Cisco Multicloud Defense

최종 변경: 2026년 11월 16일

Cisco Multicloud Defense

Cisco Multicloud Defense는 클라우드 환경 내에서 들어오고 나가는 트래픽을 검사하고 보호하기 위한 클라우드 네이티브 멀티 클라우드 네트워크 보안 솔루션입니다. SaaS 컨트롤러를 클라우드가 구축한 게이트웨이와 결합하여 AWS, Azure, Google Cloud 및 OCI 전반에서 가시성, 정책 시행, 위협 방지 및 세그멘테이션을 제공합니다.

Cisco Multicloud Defense

계정 온보딩

컨트롤러가 클라우드 리소스를 검색하고 트래픽 가시성을 활성화하며 보안 인프라를 구축할 수 있도록 클라우드 계정, 구독, 프로젝트, 폴더 또는 테넌시를 Multicloud Defense에 연결하는 프로세스입니다. 온보딩은 클라우드별 사전 요건 및 권한 모델을 통해 AWS, Azure, GCP 및 OCI를 지원합니다.

고급 보안 프로파일

Multicloud Defense 게이트웨이 데이터 경로를 통해 적용되는 세분화된 검사 및 시행 기능의 컬렉션입니다. 예를 들어 IDS/ IPS, WAF, 안티바이러스, TLS 해독, DLP, URL 필터링, FQDN 필터링, 애플리케이션 계층 제어 등이 있습니다.

애플리케이션 레이어 방화벽

IP 주소, 포트 또는 프로토콜만 사용하는 대신 레이어 7에서 애플리케이션 트래픽을 평가하는 보안 기능입니다. Multicloud Defense에서 애플리케이션 레이어 방화벽은 클라우드 워크로드 보호에 사용되며 일반적으로 WAF 및 레이어 7 위협 방어와 같은 인그레스 보호와 연결됩니다.

에셋 검색

온보딩된 클라우드 계정에서 클라우드 리소스 및 재고 목록을 검색하고 리소스가 구축 및 상호 연결되는 방식에 대한 현재 보기를 유지하는 기능입니다. 에셋 검색은 팀이 클라우드 노출을 이해하고 필요한 경우 제어하는 데 도움이 됩니다.

자동 스케일링

자동 스케일링은 트래픽 수요에 따라 게이트웨이 인스턴스를 추가하거나 제거할 수 있는 자동화된 기능입니다. Multicloud Defense 게이트웨이와 FTDv 게이트웨이에 모두 적용할 수 있습니다. 자동 스케일링은 컨트롤러에서 관리되며 클라우드 워크로드 변경에 적응하는 동시에 보안 시행을 유지하도록 설계되었습니다.

중앙 집중식 보안 모델

보안 서비스가 중앙 서비스 VPC, VNet 또는 멀티 스포크 네트워크에 대한 시행 허브 역할을 하는 보안 VPC에 배치되는 구축 모델입니다. 연결된 클라우드 네트워크 전반에서 인그레스, 이그레스 및 동-서 검사에 중앙 집중식 설계가 사용됩니다.

CIDR

Multicloud Defense에서 CIDR(Classless Inter-Domain Routing)은 네트워크 경계를 정의하는 데 사용되는 기본적인 방법입니다. AWS, Azure, GCP 및 OCI와 같은 이기종 환경에서 워크로드 서브넷을 식별하고, 트래픽을 분할하고, 보안 정책을 구축합니다.

클라우드 계정

Multicloud Defense에 연결된 클라우드 제공자 관리 범위입니다. 예를 들면 AWS 계정, Azure 구독, GCP 프로젝트 또는 폴더, OCI 테넌시가 포함됩니다.

클라우드 네이티브 키 저장소

TLS 검사 활용 사례를 활성화하면서 고객이 제어하는 클라우드 경계 내부에 개인 키를 유지하는 데 사용되는 Azure 키 저장소와 같은 클라우드 제공자 키 관리 서비스입니다.

클라우드 서비스 공급자

AWS, Azure, Google Cloud Platform 또는 Oracle Cloud Infrastructure와 같은 퍼블릭 클라우드 플랫폼입니다. Multicloud Defense는 CSP(Cloud Service Provider) 네트워킹 및 로깅 구문과 통합되어 게이트웨이를 구축하고, 에셋을 검색하며, 트래픽 가시성을 수집합니다.

결합된 보안 모델

중앙 집중식 및 분산 보안 시행을 모두 사용하는 구축 접근 방식입니다. 이 모델은 공유 검사를 중앙 집중화하면서 필요한 경우 게이트웨이를 특정 애플리케이션 또는 클라우드 네트워크에 더 가까이 배치할 수 있습니다.

콘텐츠 필터링

콘텐츠, URL, FQDN, 범주, 멀웨어 판정 또는 데이터 손실 방지 논리를 기준으로 트래픽을 제어하거나 차단하는 검사 및 시행입니다.

컨트롤러 서비스 계정

Multicloud Defense 컨트롤러에 클라우드 계정에서 리소스를 검색하고, 인프라를 오케스트레이션하며, 보안 워크플로우를 관리하는 데 필요한 권한을 부여하는 데 사용되는 클라우드 ID 또는 서비스 계정입니다.

데이터 손실 방지

민감 데이터나 기밀 데이터가 승인된 경계를 벗어나는 것을 탐지하거나 방지하는 보안 기능입니다. Cisco 설명서에서는 데이터 손실 방지(DLP)를 PII 및 PHI와 같은 데이터 유형에 대한 컴플라이언스 및 보안을 지원하는 것으로 설명합니다.

□데이터평면

아키텍처의 트래픽 처리 측이며, Multicloud Defense 게이트웨이로 표시됩니다. 데이터 평면은 컨트롤러가 제어 평면을 제공하는 동안 검사하고 트래픽에서 정책을 시행합니다.

검색, 구축, 방어

Multicloud Defense 워크플로우입니다. 검색은 클라우드 계정과 재고 목록 리소스 및 트래픽을 연결합니다. 구축에서는 VPC, VNet 및 게이트웨이를 설정합니다. 방어는 보호를 위해 정책, 규칙 집합 및 프로파일을 생성하고 관리합니다.

분산형 보안 모델

보안 시행을 중앙 허브가 아닌 애플리케이션, 워크로드 또는 개별 클라우드 네트워크와 더 가까운 위치에 두는 배포 모델입니다. 팀에서 애플리케이션 로컬 검사, 규모 또는 세그멘테이션을 필요로 할 때 유용합니다.

동적 주소 개체

클라우드 리소스가 변경되면 업데이트되는 클라우드 네이티브 리소스 속성을 기반으로 하는 정책 개체입니다. 동적 주소 개체는 지속적인 수동 업데이트 없이 정책을 클라우드 리소스에 정렬하는 데 도움이 됩니다.

동-서 보안

워크로드, 서브넷, VPC, VNet 또는 클라우드 네트워크 간에 측면으로 이동하는 트래픽을 검사 및 시행합니다. 이는 측면 이동을 제한하고 애플리케이션과 계층 간의 세그멘테이션 또는 최소 권한 액세스를 구현하는 데 도움이 됩니다.

이그레스 게이트웨이

아웃바운드 및 동-서 트래픽을 보호하는 데 사용되는 게이트웨이입니다. FQDN 필터링, URL 필터링, DLP, IDS/ IPS, 안티바이러스, 정방향 프록시, TLS 해독 및 관련 제어를 제공할 수 있습니다.

이그레스 보안

클라우드 워크로드 또는 네트워크에서 인터넷, SaaS 서비스, 다른 네트워크 또는 기타 클라우드 환경으로 향하는 트래픽을 제어합니다. 이그레스 보안은 데이터 유출, CnC(Command-and-Control) 트래픽, 멀웨어 통신, 무단 대상을 방지하는 데 도움이 됩니다.

시행 지점

트래픽 정책이 적용되는 게이트웨이 인스턴스 또는 게이트웨이 클러스터입니다. 컨트롤러는 정책을 정의하고 오케스트레이션하는 반면, 게이트웨이는 해당 정책을 인라인으로 시행합니다.

정방향 프록시

아웃바운드 클라이언트 트래픽을 위한 프록시 기능입니다. Multicloud Defense에서 정방향 프록시 기능은 일반적으로 이그레스 검사, TLS 해독, URL/FQDN 필터링, DLP 및 위협 방지와 연결됩니다.

전달 모드

전체 패킷 또는 콘텐츠 페이로드를 검사하지 않고 소스 및 대상 통신을 기반으로 액세스 제어를 수행하는 게이트웨이 작동 모드입니다. 일반적으로 IP 주소, 레이어 4 정보, 태그 또는 FQDN을 기반으로 하는 동-서 플로우 및 이그레스 필터링에 사용됩니다.

게이트웨이

Multicloud Defense 데이터 평면 구성 요소로서 고객 클라우드 계정에 PaaS 구성 요소로 구축됩니다. 게이트웨이는 트래픽을 인라인 검사하고 인그레스, 이그레스 및 동-서 활용 사례에 대한 정책을 시행합니다.

게이트웨이 인스턴스

Multicloud Defense 게이트웨이 구축의 일부를 형성하는 클라우드 컴퓨팅 인스턴스입니다. 여러 인스턴스를 클라우드 로드 밸런서 뒤에 배치하여 확장성과 고가용성을 제공할 수 있습니다.

허브 및 스포크 아키텍처

중앙 서비스 네트워크 또는 보안 허브가 멀티 스포크 VPC, VNet 또는 VPC 네트워크에 연결되는 네트워크 설계입니다. Multicloud Defense는 중앙 집중식 검사 및 시행에 이 설계를 사용합니다.

인그레스 게이트웨이

애플리케이션 또는 워크로드로 향하는 인바운드 트래픽을 보호하는 데 사용되는 게이트웨이입니다. WAF, 레이어 7 DoS 보호, IDS/ IPS, 안티바이러스, 역방향 프록시, TLS 해독, 지리 IP 제어 및 악의적인 IP 필터링을 제공할 수 있습니다.

인그레스 보안

인터넷 또는 외부 네트워크에서 클라우드 환경으로 들어오는 트래픽을 제어합니다. 인그레스 보안은 익스플로잇, 봇, 멀웨어, 악의적인 IP, DoS 시도 및 기타 인바운드 위협으로부터 웹 및 비 웹 애플리케이션을 보호합니다.

인라인 검사

트래픽이 데이터 경로의 게이트웨이를 통과하는 동안 트래픽 검사가 수행됩니다. 인라인 검사를 사용하면 트래픽이 대상에 도달하기 전에 정책에서 제어를 허용, 거부, 해독, 스캔 또는 기타 방식으로 제어할 수 있습니다.

재고 목록

검색된 클라우드 리소스의 모델, 해당 속성 및 관계입니다. 컨트롤러에서 재고 목록을 주기적으로 새로 고침하므로 관리자가 현재 리소스 및 연결 방법을 볼 수 있습니다.

최소 권한 액세스

워크로드, 계층, 환경 또는 클라우드 네트워크 간에 인증된 통신만 허용하는 세그멘테이션 원칙입니다. Multicloud Defense는 세그멘테이션을 사용하여 최소 권한의 측면 액세스를 시행합니다.

Multicloud Defense 컨트롤러

Cisco Multicloud Defense를 위한 SaaS 제어 평면입니다. 이 컨트롤러는 중앙 집중식 관리, 클라우드 계정 온보딩, 검색, 게이트웨이 라이프사이클 자동화, 정책 오케스트레이션, 기록, 알림, 측정, 서드파티 운영 도구와의 통합을 제공합니다.

Multicloud Defense 게이트웨이

Cisco Multicloud Defense의 인라인 시행 구성 요소입니다. 이는 고객 클라우드 계정에 구축되고, 컨트롤러에서 정책을 수신하고, 트래픽을 검사하고, WAF, IDS/ IPS, DLP, URL 필터링, TLS 해독, 안티바이러스와 같은 보호를 시행합니다.

Multicloud Defense Terraform 제공자

Multicloud Defense 리소스를 구축 및 관리하기 위한 IaaS(Infrastructure-as-Code) 인터페이스입니다. DevOps 및 DevSecOps 팀은 이를 통해 Terraform 워크플로우를 통해 보안 인프라와 정책을 인스턴스화할 수 있습니다.

노스바운드 트래픽

인터넷 또는 외부 네트워크에서 클라우드 호스팅 애플리케이션 및 워크로드로 향하는 인바운드 트래픽 플로우입니다. Multicloud Defense 문서에서 노스바운드 트래픽은 일반적으로 인그레스 보호 및 역방향 프록시 검사와 관련이 있습니다.

남-북 트래픽

클라우드 워크로드에서 인터넷 또는 외부 서비스로 향하는 아웃바운드 트래픽 플로우입니다. Multicloud Defense 설명서에서는 이 방향을 이그레스 보호 및 정방향 프록시 또는 전달 작업과 연결합니다.

OCI

OCI(Oracle Cloud Infrastructure)는 클라우드 컴퓨팅 플랫폼입니다. Cisco Multicloud Defense와 기본적으로 통합되어 분산된 환경에서 일관된 통합 방어를 제공합니다.

정책

허용, 거부, 암호 해독, 검사 또는 로깅된 트래픽을 표현하는 보안 규칙 및 프로파일 집합입니다. Multicloud Defense에서는 정책이 중앙에서 생성되고 클라우드 환경 전반의 시행 지점에 적용됩니다.

프록시 모드

애플리케이션 콘텐츠를 더 심층적으로 검사하기 위해 연결을 종료했다가 다시 설정하는 게이트웨이 작동 모드입니다. 프록시 모드는 역방향 및 정방향 프록시 활용 사례, TLS 해독, WAF, DLP 및 기타 콘텐츠 검사 기능을 지원합니다.

역방향 프록시

인바운드 애플리케이션 트래픽에 대한 프록시 기능입니다. Multicloud Defense에서 역방향 프록시 기능은 인그레스 게이트웨이에서 트래픽이 애플리케이션에 도달하기 전에 검사하고 보호하는 데 사용됩니다.

규칙 집합

정책의 일부로 트래픽 또는 리소스에 적용할 수 있는 그룹화된 규칙 집합입니다. 규칙 집합은 관리자가 프로파일 및 보호된 플로우에 대한 시행 논리를 구성하는 데 도움이 됩니다.

보안 프로파일

위협 방지, 웹 애플리케이션 방화벽 동작, URL 필터링, TLS 해독 또는 DLP 같은 특정 검사 또는 보호 동작을 정의하는 재사용 가능한 구성입니다.

서비스 **VPC**/서비스 **VNet**/보안 **VPC**

Multicloud Defense 게이트웨이 및 지원 서비스의 중앙 집중식 허브로 사용되는 클라우드 네트워크입니다. 스포크 네트워크에 연결하고 검사 지점을 통해 트래픽을 조정합니다.

스포크 **VPC**/스포크 **VNet**

중앙 집중식 서비스 네트워크에 연결된 애플리케이션 또는 워크로드 네트워크입니다. 스포크 네트워크의 트래픽은 검사를 위해 Multicloud Defense 게이트웨이로 라우팅할 수 있습니다.

태그 기반 정책

클라우드 리소스 태그 및 워크로드 ID를 사용하여 규칙을 동적으로 적용하는 정책 방법입니다. 태그 기반 정책은 새로 구축된 리소스가 클라우드 환경의 변화에 따라 올바른 보안 제어를 상속하도록 지원합니다.

트래픽 가시성

클라우드 환경 전반에서 통신 패턴, 대상, 위험 범주 및 노출을 이해하기 위해 플로우 로그 및 DNS 쿼리 로그와 같은 트래픽 및 DNS 데이터를 사용합니다.

TLS 복호화

검사를 위해 암호화된 트래픽을 해독한 다음 트래픽을 전달할 때 재암호화하는 기능입니다. Multicloud Defense는 프록시 및 게이트웨이 활용 사례에서 TLS 해독을 지원하는 동시에 지원되는 설계에서 키 보관에 클라우드 네이티브 키 저장소를 사용합니다.

VPC 플로우 로그**/DNS** 쿼리 로그

네트워크 플로우 및 DNS 활동에 대한 가시성에 사용되는 클라우드 로깅 데이터 소스입니다. 이는 Multicloud Defense가 리소스를 검색하고 트래픽을 이해하고 보안 인사이트를 생성하는 데 도움이 됩니다.

웹 애플리케이션 방화벽

애플리케이션 레이어 공격으로부터 웹 애플리케이션을 보호하는 데 사용되는 레이어 7 검사 기능입니다. Multicloud Defense는 인그레스 보안 기능의 일부로 WAF(Web Application Firewall)를 포함합니다.

워크로드 **ID**

태그, 클라우드 메타데이터, 구축 유형, 환경 또는 애플리케이션 계층과 같은 워크로드를 설명하는 속성입니다. Multicloud Defense는 워크로드 ID 및 검색을 사용하여 클라우드 리소스 전체에서 유동 정책을 구축합니다.

© Cisco Systems, Inc. 모든 권리 보유.

번역에 관하여
Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.