

# DDoS Protector Cloud Service

## Zero-Hassle Protection against Zero-Day Threats

Distributed Denial-of-service (DDoS) attacks are becoming more frequent, powerful and sophisticated. With the growing online availability of attack tools, the pool of possible attacks is now larger than ever. The Check Point DDoS Protector Cloud Service defends organizations against today's most advanced DDoS attacks using advanced behavioral-based detection for both network-layer (L3/4) and application-layer (L7) attacks, automatic real-time signature creation to protect against zero-day attacks, unique SSL DDoS protection and flexible cloud-based and hybrid deployment options to suit every customer.

### Zero-day DDoS Protection

Check Point provides the industry's best DDoS protection, based on behavioral-based technology to protect against known and unknown threats

### Smart SSL Attack Mitigation

Check Point's unique technology defends against potent SSL DDoS attacks without requiring full customer SSL keys and without adding latency in peacetime

### Faster Time to Security

Check Point's advanced automation technologies result in faster detection, higher-quality mitigation and reduced exposure for organizations

### Single Pane of Glass

Check Point offers a seamless security solution that provides organizations with multi-layered protection, centralized reporting and full visibility



## How Check Point Protects You Against DDoS Attacks Faster and Better

### Behavior-Based Detection

Check Point uses advanced machine-learning algorithms that analyze traffic, learn what constitutes legitimate behavior and automatically blocks malicious attacks

### Automatic Signature Creation

With patent-protected real-time signature-creation technology, Check Point provides the only cloud service that can automatically generate protection against zero-day and unknown DDoS attacks

### Multiple Deployment Options

Check Point's DDoS Protector Cloud Service can be delivered in On-Demand, Always-On, or Hybrid configuration, and can be customized to suit any customer need, network topology or threat profile

### GLOBAL COVERAGE, MASSIVE CAPACITY

Check Point's DDoS Protector Cloud Service is backed by a worldwide network of 16 global scrubbing centers, with 8 Tbps of mitigation capacity (and growing). Check Point's scrubbing centers are globally connected in full mesh mode, using Anycast-based routing. This ensures that DDoS attacks are mitigated closest to their point of origin, and provides truly global DDoS mitigation capable of absorbing even the largest volumetric attacks.



## Choosing the Right Solution for You

### On Demand

- No added latency in peacetime. Traffic diverted only upon attack detection
- Allows lowest-cost, cloud-only simple deployment
- Best suited for latency-sensitive applications and organizations that are infrequently attacked

### Always-On

- Always-available, real-time, cloud-based DDoS protection
- Provides immediate protection but with small added latency
- Best suited for applications hosted on the cloud and for organizations that constantly come under attack

### Hybrid

- Combines on-premises devices backed by cloud-based scrubbing capacity
- Real-time protection and minimal latency in peacetime
- Recommended security best practice, best suited for data center protection

## SERVICE FEATURES OF CHECK POINT DDOS PROTECTOR CLOUD SERVICE

### Complete DDoS Protection Coverage

- Behavioral-based detection using advanced, patented machine-learning algorithms to protect against known and unknown threats
- Zero-day protection against network and application layer DDoS attacks such as Burst attacks, Dynamic-IP, DNS attacks and others
- Unique protection against SSL-based attacks without requiring customers to provide full SSL certificates and without adding latency in peacetime
- Extensive compliance options and certifications, unparalleled by any rival, including industry-specific certifications such as PCI and HIPAA, as well as cloud security standards such as ISO 27001, ISO 27017, ISO 27018, ISO 27032 and others

### White Glove Support

- Expert managed service through Check Point's Emergency Response Team (ERT)
- Pre-attack alerts from Check Point's library of cyber threat advisories, gathered by continuously mining data across the web and darknet, and post-attack forensic analysis and recommendations
- Dedicated Technical Account Manager (TAM) who serves as a focal point for all issues, including configuration, integration, upgrades and attack mitigation
- Backed by the industry's most granular SLA, with detailed commitments for Time-to-Mitigate, Time-to-Detect, Time-to-Alert, Time-to-Divert, Consistency of Mitigation and overall Service Availability



### Flexibility in Deployment

- On-demand, Always-On, and Hybrid deployment options to suit any customer need or network configuration
- On-demand protection for applications hosted on public clouds such as AWS and Azure, providing both network and application-layer protection, based on Check Point's behavioral-based detection
- Seamless integration between premise-based and cloud-based components using Check Point's DefenseMessaging technology
- Protection for every asset from a single IP address to an entire data center

### Easy Management and Control

- Rich centralized dashboard to display new threats and gain visibility for all assets, both on-premises and cloud-based
- Granular alerting capabilities, including email, text message, and phone notification to make sure you're the first to know if something happens
- Easy-to-read executive reports with concise incident details
- REST API for SIEM integrations



### CONTACT US

**Worldwide Headquarters** | 5 Shlomo Kaplan, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

**U.S. Headquarters** | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | www.checkpoint.com