FQDN 및 URL 필터링 범주

FQDN / URL 필터링 범주

멀티 클라우드 방어은(는) WebRootTM BrightCloud(www.brightcloud.com)의 위협 인텔리전스를 사용하여 위험 점수에 따라 웹 사이트를 분류합니다. 여기에는 FQDN(Fully Qualified Domain Name)(도메인 이름이라고도 함) 및 URL이 포함됩니다. 퍼블릭 클라우드 환경의 트래픽이 다음 사이트로 아웃바운드 연결(이그레스)할 때 84개 범주에 대한 사이트를 제공합니다.

- FQDN(도메인) - 10억 개 이상 분류된 FQDN(도메인)
- URL - 450억 개 이상의 분류된 URL

트래픽 인식 및 처리의 효율성을 개선하기 위해 게이트웨이는 상위 100만 개 FQDN/URL 및 해당 범주의 캐시를 사전 로드합니다. 게이트웨이는 또한 상위 100만 개에 포함되지 않는 10k FQDN/URL 및 해당 범주의 런타임 캐시를 활용합니다. 트래픽에 캐시된 FQDN/URL이 포함되어 있으면 범주가 즉시 알려집니다. FQDN/URL을 캐시에 없는 경우 게이트웨이는 컨트롤러에 쿼리하여 BrightCloud를 통해 범주를 확인합니다. 이 작업은 200ms 이내에 완료될 것으로 예상됩니다. 예상 시간 내에 완료되면 학습한 범주에 따라 트래픽이 처리되고, 프로파일은 범주에 대해 정의된 정책에 따라 트래픽에서 작동합니다. 작업이 예상 시간 내에 완료되지 않으면 트래픽은 미분류로 처리되며, 프로파일은 미분류에 대해 정의된 정책에 따라 트래픽에서 작동합니다. 해결 방법이 반환되면 학습된 범주는 후속 해결을 위해 캐시에 추가됩니다. 해결 방법이 예상 시간 내에 발생하고 트래픽이 이미 처리된 경우에도 마찬가지입니다. 런타임 캐시가 소진되면 게이트웨이는 가장 최근에 액세스한 FQDN/URL 및 해당 범주에 사용할 수 있는 공간을 보장하기 위해 가장 오래된 FQDN/URL 및 해당 범주를 10개 항목씩 배치로 비웁니다.

Note 범주를 사용한 FQDN 필터링은 다음에 대해 발생합니다.

1. TLS Client Hello의 SNI
2. FQDN 조회를 위한 DNS 쿼리
3. HTTP 호스트 이름 헤더(일반 텍스트 HTTP 트래픽용)

악성 범주

멀티 클라우드 방어은(는) 다음과 같은 범주를 특히 악성으로 간주합니다.

Table 1: 악성 범주 멀티 클라우드 방어은(는) 다음 범주를 특히 악성으로 간주합니다.

범주 이름	범주 설명
악성코드 사이트	사이트는 실행 파일, 드라이브 바이 감염 사이트, 악성 스크립트, 바이러스, 트로이 목마 및 코드를 비롯한 악성 콘텐츠를 호스팅합니다.
피싱 및 기타 사기	일반적으로 사용자의 개인 정보를 수집하기 위해 평판이 좋은 사이트를 사칭하는 피싱, 파밍 및 기타 사이트입니다. 이러한 사이트는 일반적으로 수명이 매우 짧기 때문에 가동 시간 측면에서 오래 가지 않습니다.
프록시 회피 및 익명 서비스	프록시 서버 및 기타 방법을 사용하여 URL 필터링 또는 모니터링을 우회하는 모든 방식으로 URL에 액세스할 수 있습니다. 필터링을 우회하는 웹 기반 번역 사이트
키로거 및 모니터링	사용자의 키 입력을 추적하거나 웹서적을 모니터링하는 소프트웨어 에이전트입니다. 사용자 이름 및 비밀번호와 같은 민감한 데이터를 수집하는 데 자주 사용됩니다.
스팸 URL	원치 않는 이메일(스팸) 메시지를 배포하는 것으로 알려진 사이트입니다.
스파이웨어와 애드웨어	최종 사용자나 조직에 알려지지 않은 또는 최종 사용자나 조직의 명시적인 동의 없는 정보 수집이나 추적을 제공하거나 조장하는 스파이웨어 또는 애드웨어 사이트는 또한 사용자의 컴퓨터에 설치될 수 있는 원치 않는 광고 팝업 및 프로그램에 대한 광고를 진행합니다.

범주 이름	범주 설명
봇넷	이러한 URL은 봇 네트워크의 일부로 확인되는 URL이며(주로 IP 주소) 네트워크 공격이 시작되는 지점입니다. 공격에는 스팸 메시지, DOS, SQL 주입, 프록시 재킹 및 기타 요청하지 않은 접촉이 포함될 수 있습니다.

멀티 클라우드 방어에서는 **Discover(**검색**)** > **Traffic(**트래픽**)** > **DNS** 및 **Investigate(**조사**)** > **Flow Analytics(**플로우 분석**)** > **Traffic Summary(**트래픽 요약**)**를 통해 트래픽을 볼 때 트래픽 분석을 제공합니다. 여기서 사전 정의된 *Malicious Categories(*악성 범주*)* 필터를 선택하여 이러한 악성 범주 FQDN 및 URL과 통신하는 인스턴스 및 VPC를 표시할 수 있습니다.

전체 범주 목록은 아래에 나와 있습니다.

전체 범주 목록

범주 이름	범주 이름	범주 이름	범주 이름
낙태	게임	자동차	성교육
마약 남용	정부 기관	음악	셰어웨어 및 프리웨어
성인 및 음란물	혐오물	뉴스 및 미디어	쇼핑
주류 및 담배	해킹	노출	소셜 네트워킹
경매	증오 및 인종 차별	온라인 연하장	사회
봇넷	건강 및 약품	공개 HTTP 프록시	스팸 URL
비즈니스 및 경제	가정 및 원예	파킹된 도메인	스포츠
부정행위	사냥 및 낚시	유료 웹서핑	스파이웨어와 애드웨어
컴퓨터 및 인터넷 정보	불법	P2P(peer-to-peer)	스트리밍 미디어
컴퓨터 및 인터넷 보안	이미지 및 비디오 검색	개인 사이트 및 블로그	수영복 및 속옷
확인된 스팸 소스	개별 주식 자문 및 툴	개인 저장소	교육 및 툴
콘텐츠 전달 네트워크	인터넷 통신	철학 및 정치적 지지	변환
신앙 숭배 및 주술	인터넷 포털	피싱 및 기타 사기	여행
데이트	채용 정보 검색	프라이빗 IP 주소	미분류
데드 사이트	키로거 및 모니터링	프록시 회피 및 익명 서비스	확인되지 않은 스팸 소스
동적으로 생성된 콘텐츠	아동	의심스러운 항목	폭력
교육 기관	법무	부동산	무기

범주 이름	범주 이름	범주 이름	범주 이름
엔터테인먼트 및 예술	로컬 정보	레크리에이션 및 취미	웹 알림
패션 및 뷰티	악성코드 사이트	참조 및 연구	웹 호스팅
금융 서비스	대마초	종교	웹 기반 이메일
도박	군 검색 엔진	서비스	

필터링 프로파일을 정책 규칙 집합 규칙과 연결

- FQDN 필터링 프로파일을 생성/편집하려면 FQDN 필터링을 참조하십시오.
- URL 필터링 프로파일을 생성/편집하려면 URL 필터링을 참조하십시오.

BrightCloud URL/IP 조회 툴

BrightCloud는 특정 FQDN/URL이 웹 평판과 함께 어떤 범주로 분류되는지 파악하는 데 사용할 수 있는 온라인 URL/IP 조회 툴(https://www.brightcloud.com/tools/url-ip-lookup.php)을 제공합니다.