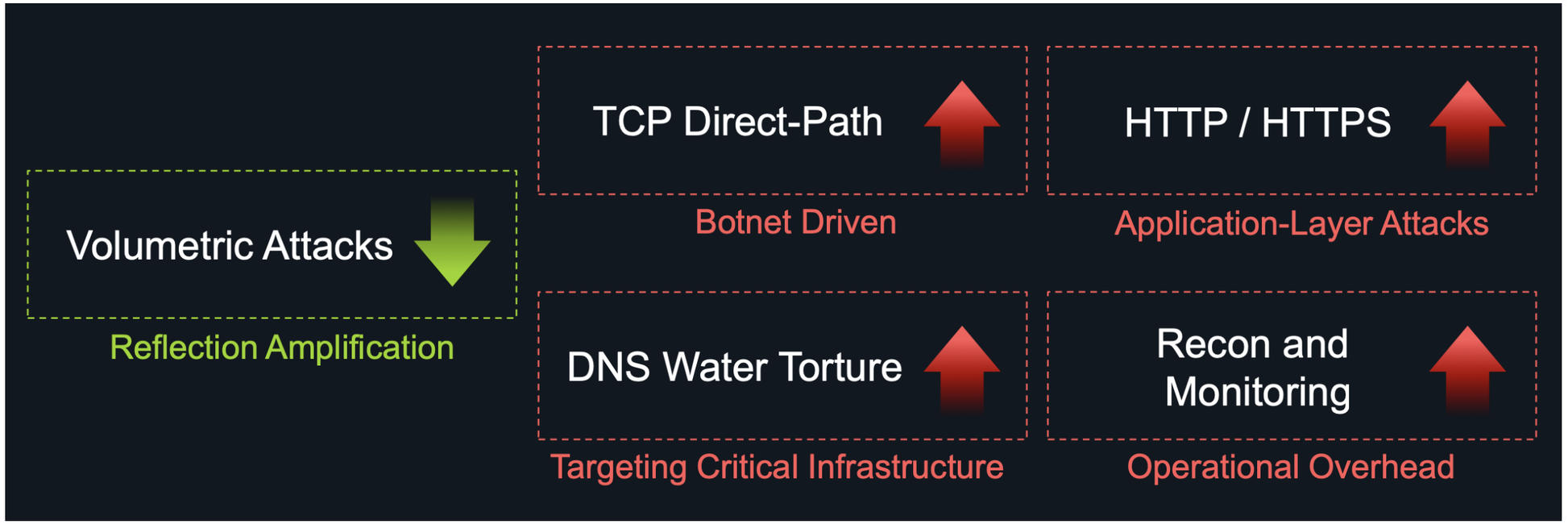
NETSCOUT

Adaptive DDoS 防護

NETSCOUT 的Adaptive DDoS 防護解決方案,專為 AED (Arbor Edge Defense) 設計。它能夠檢測和阻止不斷變化的 DDoS 攻擊,提供自動化的防護建議,並通過持續學習來適應新的威脅。該解決方案旨在應對當前 DDoS 攻擊的變化趨勢,包括 TCP 直接路徑攻擊、HTTP/HTTPS 攻擊、大規模攻擊、應用層攻擊等。

NETSCOUT

DDoS 攻擊的變化趨勢



DDoS 攻擊類型的多樣化

TCP Direct-Path、HTTP / HTTPS、Volumetric Attacks、Botnet Driven Application-Layer Attacks、Reflection Amplification、DNS Water Torture 等多種攻擊類型正在興起。這些攻擊針對關鍵基礎設施,並帶來了巨大的運營開銷。

攻擊特徵的變化

攻擊流量動態變化、高度分散的攻擊流量、攻擊資源的激增、國家支持的攻擊、高影響低流量攻擊、不可預測的攻擊流量等特徵給防禦帶來了新的挑戰。

NETSCOUT

Adaptive DDoS 防護方案

- 檢測:檢查所有對策通過的流量、檢測未被阻止的攻擊、識別攻擊類型和目標。
- 建議:為每種檢測到的攻擊類型提供有針對性的緩解建議、根據當前配置顯示推薦的保護配置更改。
- 行動:允許用戶選擇應用建議、自動應用建議(可選)、反饋循環以檢測進一步未被阻止的攻擊。

NETSCOUT 持續投資研發,以應對不斷變化的 DDoS 攻擊。