 백업 에이전트를 구성합니다.
8. [선택 사항] 이전 백업 에이전트가 설치된 가상 머신을 삭제합니다.

백업 관리자 생성

조직 관리자는 구체적으로 할당된 백업 관리자에게 백업 관리를 위임할 수 있습니다.

백업 관리자를 생성하려면

1. VMware Cloud Director 테넌트 포털에서 **관리** > **역할** > **새로 만들기**를 클릭합니다.
2. **역할 추가** 창에서 새 역할의 이름과 설명을 지정합니다.

3. 권한 목록 아래쪽으로 스크롤한 다음 **기타** 아래에서 **셀프 서비스 VM 백업 작업자**를 선택합니다.

참고
VMware Cloud Director용 플러그인을 설치하고 나면 **셀프 서비스 VM 백업 작업자** 권한을 사용할 수 있습니다. 이 작업을 수행하는 방법에 대한 자세한 내용은 "VMware Cloud Director용 플러그인 설치 및 게시"(141페이지)을(를) 참조하십시오.

4. VMware Cloud Director 테넌트 포털에서 **사용자**를 클릭합니다.
5. 사용자를 선택하고 **편집**을 클릭합니다.
6. 앞에서 생성한 새 역할을 이 사용자에게 할당합니다.

그러면 선택한 사용자가 이 조직의 가상 머신 백업을 관리할 수 있습니다.

참고
VMware Cloud Director 환경의 시스템 관리자는 **셀프 서비스 VM 백업 작업자** 권한이 활성화된 글로벌 역할을 정의한 다음 테넌트에 이 역할을 게시할 수 있습니다. 그러면 조직 관리자는 사용자에게만 역할을 할당하면 됩니다.

시스템 보고서, 로그 파일 및 구성 파일

문제 해결을 위해 `sysinfo` 도구를 사용하여 시스템 보고서를 생성해야 할 수도 있고, 에이전트가 설치된 가상 머신에서 로그 및 구성 파일을 확인해야 할 수도 있습니다.

vSphere Client에서 콘솔을 열어 가상 머신에 직접 액세스할 수도 있고 SSH 클라이언트를 통해 원격으로 가상 머신에 액세스할 수도 있습니다. SSH 클라이언트를 통해 가상 머신에 액세스하려면 먼저 이 머신에 대한 SSH 연결을 활성화해야 합니다.

가상 머신에 대한 SSH 연결을 활성화하려면

1. vSphere Client에서 에이전트가 설치된 가상 머신의 콘솔을 엽니다.
2. 명령 프롬프트에서 `/bin/sshd` 명령을 실행하여 SSH 디먼을 시작합니다.

그러면 WinSCP 등의 SSH 클라이언트를 사용하여 해당 가상 머신에 연결할 수 있습니다.

sysinfo 도구를 실행하려면

1. 에이전트가 설치된 가상 머신에 액세스합니다.
   - 해당 가상 머신에 직접 액세스하려면 vSphere Client에서 가상 머신의 콘솔을 엽니다.
   - 가상 머신에 원격으로 액세스하려면 SSH 클라이언트를 통해 가상 머신에 연결합니다.
     기본 로그인:비밀번호 조합 `root:root`를 사용합니다.
2. `/bin` 디렉토리로 이동하여 `sysinfo` 도구를 실행합니다.

```
# cd /bin/
# ./sysinfo
```

그러면 시스템 보고서 파일이 기본 디렉토리인 `/var/lib/Acronis/sysinfo`에 저장됩니다.

`--target_dir` 옵션을 사용해 `sysinfo` 도구를 실행하면 다른 디렉토리를 지정할 수 있습니다.

```
./sysinfo --target_dir path/to/report/dir
```

3. SSH 클라이언트를 사용해 생성된 시스템 보고서를 다운로드합니다.

로그 또는 구성 파일에 액세스하려면

1. SSH 클라이언트를 통해 가상 머신에 연결합니다.
   기본 로그인:비밀번호 조합 root:root를 사용합니다.
2. 원하는 파일을 다운로드합니다.
   로그 파일의 위치는 다음과 같습니다.
   - 백업 에이전트: /opt/acronis/var/log/vmware-cloud-director-backup-service/log.log
   - 관리 에이전트: /opt/acronis/var/log/vmware-cloud-director-management-agent/log.log

   구성 파일의 위치는 다음과 같습니다.
   - 백업 에이전트: /opt/acronis/etc/vmware-cloud-director-backup-service/config.yml
   - 관리 에이전트: /opt/acronis/etc/vmware-cloud-director-management-agent/config.yaml

Cyber Protect 콘솔 액세스

다음 관리자는 VMware Cloud Director 조직의 가상 머신 백업을 관리할 수 있습니다.

- 조직 관리자
- 구체적으로 할당된 백업 관리자
  이러한 관리자를 생성하는 방법에 대한 자세한 내용은 "백업 관리자 생성"(146페이지)을(를) 참조하십시오.

관리자는 테넌트 포털의 탐색 메뉴에서 **Cyber Protection**을 클릭하여 사용자 정의 Cyber Protect 콘솔에 액세스할 수 있습니다.

참고
조직 관리자만 SSO(Single Sign-On)를 사용할 수 있지만 VMware Cloud Director 테넌트 포털을 사용하는 시스템 관리자의 경우에는 SSO가 지원되지 않습니다.

관리자는 Cyber Protect 콘솔에서 해당 조직의 VMware Cloud Director 조직 요소(가상 데이터 센터, vApp, 개별 가상 머신)에만 액세스할 수 있습니다. 그리고 VMware Cloud Director 조직 리소스의 백업과 복구를 관리할 수 있습니다.

파트너 관리자는 고객 테넌트의 Cyber Protect 콘솔에 액세스할 수 있으며 고객 대신 백업과 복구를 관리할 수 있습니다.

백업 및 복구 수행

보호 계획 생성

백업 설정을 구성하려면 보호 계획을 생성해야 합니다.

여러 머신에 보호 계획 하나를 적용할 수 있으며 같은 머신에 여러 보호 계획을 적용할 수도 있습니다.

제한 사항

- 전체 머신의 백업만 지원되며 개별 디스크나 볼륨을 백업할 수는 없습니다.
- 파일 필터(포함/제외)는 지원되지 않습니다.
- 사용 가능한 백업 위치는 클라우드 스토리지뿐입니다. 스토리지는 관리 에이전트 설정에서 구성되며 사용자가 보호 계획에서 스토리지를 변경할 수는 없습니다.
- 동적 그룹은 지원되지 않습니다.
- 지원되는 백업 구성표는 **항상 증분(단일 파일)**, **항상 전체** 및 **매주 전체, 매일 증분**입니다.
- 백업 이후의 정리만 지원됩니다.

보호 계획을 만들려면

1. Cyber Protect 콘솔에서 **장치** > **VMware Cloud Director**로 이동합니다.
2. 보호할 머신을 선택하고 **보호**를 클릭합니다.
3. [이미 적용된 계획이 있는 경우] **계획 추가**를 클릭합니다.
4. **계획 생성**을 클릭합니다.
5. **암호화**에서 암호화 설정을 구성합니다.
6. [선택 사항] 보호 계획의 이름을 변경하려면 연필 아이콘을 클릭하고 새 이름을 입력하십시오.
7. [선택 사항] 백업 구성표나 스케줄을 변경하려면 **스케줄**을 클릭하고 설정을 구성합니다.
8. [선택 사항] 보존 규칙을 변경하려면 **보관 개수**를 클릭하고 설정을 구성합니다.
9. [선택 사항] 백업 옵션을 변경하려면 **백업 옵션**을 클릭하고 설정을 구성합니다.
10. **적용**을 클릭합니다.

머신 복구

원래 가상 머신이나 새 가상 머신으로 백업을 복구할 수 있습니다.

제한 사항

- 파일 수준 복구는 지원되지 않습니다.
- VMware Cloud Director 10.4 이상 버전에서는 새 가상 머신으로 백업을 복구할 수 있습니다. 에이전트 버전 24.02 이상에서 생성된 백업만 새 가상 머신으로 복구할 수 있습니다. 에이전트가 설치된 가상 머신의 `/etc` 디렉토리에 있는 `ProductVersion.conf` 파일에서 에이전트 버전을 확인할 수 있습니다.
- 새 머신으로 백업을 복구하고 나면 **장치** > **VMware Cloud Director** > 조직 > 가상 데이터 센터 > **독립형 VM**에 새 머신이 표시됩니다. 특정 vApp을 복구 대상으로 선택할 수는 없습니다.

머신을 복구하려면

원래 머신으로

1. Cyber Protect 콘솔에서 다음 방법 중 하나로 복구 지점을 선택합니다:
   - **장치** > **VMware Cloud Director**로 이동하여 백업한 머신을 선택하고 **복구**를 클릭한 다음 복구 지점을 선택합니다.

- **장치** > **VMware Cloud Director**로 이동하여 백업 아카이브를 선택하고 **백업 표시**를 클릭한 다음 복구 지점을 선택합니다.

2. **머신 복구**를 클릭합니다.
3. **복구 시작**을 클릭합니다.

새 머신으로

1. Cyber Protect 콘솔에서 다음 방법 중 하나로 복구 지점을 선택합니다:
   - **장치** > **VMware Cloud Director**로 이동하여 백업한 머신을 선택하고 **복구**를 클릭한 다음 복구 지점을 선택합니다.
   - **장치** > **VMware Cloud Director**로 이동하여 백업 아카이브를 선택하고 **백업 표시**를 클릭한 다음 복구 지점을 선택합니다.
2. **머신 복구**를 클릭합니다.
3. **대상 머신**을 클릭한 다음 **새 머신**을 선택합니다.
4. 새 머신용 가상 데이터 센터를 선택합니다.
5. 새 머신의 이름을 지정합니다.
   기본적으로 원래 머신의 이름이 추천 이름으로 표시됩니다.
6. **확인**을 클릭합니다.
7. [선택 사항] **VM 설정**을 클릭하여 새 머신의 다음 설정을 변경한 후에 **확인**을 클릭합니다:
   - RAM 크기
   - 가상 프로세서 수
   - 소켓당 코어 수
   - 스토리지 프로필
   - 네트워크 어댑터 및 할당된 네트워크
8. [선택 사항] **디스크 매핑**을 클릭하여 디스크 매핑이나 스토리지 프로필을 변경한 다음 **확인**을 클릭합니다.
9. **복구 시작**을 클릭합니다.

VMware Cloud Director를 사용하여 통합 제거

구성을 되돌리고 Cyber Protect Cloud에서 VMware Cloud Director 인스턴스의 등록을 해제하려면 복잡한 절차를 수행해야 합니다. 도움이 필요한 경우 지원 담당자에게 문의하십시오.

색인