자산 및 인벤토리 목록 검색

검색은 멀티 클라우드 방어의 "검색, 구축 및 방어" 접근 방식에서 중요한 구성 요소입니다.

검색은 온보딩된 클라우드 어카운트에 구축된 현재 리소스에 대한 실시간 가시성을 제공합니다. 또한 VPC 플로우 로그 및 DNS 로그에 대한 인터페이스를 제공하여 클라우드 구축을 완벽하게 파악할 수 있습니다. IAM 역할(AWS 및 OCI), AD 앱 등록(Azure) 또는 서비스 어카운트(GCP)에 부여된 권한을 통해 멀티 클라우드 방어 컨트롤러는 클라우드 리소스를 주기적으로 크롤링하고 변경 사항을 계속 모니터링하여 "에버그린" 인벤토리 목록 모델을 유지합니다.

Discovery(검색**)** 탭을 사용하면 리소스의 속성과 이러한 리소스가 상호 연결된 방식을 확인할 수 있습니다. 멀티 클라우드 방어에서는 구성과 관련된 모든 리소스 보안 상태의 간결한 보기에 이 정보를 수집하고, 트래픽 흐름에 대한 컨텍스트도 파악합니다.

검색 요약

Discovery Summary(검색 요약) 페이지는 사용 가능한 트래픽 및 인벤토리를 요약하는 위젯 모음입니다. 페이지 맨 위의 필터 를 사용하여 위젯의 기록을 변경할 수 있습니다.

트래픽 요약 위젯

현재 멀티 클라우드 방어은 DNS 트래픽용 위젯과 VPC 및 VNet 플로우 로그용 위젯의 두 가지 위젯으로 트래픽의 압축된 블록을 표시합니다. 트래픽에 대한 이러한 창은 악성 트래픽과 DNS 또는 VPC/VNet 트래픽을 각각 구분합니다. 특정 시간 프레임으로 확대하려면 이러한 위젯의 내부를 클릭합니다.

이 요약 페이지에서 **Logs(**로그**)** 토글을 클릭하여 해당 위젯에 대한 로그를 활성화하거나 비활성화할 수 있습니다. 이러한 로그 유형과 컴파일되는 트래픽에 대한 자세한 내용은 트래픽 유형를 참조하십시오.

검색 요약

검색 요약은 클라우드 서비스 제공자를 연결할 때 검색 프로세스의 일부로 멀티 클라우드 방어이 복구한 일련의 인벤토리 창입니다. 이러한 통계는 빠르게 미리 볼 수 있도록 여기에 요약되어 있습니다. 자세한 내용은 인벤토리, 2 페이지를 참조하십시오.

인벤토리

IAM 역할(AWS 및 OCI), AD 앱 등록(Azure) 또는 서비스 어카운트(GCP)에 부여된 권한을 통해 멀티 클라우드 방어는 클라우드 리소스의 "에버그린" 인벤토리 목록 모델을 지속적으로 유지하고 클라우드 서비스 공급자 어카운트, 구독 및 고급 네트워크 보안 적용과 관련된 프로젝트에 존재하는 실시간 검색을 유지합니다. 검색된 리소스는 관리자가 애플리케이션 노출의 위험을 완화하는 보안 규칙을 신속하게 구축할 수 있는 워크플로우에서 사용할 수 있습니다. 모든 활동은 멀티 클라우드 방어 컨트롤러을(를) 통해 즉시 보고됩니다.

인벤토리 목록이 활성화된 경우 멀티 클라우드 방어 컨트롤러에서 전체 인벤토리 목록 검색을 주기적으로 수행합니다. 기본값은 60분이지만 조정 가능합니다. 실시간 인벤토리 목록 검색은 CloudFormation 템플릿이 구축된 지역에서 활성화됩니다.

검색 프로세스 중 일부에서는 각 클라우드 서비스의 로그가 강조 표시됩니다. 서비스 제공자별로 다음과 같은 로그 유형을 확인할 수 있습니다.

- **AWS** - VPC 플로우 로그, Mount53 플로우 로그 및 DNS 로그.
- **Azure** - NSG 플로우 로그.
- **GCP** - VPC 플로우 로그.

멀티 클라우드 방어은(는) 모든 클라우드 서비스 제공자에게 동일한 레벨의 지원을 제공합니다.

애플리케이션

Application(애플리케이션)에 클라우드 어카운트에 대한 모든 로드 밸런서 및 API 게이트웨이가 표시됩니다. **Inventory(**인벤토리 목록**)**의 Applications(애플리케이션) 섹션에는 **Known Tags(**알려진 태그**)**, **Tags(**태그**)** 및 **Applications(**애플리케이션**)**이라는 3개의 필터 버튼이 있습니다. **Applications(**애플리케이션**)**에서 사용자는 특정 애플리케이션에 대한 보호를 생성하고 적용하는 워크플로우를 호출할 수 있습니다.

애플리케이션 태그

애플리케이션을 식별하는 데 사용되는 **Application Tags(**애플리케이션 태그**)** 목록을 만듭니다. 인벤토리 검색 중에 지정된 태그가 있는 모든 검색된 로드 밸런서가 애플리케이션으로 처리됩니다.

예를 들어 애플리케이션 역할을 하는 모든 로드 밸런서에 **Application Tags(**애플리케이션 태그**)**를 할당할 수 있습니다. 이 태그의 값은 검색된 인벤토리 목록에 애플리케이션 태그로 표시됩니다. 아래 표를 시각적 예로 참조하십시오.

로드 밸런서	태그	값
로드 밸런서 1	ApplicationName	Billing
로드 밸런서 2	ApplicationName	UserManagement

검색된 인벤토리 목록에는 검색된 애플리케이션 자산 내의 **Billing** 및 **UserManagement** 애플리케이션이 표시됩니다.

애플리케이션 태그 목록을 생성하려면 **Create(**생성**)**를 클릭합니다.

매개변수	설명
이름	사전 채워집니다.
설명	사용자 지정 설명입니다.
값	로드 밸런서에 할당하는 데 사용할 태그 값입니다.

애플리케이션 태그에 대한 자세한 내용은 애플리케이션 태그를 참조하십시오.

Known Tags(알려진 태그**)**

Known Tags(알려진 태그**)**는 관리자가 알려진 태그로 식별한 클라우드 어카운트의 애플리케이션 로드 밸런서에서 식별한 애플리케이션을 보여줍니다. 이러한 알려진 태그가 **Settings(**설정**)** > **Management(**관리**)** > **Account(**계정**)** > **Application Tags(**애플리케이션 태그**)**에 나열되어 있습니다.

태그

Tags(태그)는 태그 키와 태그 값을 표시하는 필드와 함께 애플리케이션 로드 밸런서, 그리고 해당 애플리케이션이 멀티 클라우드 방어 게이트웨이로 보호되는지 여부를 통해 식별한 모든 애플리케이션을 표시합니다.

검색된 자산

클라우드 어카운트에 대한 지역의 인벤토리 목록 검색을 활성화하면 멀티 클라우드 방어 컨트롤러이(가) 클라우드 자산을 지속적으로 검색합니다. 검색된 자산을 보려면 **Discover(**검색**)** 또는 **Manage(**관리**)** > **Inventory(**인벤토리 목록**)**로 이동합니다. 기본 보기에는 모든 클라우드 어카운트에 대해 검색된 자산이 표시됩니다. 특정 클라우드 어카운트으로 필터링하려면 **Select Account(**어카운트 선택**)**를 사용하여 특정 클라우드 어카운트를 지정하고 검색된 자산을 확인합니다.

검색된 자산 범주 및 이러한 범주가 참조하는 항목은 다음과 같습니다.

- 보안 그룹 - AWS 보안 그룹(SG) 및 Azure NSG(네트워크 보안 그룹)
- 네트워크 ACL - AWS NACL(Network Access Control List).
- 서브넷.
- 경로 테이블.

- 네트워크 인터페이스.
- VPC/VNet - AWS VPC, Azure VNet 및 GCP VPC.
- 애플리케이션 - 애플리케이션은 AWS ALB(Application Load Balancer)에 의해 식별됩니다.
- 로드 밸런서.
- 인스턴스 - AWS 인스턴스, Azure 가상 머신 및 GCP 컴퓨팅 인스턴스.
- 태그 - AWS 태그, Azure 태그 및 GCP 레이블.
- 인증서 - AWS Certificates Manager(ACM) 인증서

자산 검색 및 인벤토리 목록 활성화

클라우드 어카운트에서 자산 검색을 활성화하려면:

단계 **1** **Manage(**관리**)** > **Accounts(**계정**)**로 이동합니다.

단계 **2** 클라우드 어카운트 옆의 확인란을 선택하고 **Manage Inventory(**인벤토리 관리**)**를 클릭합니다.

단계 **3** 멀티 클라우드 방어가 검색하려는 클라우드 자산이 있는 **Regions(**지역**)**을 선택합니다. 새로 고침 간격은 인벤토리 목록이 새로 고쳐지는 시간(분)입니다(권장 기본값은 60분). 또한 멀티 클라우드 방어는 일반 폴링 대신 클라우드 서비스 공급자의 API 및 이벤트를 사용하여 지속적 검색을 수행합니다. 여기에 지정된 새로 고침 시간 간격은 전체 재크롤링을 위한 것입니다. 이렇게 하면 실시간 검색 중에 누락된 이벤트에 대한 모든 자산이 조정됩니다.

새 행을 추가하고 원하는 영역을 선택하여 각 영역에 대해 다른 새로 고침 간격을 정의할 수 있습니다. 영역은 단일 새로 고침 간격에만 속할 수 있습니다.

단계 **4** **Finish(**마침**)**를 클릭하여 저장합니다.

Note 멀티 클라우드 방어 컨트롤러는 저장 후 즉시 새로 추가된 영역에 대한 자산 인벤토리 목록을 요청합니다.

What to do next

검색된 자산을 검토하려면 **Manage(**관리**)** > **Inventory(**인벤토리 목록**)**로 이동합니다.

보안 인사이트

인사이트는 AWS, Azure 및 GCP에서 검색되어 결과로 표시되는 자산에 대한 규칙 기반 평가입니다. 인사이트는 멀티 클라우드 방어 컨트롤러에서 수용하는 주기적인 실시간 인벤토리 목록 모니터링을 기반으로 작동하므로 멀티 클라우드 방어 게이트웨이을(를) 구축하지 않고도 사용할 수 있습니다.

단계 **1** 멀티 클라우드 방어 컨트롤러 인터페이스에서 **Add Account(**어카운트 추가**)**를 클릭합니다. 또는 쉬운 설정 마법사를 사용하여 어카운트에 연결하는 것을 강력하게 권장합니다. 계정을 연결하는 단계를 진행합니다.

단계 **2** 계정이 연결되고 온보딩되면 자산 검색 및 인벤토리 목록 활성화합니다.

단계 **3** **Discover(**검색**)** > **Discovery Summary(**검색 요약**)**로 이동합니다. 이 페이지에는 검색된 모든 자산 및 인사이트 결과의 요약 보기가 표시됩니다.

보안 인사이트 유형

대시보드의 기능을 이해하려면 다음 보안 인사이트 유형을 자세히 읽어보십시오.

보안 그룹

고객은 종종 보안 그룹의 급증으로 어려움을 겪습니다. 보안 그룹은 위험을 초래할 수 있는 리소스 간에 공유되는 경우가 많습니다. 특정 리소스를 대상으로 하는 보안 그룹을 변경하면 더 큰 리소스 그룹에 영향을 줄 수 있습니다.

Security Groups(보안 그룹)은 모든 보안 그룹, 세부 정보 및 보안 그룹을 활용하는 리소스 집합의 목록을 제공합니다. **Is Inbound Public(**인바운드 공용 여부**)** 및 **Is Outbound Public(**아웃바운드 공용 여부**)** 필드는 0.0.0.0/0으로 설정된 보안 그룹을 나타냅니다.

검색 창에서 검색 기준을 기반으로 규칙을 생성하는 옵션을 사용하여 필드 및 해당 값을 기반으로 검색 기준을 정의합니다.

규칙

규칙은 구성된 인바운드 및 아웃바운드 규칙을 기반으로 보안 그룹을 보여줍니다.

포트

포트는 구성된 인바운드 및 아웃바운드 포트를 기반으로 보안 그룹을 볼 수 있습니다.

애플리케이션 보안 그룹

애플리케이션 보안 그룹 은 AWS 보안 그룹과 유사한 Azure 구조입니다. Azure 애플리케이션 보안 그룹에는 해당 시스템과 시스템의 인터페이스를 포함하는 보안 그룹의 멤버가 있습니다. 멤버십과 보안 컨트롤이 모두 있습니다. 따라서 멀티 클라우드 방어은 멤버십 구성을 사용하여 동적 정책을 구축합니다. Azure 환경 내에서 애플리케이션 보안 그룹을 생성하고 사용하면, 멀티 클라우드 방어이 변경 사항을 인식하고 정책을 조정하여 통합합니다.

Azure의 애플리케이션 보안 그룹 및 작동 방식에 대한 자세한 내용은 Microsoft Azure 설명서를 참조하십시오.

네트워크 **ACL**

네트워크 ACL(Access Control List)은 모든 네트워크 ACL의 목록과 세부 정보를 제공합니다. **Is Inbound Public(**인바운드 공용 여부**)** 및 **Is Outbound Public(**아웃바운드 공용 여부**)** 필드는 0.0.0.0/0으로 설정된 네트워크 ACL을 나타냅니다.

규칙

규칙은 구성된 인바운드 및 아웃바운드 규칙을 기반으로 네트워크 ACL을 보여줍니다.

서브넷

서브넷은 모든 서브넷 및 세부 정보의 목록을 제공합니다. **Is Public(**퍼블릭**)** 필드는 자동 할당 공용 IP의 활성화 여부에 따라 공개적으로 액세스 가능한 서브넷을 나타냅니다.

경로 테이블

경로 테이블은 모든 경로 테이블 및 세부 정보의 목록을 제공합니다. **Is Inbound Public(**인바운드 공용 여부**)** 및 **Is Outbound Public(**아웃바운드 공용 여부**)** 필드는 기본 액세스 인터넷을 제공하도록 구성된 경로 테이블을 나타냅니다.

네트워크 인터페이스

네트워크 인터페이스는 모든 네트워크 인터페이스 및 상세정보 목록을 제공합니다. **Is Inbound Public(**인바운드 퍼블릭**)** 및 **Is Outbound Public(**아웃바운드 퍼블릭**)** 필드는 개방형 보안 그룹(0.0.0.0/0)으로 구성된 네트워크 인터페이스 또는 인터넷에 대한 기본 액세스를 허용하는 경로 테이블을 나타냅니다.

VPC\VNets

VPC/VNet은 모든 VPC/VNet 및 해당 세부 정보의 목록을 제공합니다.

애플리케이션

Applications(애플리케이션)에서는 구축된 모든 애플리케이션 로드 밸런서 및 해당 세부 정보의 목록을 제공합니다. **Secured(**보안**)** 필드는 멀티 클라우드 방어 게이트웨이 및 보안 정책이 애플리케이션을 보호하기 위해 적용되는지 여부를 식별하며, 애플리케이션을 보호하는 워크플로우를 호출하는 기능을 제공합니다.

로드 밸런서

로드 밸런서는 모든 구축된 애플리케이션, 네트워크 및 게이트웨이 로드 밸런서 목록과 해당 세부 정보를 제공합니다. **Public** 필드에는 리소스가 인터넷 연결 로드 밸런서인지 여부가 표시됩니다. **CSP WAF Enabled(CSP WAF** 활성화**)**는 애플리케이션 로드 밸런서에 대해 CSP WAF가 활성화되었는지 여부를 표시합니다.

인스턴스

인스턴스는 리소스에 대해 할당 및 구성된 보안 그룹 및 인터페이스 수에 대한 요약 정보와 함께 모든 인스턴스의 목록을 제공합니다. **Is Inbound Public(**인바운드 퍼블릭**)** 및 **Is Outbound Public(**아웃바운드 퍼블릭**)** 필드는 개방형 보안 그룹(0.0.0.0/0)으로 구성된 네트워크 인터페이스가 있는 인스턴스 또는 인터넷에 대한 기본 액세스를 허용하는 경로 테이블을 나타냅니다.

태그

태그는 태그로 구성된 모든 VPC/VNet, 서브넷, 보안 그룹, 인스턴스 및 로드 밸런서의 목록을 제공합니다.

인증서

인증서는 AWS 인증서 관리자에서 사용 가능한 모든 인증서의 목록과 함께 발급자, 도메인 이름 및 만료일에 대한 요약 정보를 제공합니다.

토폴로지

이 탭에는 클라우드 어카운트에 있는 클라우드 자산의 지역별 개략적인 맵 보기가 표시됩니다. 화면 상단의 필터 막대를 사용하여 시각적 개체를 세부적으로 조정할 수 있습니다. 여기에서 데이터 drom을 가져올 클라우드 서비스 제공자 어카운트, 세계의 지역, 특정 VNet 또는 VPC, 인스턴스 및 기록의 기간을 결정할 수 있습니다.

세계 지도의 글로벌 보기를 사용하면 위에서 언급한 필터 표시줄로 지정한 특정 지역을 스크롤하여 자세히 살펴볼 수 있습니다. 맵의 바로 왼쪽에서 확인할 트래픽 및 인벤토리 유형을 표시할 수 있습니다. 표시할 내용에 대해 적절하게 확인란을 선택하고 선택 취소합니다.

통찰력

인사이트는 AWS, Azure 및 GCP에서 검색되어 결과로 표시되는 자산에 대한 규칙 기반 평가입니다.

규칙

규칙은 검색된 자산의 결과를 식별하기 위한 평가 집합입니다. 멀티 클라우드 방어에서는 기본 규칙 집합을 제공합니다. 인벤토리 목록 범주(예: 보안 그룹, 애플리케이션, 로드 밸런서, 태그 등)를 선택하고 검색 기준을 정의하고 **Add Rule(**규칙 추가**)**을 선택하고 추가 필수 정보를 지정하여 새 규칙을 생성할 수 있습니다. 새 규칙을 보려면 **Insights(**인사이트**)** > **Rules(**규칙**)** 로 이동합니다. 여기에서 기존 및 새로 검색된 자산을 대상으로 작업을 수행할 수 있습니다.

결과

결과는 정의된 규칙 집합과 일치하는 검색된 자산의 목록입니다.

규칙 및 결과

클라우드 리소스를 확인하고 가드 레일을 사용하도록 규칙을 구성할 수 있습니다.

규칙 및 결과

클라우드 리소스를 확인하고 가드 레일을 사용하도록 규칙을 구성할 수 있습니다.

사전 정의된 규칙

멀티 클라우드 방어 컨트롤러에는 몇 가지 사전 정의된 기본 규칙이 있습니다.

- 클라우드 서비스 제공자 WAF가 활성화되지 않은 애플리케이션 로드 밸런서.
- 인그레스가 열려 있는 인스턴스가 거의 없는 보안 그룹(5개 미만). 보안 그룹의 사용률이 낮으면 확인하기 어려운 격차가 발생하고 공격이 쉽게 발생할 수 있습니다.
- 네트워크 인터페이스가 두 개 이상인 인스턴스.
- 열린 아웃바운드(0.0.0.0/0) 액세스 권한이 있는 보안 그룹.
- 퍼블릭 서브넷 - **Auto-Assign Public IP(**자동 할당 공용 **IP)** 가 활성화된 모든 AWS 서브넷.
- 인터넷에 너무 많은 송신 포트(25개 이상)가 열려 있는 보안 그룹.
- 인터넷에 너무 많은 수신 포트(5개 이상)가 열려 있는 보안 포트.
- 공개 액세스가 활성화된 상태에서 65,535개의 포트가 열려 있는 보안 그룹.
- 30일 후에 만료되는 인증서 - AWS Certificate Manager에만 해당.

규칙과 일치하는 클라우드 리소스는 심각도와 일치하는 결과로 플래그가 지정됩니다.

맞춤형 규칙 생성에 대한 자세한 내용은 사전 정의된 규칙, on page 8를 참고하십시오.

맞춤형 규칙

사용자는 리소스에 대한 추가 규칙을 구성할 수 있습니다.

1. **Discovery(**검색**)** > **Inventory(**인벤토리 목록**)**으로 이동하고 리소스(예: 로드 밸런서)를 선택합니다.
2. 텍스트 영역에서 규칙 기준을 생성하고 **Add Rule(**규칙 추가**)**를 선택합니다.
3. 다음 항목의 콘텐츠와 규칙 기준을 충족하는 발견 항목 수를 입력합니다.
   - 이름
   - 설명
   - 심각도
   - 기본 작업
   - 유형
   - 계정
4. **Save(**저장**)**를 클릭합니다.

규칙의 기본 작업은 **info(**정보**)** 또는 알림**(alert)**일 수 있습니다. 규칙이 기본 작업으로 알림으로 구성된 경우, 규칙에 대한 새 결과가 발생하면 멀티 클라우드 방어 컨트롤러에서 알림 알림이 생성됩니다. 알림의 기본 작업을 원하는 경우 다음 구성이 필요합니다.

- 사용자가 ServiceNow, PagerDuty 또는 Webhook 알림을 원하는지 나타내도록 알림 프로파일을 구성합니다.
- 지정된 심각도 레벨을 사용하여 **Alert Rule of type Discovery(**검색 유형의 알림 규칙**)** 및 하위 유형 **Insights Rule(**인사이트 규칙**)**을 구성합니다.

결과

사전 정의된 규칙과 맞춤형 규칙을 기반으로 리소스에 대한 결과를 볼 수 있습니다. **Findings Summary(**결과 요약**)**는 대시보드에 위치하며 Inventory(인벤토리 목록) 탭의 Summary(요약) 보기에도 쉽게 액세스할 수 있습니다.

결과