Cisco Secure Cloud WAF and Bot Protection

Contents

Application Security for Business Availability and Resilience

Adaptive Protection for an Evolving Threat Landscape

Web application development is becoming increasingly complex. As web application development times shrink, risk and vulnerabilities increase. The Cisco® Secure Cloud WAF[1] offers industry-leading web application and API protection. Using a positive security model based on machine-learning technologies, Secure Cloud WAF provides comprehensive protection against OWASP top 10 threats as well as zero-day attacks and other application security vulnerabilities.

The Cisco Cloud WAF service provides dynamic security policies with automatic false-positive correction, built-in application distributed-denial-of-service (DDoS) protection, integrated bot mitigation, and many other features to help protect organizations from risk of data loss.

Comprehensive application security
Secure Cloud WAF provides full web application protection including OWASP top 10 coverage, advanced attack protection, and zero-day attack protection using both negative and positive security models.

Reduced overhead and cost
Secure Cloud WAF's automated defenses, backed by expert 24x7 managed services, take the burden off the IT staff and provide improved security outcomes with reduced overhead and expense.

Faster time to security
Secure Cloud WAF automatically detects threats and protects new web applications as they are added to the network using automatic policy generation technology.

Simplified management and reporting
Secure Cloud WAF offers an integrated security solution that provides multivector web application protection with centralized management and reporting.

[1] Cisco Secure WAF Protection solutions are powered by Radware, Inc.

Security and Agility

Cisco Secure Cloud WAF Protection leverages multiple industry-leading technologies to protect your business from application attacks.

Continuous learning – Secure Cloud WAF uses advanced machine-learning algorithms to analyze traffic, learn what legitimate traffic looks like, and automatically block malicious activity.

Application mapping – Secure Cloud WAF automatically maps protected applications, detects code changes whenever features are added or modified, and identifies potential security vulnerabilities.

Adaptive security policies – Secure Cloud WAF continuously adapts and refines security policies to optimize application security, maximize overall security protection, and minimize false positives.

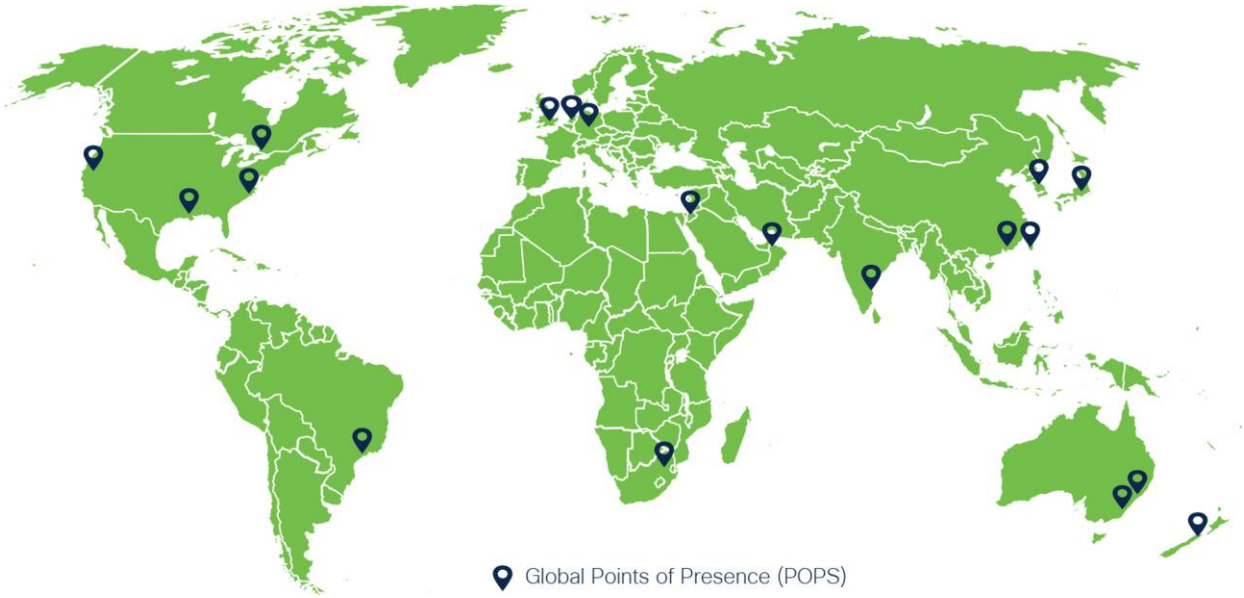
Expert managed services support – Secure Cloud WAF is supported by our global Emergency Response Team (ERT), providing unparalleled, 24x7 security expertise and managed services support.

Full PCI Compliance

Cisco Secure Cloud WAF Protection fully implements all ten recommended security mechanisms of the PCI DSS Requirement 6.6, which includes enforcing a positive security model and implementing data leakage prevention (DLP) controls. Secure Cloud WAF is also PCI DSS certified and utilizes technologies that are certified by NSS Labs and ICSA Labs, allowing customers to deploy our cloud WAF services with confidence.

Global WAF Points of Presence

Secure Cloud WAF Protection is backed by a global network of strategically located WAF points of presence (POPs), ensuring that you are protected by the PoP that is closest to your origin server. These POPs are located at major traffic hubs with connections to Tier 1 ISPs to ensure low latency and minimal impact on web application performance.



Cloud WAF Protection Service Features

Complete Protection against OWASP Top 10 and Zero-Day Attacks

- Based on a combination of a negative and positive security model that uses advanced behavioral-analysis technologies to detect malicious threats.
- Complete API discovery and protection that provides visibility, enforcement, and mitigation of all forms of API abuse and manipulation, whether for on-premises or cloud-hosted environments.
- Built-in DDoS protection to stop application-layer DDoS attacks. For more information on Cisco Secure DDoS Protection, see https://www.cisco.com/go/secure-ddos.
- Seamless integration with bot management technology to detect and mitigate the most sophisticated, human-like bots.
- Data leakage prevention mechanisms to automatically mask sensitive user data, such as Personally Identifiable Information (PII).

Agile, Adaptive Application Security

- Automated API discovery that requires no application or security expertise and provides adaptive protection for both documented and undocumented APIs.
- A dedicated Technical Account Manager (TAM) serves as a focal point for all issues, including configuration, integration, upgrades, and attack mitigation.
- Continuously adaptive policies that automatically map applications, detect changes, and dynamically deploy the optimal security policies.
- Automatic false-positive correction using powerful machine-learning algorithms that identify legitimate application behavior.
- Automated continuous security policy refinements, based on advanced machine-learning algorithms, automatically and continuously review large log files, find anomalies, and automatically suggest policy refinements.

Flexible Deployment

- Application protection for any cloud, including public clouds and hybrid environments with Radware SecurePath™, an innovative, API-based, out-of-path service that enables reduced latency and increased uptime[2]. SecurePath eliminates inline bottle necks and does not require SSL key sharing or traffic redirection.
- Support for high-capacity SSL traffic to ensure full SSL availability from the nearest PoP, even during peak times.
- Global CDN service based on Amazon CloudFront CDN, with over 300 PoPs in more than 90 cities across more than 47 countries and portal integration for unified management and reporting from a single dashboard.

[2] SecurePath is a registered trademark of Radware, Inc.

- Advanced load-balancing capabilities, which includes both local and global site load balancing (GSLB), site failover, high availability, and health monitoring.
- Extensive compliance and certifications including industry-specific certifications such as PCI and HIPAA and cloud security standards such as ISO 27001, ISO 27701, ISO 27017, ISO 27018, ISO 27032, and others.

Simplified Control and Management

- Rich centralized dashboard to display threats and manage configuration
- Granular alerting capabilities to make sure that you are the first to know if something happens
- Easy-to-read executive reports with concise incident details
- Centralized reporting for Web Application and API Protection, bad bots, and DDoS attacks.

Protection from Malicious Bots

Over half of all internet traffic is generated by bots — some legitimate, some malicious. Competitors and adversaries alike often deploy malicious bots that leverage multiple vectors to attack applications and data. This includes account takeover, scraping data, denying available inventory, and launching denial-of-service (DoS) attacks with the intent of stealing data or causing service disruptions. Sophisticated large-scale attacks often go undetected by conventional mitigation systems and strategies.

Leveraging proprietary, semisupervised machine-learning capabilities, Cisco bot management allows precise bot management across web and mobile applications and APIs, combining behavioral modeling for granular intent analysis, collective bot intelligence, and device fingerprinting. A nonintrusive, API based approach detects and blocks highly sophisticated human-like bots in real time, which can be massively distributed or adequately “low and slow” to operate under the permissible limits of rule-based security measures. Collective bot intelligence, provided by Radware, gathers bot signatures from clients worldwide to build a database of bot fingerprints and proactively stop bots from infiltrating into your internet properties.

Intent-based Deep Behavioral Analysis (IDBA)
Accurately identifies the intent of bots using proprietary semisupervised machine learning models

Full Coverage of OWASP Automated Threats
Protection from all forms of account takeover, denial of inventory, DDOS, card fraud, and web scraping

Secure all Channels: Web, Mobile, and APIs
Protects against bots that target digital assets, including sophisticated bots designed to attack multiple targets

Flexible Integration Options
Nonintrusive deployment using SDK, web server, or content delivery network (CDN) plug-ins, JavaScript (JS) tag or as a reverse proxy with no impact on the technology stack

Detection and Mitigation With High Accaccuracy

Cisco bot management uses a proprietary Intent-Based Deep Behavior Analysis (IDBA) to understand the intent of highly sophisticated nonhuman traffic. It does this by collecting over 250 parameters including browsing patterns, mouse movements, keystrokes, and URL traversal data points from the end user's browser and using proprietary algorithms to build a unique digital fingerprint of each visitor. IDBA uses this information to perform a behavioral analysis at a higher level of abstraction of "intent," unlike the commonly used shallow "interaction"-based behavior analysis. Capturing intent enables IDBA to provide significantly higher levels of accuracy while detecting bots with advanced human-like interaction capabilities. IDBA uses semisupervised machine learning and leverages the latest developments in deep learning for accurate identification and management of bots.

Ability to Handle Bot Traffic in Multiple Ways

Actions are customized based on bot signatures and bot types. Our bot management solution uses multiple techniques to identify and analyze suspected bots, leveraging responses in a closed-loop feedback system to minimize false positives.

Dedicated API Protection

The solution provides control of navigation flow and fingerprint machine-to-machine communications to reduce risk and avoid invoking APIs that are accessed or targeted by misbehaving bots.

Complete Application Security Suite

The suite includes a WAF, a bot manager, API security, and DoS mitigation brought together to provide the most robust application protection. Device fingerprinting implemented in Secure Cloud WAF uses dozens of characteristics of the device in a unique way to identify and distinguish it from all others. Using proprietary tracking, the solution can generate device reputational profiles that combine both historical behavioral information aiding in the detection and mitigation of threats such as DDoS, intrusions, and fraudsters alike. By correlating past security violations of specific devices over time and across visits regardless of changing IP address, Cisco bot management can consistently and accurately profile legitimate and illegitimate users.

Cisco API Protection Solution

WAF, bot management solutions (with API protection algorithms), and API gateways are the primary inline security tools for API protection. While API gateways usually offer authentication and authorization features, their HTTP traffic and payload analysis as well as their OWASP top 10 API security risks and web protection capabilities are either limited or absent.

By combining positive and negative security models together with an auto-learning and a purpose-built bot management solution for APIs, Cisco secures APIs from known and zero-day attacks as part of its web application security solution.

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**.

Printed in USA C22-xxxxxx-xx 04/23