멀티 클라우드 방어 구성 요소

다음 구성 요소가 멀티 클라우드 방어 경험을 구성합니다.

멀티 클라우드 방어 컨트롤러

멀티 클라우드 방어 컨트롤러는 CDO와 함께 제공되는 SaaS(Software as a Service) 구성 요소입니다. 멀티 클라우드 방어의 컨트롤 플레인으로 작동하며 관리자가 멀티 클라우드 방어의 모든 측면을 구축, 구성 및 관리할 수 있는 기능을 제공합니다. 또한 멀티 클라우드 방어 컨트롤러 또는 Terraform 제공자에서 수행되는 작업과 클라우드 서비스 제공자 내에서 해당 작업의 오케스트레이션 간의 변환 레이어이기도 합니다.

멀티 클라우드 방어 컨트롤러를 통해 제공되는 기능은 다음과 같습니다.

- 클라우드 서비스 제공자 계정 온보딩.
- 클라우드 서비스 제공자 자산 및 트래픽 가시성 검색.
- 서비스 VPC/VNet 생성 및 관리.
- 스포크 VPC/VNet 보호 관리.
- 게이트웨이 구축, 자동 확장 및 업데이트.
- 보안 정책 정의 및 구축.
- 타사 SIEM 및 알림 통합.
- 트래픽 및 보안 이벤트 조사와 분석.
- 검색 및 위협 인식 보고서 생성.

CDO 작업은 멀티 클라우드 방어 컨트롤러 업데이트를 담당합니다. 개선 사항 및 업데이트는 자주 제공되며, 계획된 릴리스 업데이트에 따라 정기적으로 제공되거나 중요 수정을 신속하게 해결하기 위해 핫픽스로 구축될 수 있습니다.

멀티 클라우드 방어 게이트웨이

멀티 클라우드 방어 게이트웨이는 클라우드 서비스 제공자 계정에 구축된 데이터플레인으로 작동하여 공용 클라우드 워크로드를 보호하는 PaaS(Platform as a service) 제공 구성 요소입니다. 멀티 클라우드 방어 게이트웨이는 전적으로 클라우드 서비스 제공자 계정 내에서 구축 및 운영됩니다. 모든 트래픽 처리 및 보안 보호는 클라우드 서비스 제공자 내부에서 이루어집니다.

멀티 클라우드 방어 게이트웨이가 제공하는 기능은 다음과 같습니다.

- 워크로드를 보호하는 클라우드 네이티브 아키텍처.
- 인그레스, 이그레스 및 이스트-웨스트 활용 사례.
- 전달 및 프록시 기반 처리.
- 트래픽 페이로드 검사를 위한 전체 암호 해독.
- WAF(Web Application Firewall), IDS/IPS, DLP 및 L7 DOS의 고급 보안 기능.
- L4, URL/URI, 악성 및 지리적 IP를 통한 필터링.
- 멀티 클라우드 방어 컨트롤러 및 Terraform 제공자를 통한 오케스트레이션.
- 멀티 클라우드, 다중 지역 및 다중 가용성 영역 구축.
- 워크로드 수요에 기반한 동적 자동 확장.
- 클라우드 구조를 사용하는 동적 멀티 클라우드 보안 정책.

고객은 중단 없이 몇 분 안에 끝나는 간단한 업그레이드 절차를 통해 멀티 클라우드 방어 게이트웨이를 업데이트해야 합니다. 게이트웨이 개선 사항 및 업데이트는 자주 제공됩니다.

멀티 클라우드 **Defense Terraform** 제공자

멀티 클라우드 방어 terraform 제공자는 CICD(지속적인 통합, 지속적인 구축) 파이프라인을 통해 전체 멀티 클라우드 방어 구축을 구축, 구성 및 관리하는 데 사용되는 멀티 클라우드 서비스 제공자 IaC(infrastructure-as-code) 오케스트레이션 언어입니다. 독점적으로 또는 멀티 클라우드 방어 컨트롤러와 함께 사용할 수 있으며 컨트롤러로 수행할 수 있는 대부분의 작업을 수용합니다.

고객은 원하는 Terraform 릴리스를 참조하여 멀티 클라우드 방어 terraform 제공자를 업데이트하고 참조된 버전을 로드하는 `Terraform update` 명령을 실행해야 합니다.