1. Client requests URL – request made to Akamai DNS service with global scale and segmented architecture to absorb the largest DDoS attacks
2. DNS resolves to the optimal Akamai Edge server with fewer lookups using zone apex mapping
3. Client connects and sends request to designated Edge server
4. Edge server inspects and takes action on malicious or bot requests:
   a. Adaptive rate controls automatically respond within seconds to block requests when the rate exceeds customer-defined thresholds. Also, IP blacklists and geo-blocking block requests from clients as defined
   b. Web Application Firewall inspects requests for malicious patterns and blocks based on anomaly risk score. Proprietary Kona Rule Set and nightly WAF testing maintains low false positives and false negatives.
   c. Bot Manager blocks or takes advanced management actions on requests generated by different types of automated bots, based on customer-defined bot categories
   d. Client Reputation leverages Akamai’s Cloud Security Intelligence big-data analysis engine to block requests from IP addresses that Akamai has observed attacking other Akamai customers
5. For cloud environments or smaller data centers without a /24, customers can configure origin ACLs to only allow communication from Akamai Site Shield servers and “cloak” the origin from attackers
6. For larger data centers with a /24, customers can route all network traffic (for both web and non-web applications) through an Akamai scrubbing center, where the Akamai SOC will inspect for and block any DDoS attack traffic