

Alibaba Cloud Anti-Bot Service

產品簡介

檔案版本：20180929

目錄

1 什麼是爬蟲風險管理.....	1
2 核心功能.....	2
3 產品優勢.....	3
4 應用情境.....	4

1 什麼是爬蟲風險管理

雲盾爬蟲風險管理 (Anti-Bot Service , 簡稱Anti-Bot) 是一款網路應用安全防護產品 , 可有效檢測進階爬蟲 , 降低爬蟲、自動化工具對網站業務的影響。

雲盾爬蟲風險管理提供從Web、APP、到API介面一整套全面的惡意Bot防護解決方案 , 避免由於業務中某一環節的防護薄弱而導致安全短板。

購買開通Anti-Bot產品後 , 您只需要將您的網站網域名稱解析到Anti-Bot產品提供的CNAME地址 , 並在爬蟲風險管理控制台中配置來源站點伺服器IP , 即可啟用防護。將網站網域名稱接入Anti-Bot產品後 , 您網站所有的公網流量都將先經過Anti-Bot執行個體 , 所有惡意爬蟲流量都將在雲端被檢測、過濾 , 最終將正常的流量返回給來源站點伺服器 , 從而確保來源站點業務免受惡意爬蟲流量引發的資料泄露、業務欺詐等安全問題的影響。

2 核心功能

雲盾防爬蟲風險管理主要提供以下功能。

- 防護效果可視化：對風險及線上策略進行即時異動監控，並提供防護效果的匯總報表。
- 惡意Bot流量精準攔截：多維度刻畫並過濾Bot流量，防護業務避免遭受損失。
- 雲端共用威脅情報：利用雲端優勢共用海量的威脅情報，並對行業內集中性攻擊作出快速對抗響應。
- 豐富的處置方式手段：針對可疑機器流量請求，可直接攔截，同時提供自訂UI滑塊驗證互動。

3 產品優勢

雲盾爬蟲風險管理具有以下優勢。

風險生態體系

- 通過跨多行業的爬蟲行為分析，利用關係網路實現惡意爬蟲的擴充發現。
- 爬蟲在行業性業務目的方面非常明確，利用生態體系達成行業內協同防禦。
- 沉澱網路黑灰產業中已知常用的針對性惡意爬蟲的IP/User Agent資料。
- 共用億級由阿里巴巴集團業務經驗沉澱的風險情報。

雲端部署

- 部署在惡意Bot流量到達來源站點前，通過識別、過濾，使您的業務來源站點避免遭受攻擊壓力。
- 雲上資源支援彈性擴容，針對業務高峰可自由收縮，具備百萬級QPS業務的風險防控能力。
- 由專業安全技術團隊提供產品策略的持續更新，快速下發最新的攻防規則。
- 雲上可共用即時發現的惡意Bot特徵，形成協同防禦體系。

多層防護策略

- 提供最合適Web、H5、APP、API業務的惡意Bot防護方案。
- 提供多維度防護策略，更精準地刻畫惡意Bot特徵。
- 針對不同風險等級的惡意Bot，提供不同的處置手段。

4 應用情境

雲盾爬蟲風險管理在以下情境中都能為您的業務提供安全防護，有效避免業務遭受損失。

航空公司佔座

黃牛黨利用惡意爬蟲遍曆航空公司的低價票，同時批量發起機器請求進行佔座，導致航班座位資源被持續佔用產生浪費，最終引發航班空座率高對航空公司造成業務損失，並且損害正常使用者的利益。

電商活動黃牛

黃牛黨在電商活動時針對有限的高價值商品的限時秒殺、優惠活動等可牟利情境，批量發起機器請求來類比正常的交易，再將商品、資源進行倒賣從中賺取價差，導致電商企業的營銷資源無法觸達正常使用者，而被黃牛牟取暴利。

核心介面被刷

登入、註冊、SMS等業務環節作為業務中的關鍵節點，相關介面往往會被駭客利用，為後續的欺詐行為作準備。