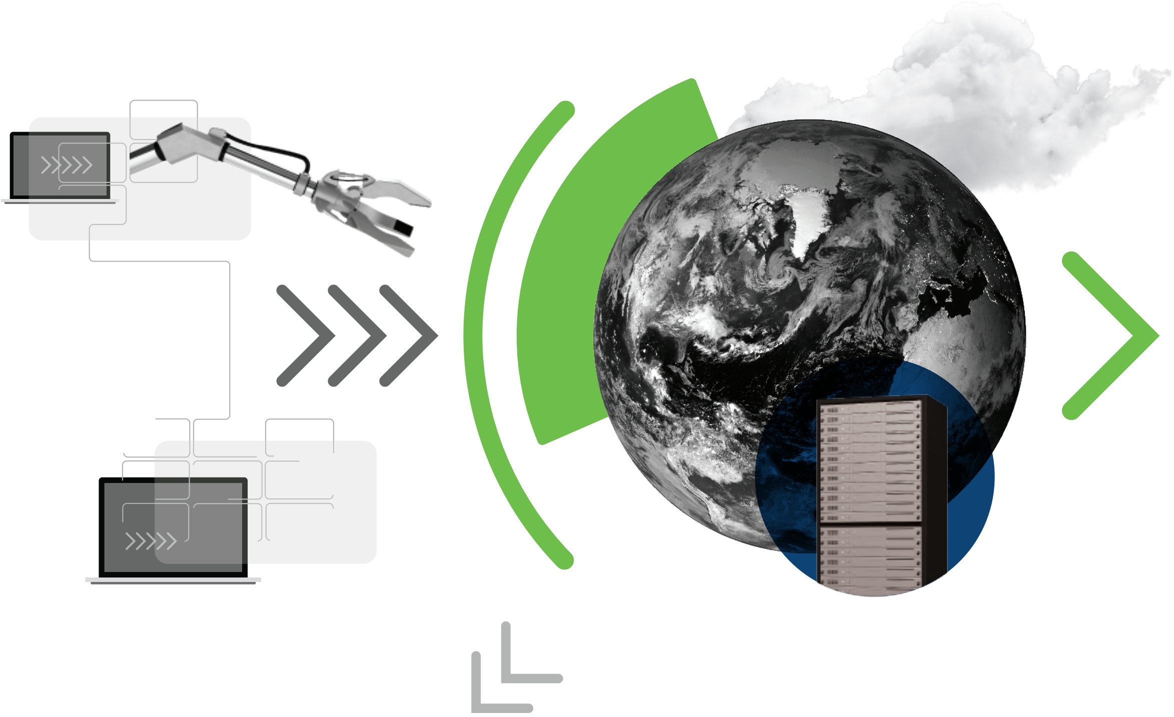
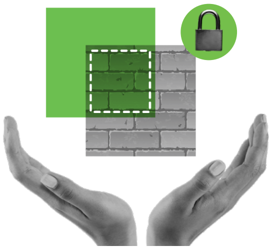
CISCO SECURE

Solution Brief
Cisco Public

Cisco Secure Cloud DDoS Protection



CISCO The bridge to possible



Distributed Denial-of-Service (DDoS) attacks are becoming more frequent, powerful, and sophisticated. With the growth in online availability of attack tools, the pool of possible attacks is now larger than ever. Cisco® Secure Cloud DDoS Protection[1], powered by Radware, 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 that suit every customer.

State-of-the-Art DDoS Protection

Comprehensive DDoS protection from all possible threats using behavioral-based detection, automatic signature creation, and unique SSL attack mitigation.

Industry-Leading SLAs

Committed to detect, alert, divert, and mitigate due to advanced automation and predefined workflows. Broad set of additional services and metrics for visibility and control.

Multiple Deployment Options

On-demand, always-on, and hybrid deployment models to uniquely suit customer needs, network topology, or threat profile.

Expert Global Support

A global emergency response team serves as the focal point for best practices, strategy, and alerts throughout an attack.

Quadrant Knowledge Solutions
SPARK MATRIX: DDoS Mitigation, 2023
LEADER

Quadrant Knowledge Solutions
SPARK MATRIX: DDoS Mitigation, 2022
LEADER

FORRESTER®
WAVE LEADER 2021
DDoS Mitigation Solutions

IDC
Analyze the Future

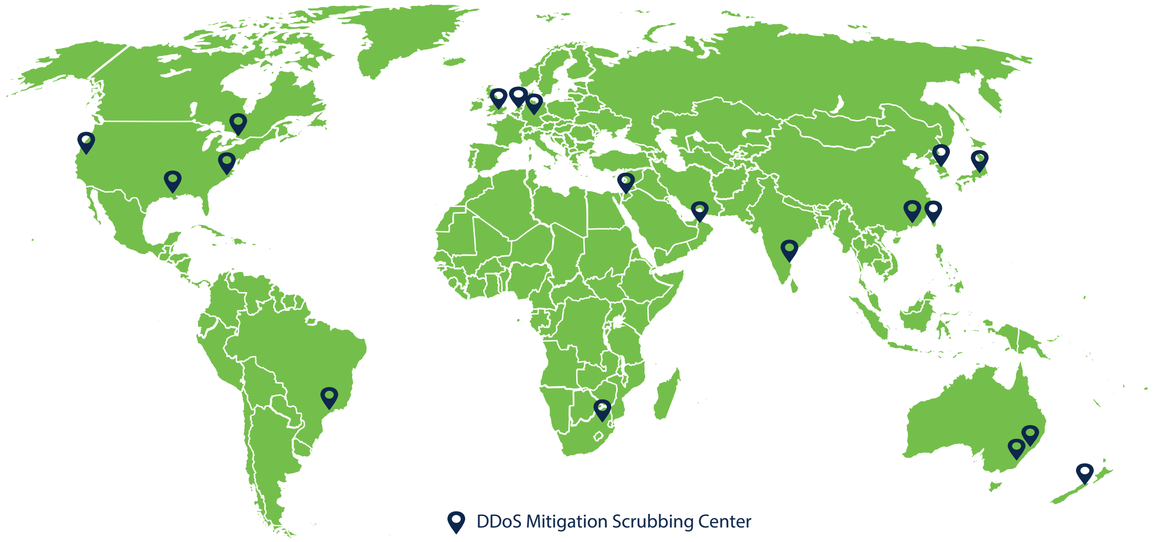
[1] Cisco Secure DDoS Protection solutions are sold by Cisco through its global OEM partnership with Radware, Inc.

Cloud DDoS Deployment Options

On-Demand	Always-On	Hybrid (includes on-prem)
No added latency in peacetime; traffic diversion only upon attack detection	Always-available, real-time, cloud-based DDoS protection	Combines on-premise devices backed by cloud-based scrubbing capacity
Allows lowest cost, cloud-only simple deployment	Provides immediate protection but with minimal added latency	Real-time protection and minimal latency in peacetime
Best suited for latency-sensitive applications and organizations that are infrequently attacked	Best suited for cloud-hosted applications and organizations constantly under DDoS attacks	Recommended security best practice; best suited for data center protection

Global Coverage, Massive Capacity

Secure Cloud DDoS Protection is backed by Radware's worldwide network of 19 scrubbing centers with 12 Tbps of mitigation capacity (and growing). The 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.



Simplified Management and Control

Full Visibility

Provides a single location for all relevant information and data. Includes detailed traffic information and important peacetime information as well as advanced analytics that contribute to the management of the network.

Enhanced User Experience

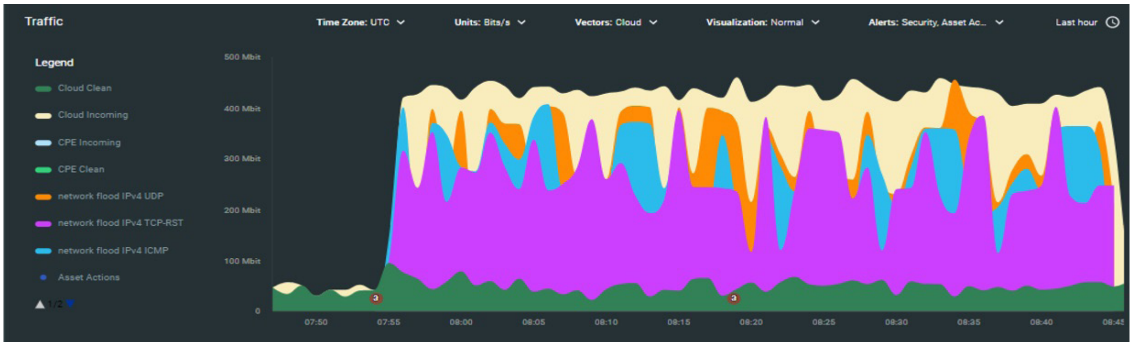
With a highly intuitive user interface, navigation across screens and interfaces requires only a few clicks. The UI includes a dark mode option as a well as a regular mode to meet the user's preference.

Attack Centric

Network health status is updated in real time while under attack, and a clear indication is displayed. An attack asset display provides important attack information. This enables users to respond promptly.

Detailed Reporting

Valuable reports and analysis are provided whether in peace time or under attack. Information is easily viewed by a single widget. This data can be exported for additional analysis.



Traffic

Time Zone: UTC
Units: Bits/s
Vectors: Cloud
Visualization: Normal
Alerts: Security, Asset Ac...
Last hour

White Glove Support

- An expert managed service is provided by the Radware Emergency Response Team (ERT), Cisco's OEM DDoS partner.
- Pre-attack alerts from Radware's library of cyberthreat advisories, gathered by continuously mining data across the web, darknet, and post-attack forensic analysis and recommendations.
- A dedicated ERT Technical Account Manager (TAM) serves as a focal point for all issues, including configuration, integration, upgrades, and attack mitigation.
- Backed by the industry's most granular and comprehensive Service-Level Agreement (SLA), with detailed commitments for time to mitigate, detect, alert, and divert, enabling consistency of mitigation and overall service availability.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte.Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at https://www.cisco.com/go/offices.