



Managed DDoS Protection

Advanced DDoS protection as a managed service

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. Leveraging Radware's Cloud DDoS Protection, CBTS' Managed DDoS Protection Service defends against today's most advanced DDoS attacks. The service includes 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

Providing the industry's best DDoS protection, using behavioral-based technology to protect against known and unknown threats.



SMART SSL ATTACK MITIGATION

Unique technology defends against potent SSL DDoS attacks without adding latency and without compromising customer privacy.

FASTER TIME TO SECURITY

Advanced automation technologies result in faster detection, higher-quality mitigation and reduced exposure for organizations.



24x7x365 MANAGEMENT

Monitoring, alerting, escalation, and resolution of incidents in a fast and timely manner following industry ITIL best practices.



Protecting against DDoS attacks faster and better

Behavioral-Based Detection

Including advanced machine learning algorithms that analyze traffic, learn what constitutes legitimate behavior, and automatically block malicious attacks.

Automatic Signature Creation

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

Multiple Deployment Options

Our managed DDoS protection service can be delivered in On-Demand, Always-On or Hybrid configurations and can be custom-tailored to suit any customer need, network topology, or threat profile.

Global coverage, massive capacity

By partnering with Radware, CBTS' Managed DDoS Protection Service is backed by a worldwide network of 13 scrubbing centers, with 5TBs of mitigation capacity (and growing). Radware'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-on 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 Radware's Cloud DDoS Protection 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, Dynamic IP, DNS, and other attacks.
- 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 27002, ISO 27017, ISO 27018, ISO 27032, and others.

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 Amazon Web Services (AWS) and Azure, providing both network- and application-layer protection, based on Radware's behavioral-based detection.
- Seamless integration between premises-based and cloud-based components.
- Protection for every asset, from a single IP address to an entire data center.

White Glove support

- Expert monitoring service of pre-attack alerts are received from Radware's library of cyberthreat advisories, gathered by continuously mining data across the web and darknet, and post-attack forensic analysis and recommendations.
- Notification, action and remediation by CBTS based off SLA.
- Support from our state-of-the-art Enterprise Network Operations Center staffed by our highly certified engineers and operations experts.
- Backed by the industry's most granular service-level agreement (SLA), with detailed commitments for time to mitigate, time to detect, time to alert, time to divert, consistency of mitigation and overall service availability.

Eliminate the burden of monitoring and management

- Focus on strategic initiatives that improve your bottom line.
- Manage budget while improving your security posture.
- Gain access to skilled security professionals.



cbts

Managed DDoS Protection
cbts.com 001210216 B



Security, covered.