AKAMAI PRODUCT BRIEF

PROLEXIC

Defend internet-facing infrastructure against DDoS attacks

The risk of distributed denial-of-service (DDoS) attacks has never been higher, and more organizations need DDoS protection than ever before. To relieve the threat pressure, Akamai offers three purpose-built solutions to provide holistic cloud-delivered DDoS defense. Depending on the use case, application requirements, and desired time-to-mitigate service-level agreements (SLAs), App & API Protector, Edge DNS, and/or Prolexic would provide the highest-quality DDoS mitigation to keep web and internet-facing assets available and protected.

Overview

For data center and hybrid infrastructure protection, Prolexic provides cloud-delivered mitigation across all ports and protocols to stop DDoS attacks before they become business-impacting events.

Prolexic connectivity

Prolexic is purpose-built to stop DDoS attacks in the cloud, before they reach applications, data centers, and internet-facing infrastructure (public or private). Network traffic is directed in one of two ways via a border gateway protocol route advertisement change or DNS redirection (A record or CNAME record). Available as an always-on or on-demand service, Prolexic offers flexible integration models based on the needs of your desired security posture across hybrid origins.

With 20 global high-capacity scrubbing centers, Prolexic can stop attacks closer to the source to maximize performance for users and maintain network resiliency through cloud distribution. Traffic is routed via Anycast through the closest scrubbing center where the Akamai Security Operations Command Center (SOCC) deploys proactive and/or custom mitigation controls designed to stop attacks instantly — ensuring fast and accurate DDoS defenses.

Clean traffic is then returned to the customer origin via GRE tunnels, Layer 2 VLAN connections, and/or virtual IP (VIP)-to-origin back-end mapping.

BENEFITS FOR YOUR BUSINESS

Reduce DDoS risk

Proactive mitigation controls that stop more than 80% of the attacks we see instantly via Prolexic's zero-second SLA — to reduce attack surfaces

Stop the largest attacks

Proven ability to stop highly complex, record-breaking 1.44 Tbps and 809 Mpps attacks without sacrificing quality of mitigation

Optimize incident response

Custom runbooks, service validation exercises, and operational readiness drills help ensure business continuity

Unify security postures

DDoS mitigation policies applied consistently, regardless of where applications are hosted

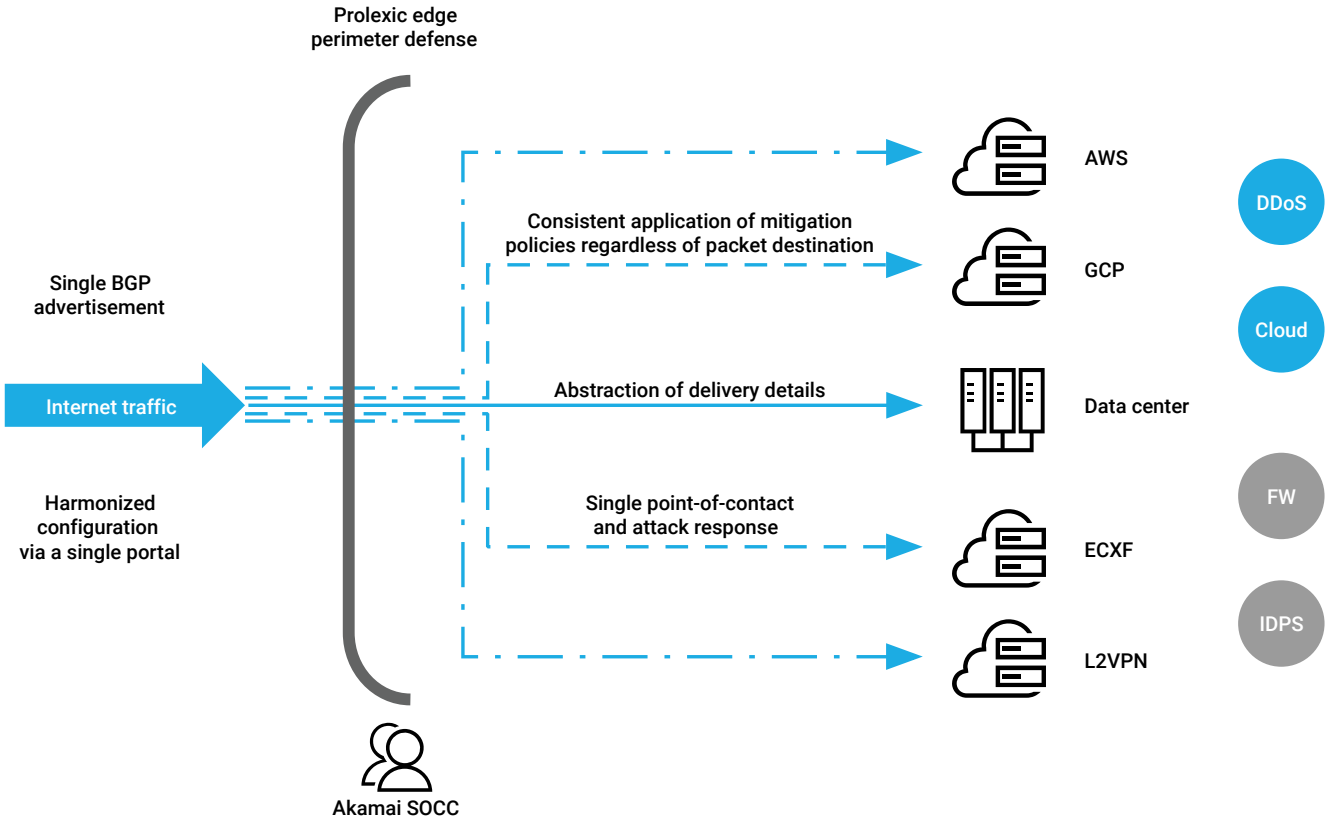
Scale security resources

Fully managed solution — backed by 225+ frontline SOCC responders — frees up defenders to focus on high-priority areas of security programs

Akamai

Prolexic integration options

- **Prolexic Routed — GRE:** Designed to be carrier agnostic for customers with a routable IP space (IPv4 /24 and/or IPv6 /48), configured via logical GRE tunnels for asymmetric clean traffic return to origin. Supports AWS BYOIP hybrid deployments.
- **Prolexic Routed — Connect:** Designed for customers with a routable IP space (IPv4 /24 and/or IPv6 /48), configured via direct VLAN connections to origin with asymmetric clean traffic return. Global platform partners include Equinix Cloud Exchange, GTT Communications, Megaport, and AT&T Tao, with more being added in the future.
- **Prolexic IP Protect:** Designed for customers with less than a routable IPv4 /24 and/or IPv6 /48, fragmented IP space, or cloud-hosting provider. Supports clean traffic to origin via symmetric routing.



Prolexic key capabilities

- **High-capacity defense:** Prolexic DDoS defense capacity increased from 8.2 Tbps to 10 Tbps — bringing the total Akamai edge capacity to 200+ Tbps — with plans to expand cloud-scrubbing centers into new locations globally.
- **Industry-leading zero-second SLA:** Prolexic mitigates approximately 80% of attacks via our zero-second mitigation SLA. This is achieved by working closely with customers to implement proactive defensive controls tailored to a customer's attack surface and risk profile, which takes place during the service validation process.
- **Intelligent defense stack:** Mitigation controls dynamically scale capacity to stop attacks across IPv4 and IPv6 traffic flows. Compute resources can be dynamically allocated to whatever mitigation controls need to be scaled up.
- **Broad and comprehensive SLA coverage:** In addition to our zero-second mitigation SLA, Prolexic offers 100% platform availability, time to mitigate, time-to-alert notification, time to respond, and individual time-to-mitigate SLAs based on specific attack vectors.
- **Laser-focused mitigation:** By creating bypass networks that passively analyze all customer traffic, Prolexic can mitigate each attack down to the specific /32 IP endpoint under attack without collateral damage. This /32 data can be integrated into a customer's security information and event management, billing systems analytics (to enrich data), analytics, business intelligence, or threat intelligence platforms via our 100+ APIs.

To learn more, visit the Prolexic page or contact your Akamai sales team.