CISCO SECURE

Solution Brief
Cisco Public

Cisco Secure Web Application Firewall (WAF) Integrated Application Protection

The bridge to possible

Contents

Contents

The Web Application Security Space

The web application attack landscape is evolving quickly in conjunction with ongoing changes around application development, hosting, and maintenance. Trends such as DevOps and cloud migration are forcing application security teams to investigate new ways to keep up with new vulnerabilities and to manage policies across disparate hosting environments. One of the most commonly used products and services for web application security and API protection is the web application firewall (WAF) that sits in front of the application server and inspects inbound and outbound requests and responses to ensure they comply with various policies.

The following document reviews (1) the security requirements for web application protection and API protection and (2) Cisco's web application security and API protection solution, Cisco® Secure WAF, which is available in several form factors, including integration into Cisco Secure Application Delivery Controller (ADC).[1]

Assessing the Application and API Attack Landscape

Application Vulnerabilities

The top application security challenges are defined by the Open Web Application Security Project (OWASP) Top 10 application threats. Organizations that seek effective application protection use the OWASP Top 10 as a starting point for ensuring protection from the most common threats and application misconfigurations that can lead to security vulnerabilities.

In addition to the OWASP Top 10 project, many other types of attacks complicate web application security. These attack vectors can involve HTTP protocol manipulation, leading to HTTP request splitting and HTTP response splitting attacks.

They can also include various traffic processing weaknesses, which may result in a denial of service or other application-based attacks such as Buffer Overflow, Directory Traversal, OS Commanding, Path Traversal, and others.

OWASP Top 10 – 2021

A01:2021-Broken Access Control

A02:2021-Cryptographic Failures

A03:2021-Injection

A04:2021-Insecure Design

A05:2021-Security Misconfiguration

A06:2021-Vulnerable and Outdated Components

A07:2021-Identification and Authentication Failures

A08:2021-Software and Data Integrity Failures

A09:2021-Security Logging and Monitoring Failures

A10:2021-Server-Side Request Forgery (SSRF)

Figure 1. OWASP Top 10 list

[1] Cisco Secure WAF, bot management, and Secure ADC are sold under Cisco's global OEM partnership with Radware.

API-Related Risks

As the popularity of applications continues to grow, the use of APIs has grown rapidly. APIs enable applications to interoperate with other services by integrating different clients and applications across multiple services.

APIs are used in a variety of modern applications, and the number of use cases is continuously growing. The most common examples are:

- Web APIs, mostly in single-page applications
- Mobile applications
- Embedding public and third-party APIs as external services into an existing application (such as Google Maps APIs)

APIs are also used to save time and facilitate the flexible development of microservices architecture apps, agile development methodologies, and continuous delivery.

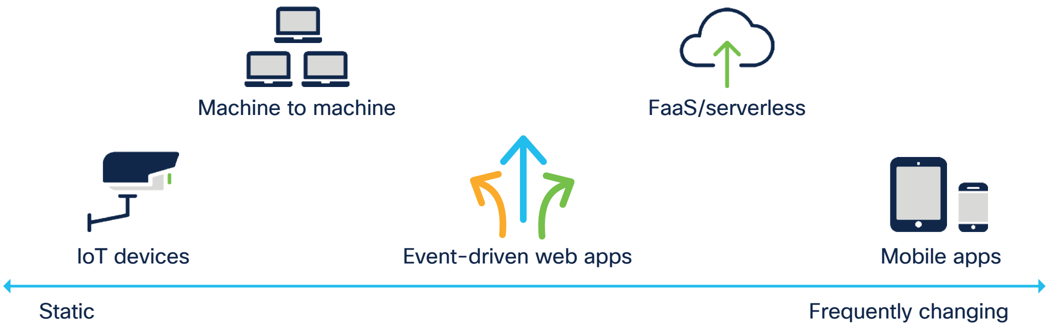


Figure 2. The API economy and use cases

DevOps environments, and the ever-increasing demand for continuous delivery, require complete process automation and the ubiquitous use of APIs:

- Service provisioning and management (for example, Amazon Web Services API)
- Platform management apps
- Continuous delivery process automation

The API Security Problem

While APIs offer tremendous benefits, they also introduce new security risks, including service disruption and data theft.

APIs are vulnerable to all types of attacks and threats against web applications. Most APIs are REST APIs with JSON bodies (REST-JSON), which run on top of the HTTP protocol. As such, most of the web application security risks are just as relevant for APIs. Additionally, APIs introduce other security challenges mostly around access control, as the APIs may be served independently and not only as a whole set of web application resources.

APIs submit and retrieve data and may expose application logic and potentially sensitive data. As a result, they have increasingly become a target for attackers trying to find easier ways into applications.

OWASP API Security Top 10
API1 - 2019 Broken Object Level Authorization
API2 - 2019 Broken User Authorization
API3 - 2019 Excessive data exposure
API4 - 2019 Lack of Resources & Rate Limiting
API5 - 2019 Broken Function Level Authorization
API6 - 2019 Mass Assignment
API7 - 2019 Security Misconfiguration
API8 - 2019 Injection
API9 - 2019 Improper Assets Management
API10 - 2019 Insuffcient Logging & Monitoring

Figure 3. Top 10 API security risks

API Protection Considerations

Because of the wide variety of API threats, API protection requires a combination of access controls (such as authentication and authorization mechanisms), injection prevention, bot management, DoS mitigation, and more.

Hackers may also try some API-specific attacks, such as using invalid schemas, parameter tampering, or token manipulations. In addition to supporting OpenAPI, an API protection solution should also cover unknown, undocumented APIs.

Access violation	Denial of service	Irregular expressions	Protocol attacks
38%	36%	33%	30%

Source: Radware application security research

Figure 4. Common attacks targeting APIs

The Challenge of False Positives and False Negatives

Web applications and API services are being accessed both by desired legitimate users and undesired attackers (malicious users whose goal is to harm the application and/or API end points). One of the biggest challenges in protecting web applications and API services is the ability to accurately differentiate between the two and identify and block malicious traffic while ensuring continuous service for legitimate users.

A false negative is caused when an attack is not detected or blocked by the WAF. False positives are the opposite problem – heightened security policies that cannot effectively differentiate legitimate users from attacks and therefore block legitimate users' transactions. Typically, organizations are more sensitive to false positives to the point of lowering their overall security posture to the level of not blocking any legitimate traffic at the risk of introducing false negatives.

Protection Quality – Negative Security Model

The most common protection scheme is based on a negative security model, which defines what is disallowed while implicitly allowing everything else. Most web application security solutions leverage a negative security model that utilizes few signatures for specific, previously witnessed attacks. To avoid false positives, many organizations tend to reduce the coverage of their negative security policies, focusing on known attack types and thereby resulting in a low protection quality.

While a well-tuned policy based on a negative security protection can provide reasonable protection against known attacks, it still leaves applications exposed to zero-day attacks. Certain OWASP Top 10 vulnerabilities (broken authentication, broken access control, and more) cannot be properly addressed with an application solution that relies solely on a negative security model.

Protection Quality – Positive Security Model

Protecting an application (or its API) against zero-day attacks (i.e., previously unseen attacks) requires a positive security model that defines the set of allowed transactions, data types, and values to ensure only legitimate activity is taking place. For example, if a positive security rule defines the allowed value type of a certain parameter as integer only, it will prevent SQL injection attacks even if there is no signature defined for that attack.

Most application protection solutions offering a positive security model often require significant human effort to create such rules manually, directly impacting the continuous validity of such a solution, and, subsequently, its total cost of ownership. This tedious process is also prone to human errors where these rules may generate false positives.

Auto-Policy Generation

To reduce the effort involved in creating a positive security policy and avoid the risks of human errors, an application protection solution should provide auto-policy generation based on machine learning capabilities for automatic rule definition and maintenance. Auto-policy generation is often based on the ability to identify and profile legitimate application transactions and creating "allow" rules based on it.

Anti-Bot Protection

Competitors and adversaries often deploy malicious bots that leverage a variety of methods to attack applications and application data. This includes account takeover, scraping of web 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 because bots have evolved from basic scripts to large-scale distributed bots with human-like interaction capabilities to evade detection mechanisms such as CAPTCHA and other challenges.

As the use of APIs increases, bot attacks targeting APIs are also becoming more common. Detecting malicious behavior on APIs is different than web and mobile applications and requires distinguishing between "good" and "bad" API calls.

To effectively stay ahead of the threats that bad bots impose on web applications and APIs requires a holistic approach that can correlate several bad bot characteristics for accurate detection and apply the most effective mitigation technique without impacting legitimate users. Here are some key capabilities:

- Effective device and browser fingerprinting (for example, detecting bots with changing IP addresses)
- Intent and behavioral analyses (such as correlating of intent signatures across devices)
- Collective bot intelligence and threat research
- Dedicated protection model to safeguard API against bot attacks
- Identifying authentic API access patterns to pinpoint malicious access attempts

An enterprise-grade bot detection engine should have deep-learning and self-optimizing capabilities to identify and block constantly evolving bots that alter their characteristics to evade detection by basic security systems.

Managed Services and Support

As application attacks increase in complexity, so must application security solutions. Deploying a WAF or a bot protection solution often leads to false positive. The amount of human resources and expertise required to keep the application protection service updated across heterogeneous environments while constantly tuning security policies is something many organizations don't have the resources for.

This is why buying a best-of-breed application protection solution is often not enough. One should also acquire access to professional services that support the deployment and maintenance of the solution as well as fight application attacks as they occur in real time. While a wide variety of application protection solutions exist in the market, not all vendors can offer complementary expert services.

Cisco Web Application and API Security

Cisco Secure Application Delivery Controller (ADC) provides a comprehensive set of application security tools that include its ICSA Labs–certified WAF, bot manager integration, API protection modules, and a live threat intelligence feed.

Cisco Secure WAF delivers full web application protection, including OWASP Top 10 coverage, advanced attack protection, and zero-day attack protection that automatically adapts to evolving threats and protected assets.

The bot management module allows precise bot management across web and mobile applications, combining behavioral modeling for granular intent analysis, collective bot intelligence, and device fingerprinting. A combination of WAF-based and bot manager-based dedicated API protection modules provide coverage against a wide variety of API attacks.

Additionally, a threat intelligence network continuously monitors ongoing attacks and potential attackers to produce a live feed of active attackers' IP to block those attackers before they can strike. This combination of application security and delivery modules provides organization with unmatched application protection.

Widest Application Vulnerability Protection with Cisco Secure WAF

Cisco's web application protection solution delivers comprehensive and accurate security coverage of known and unknown web application threats. It provides full security coverage out of the box against OWASP Top 10 threats. Its protection extends to the Web Application Security Consortium (WASC) threats as well as zero-day attacks.

By effectively providing defenses against those threats, Cisco improves and maximizes the web application's security, blocking or diverting future attacks.

Parsing and Normalization

Cisco's WAF technology terminates the client TCP connection to detect different evasion techniques such as TCP packet reply attack. It then applies the HTTP RFC inspections to detect HTTP protocol manipulations, such as HTTP Request Splitting attacks. Next, it decodes and normalizes the client inputs to bring them to their basic ASCII representation, similarly to what the web server would do.

XML and JSON

A key element in the parsing of HTTP requests is the processing of XML and JSON inputs to extract the key value pairs for proper inspection. XML and JSON key values are processed by web servers and can be used like any other client input to generate various attacks such as an XML Injection attack.

Cisco's WAF technology parses XML and JSON structures, allows definition of schema and structure restrictions, and extracts key value pairs for detailed parameter inspection by all signatures and rules defined by positive and negative security model in the policy.

Security Filters

Once the parsing of the traffic is accomplished, the application security rules are applied through a set of security filters. To a large extent, these are the security policy building blocks applying the protection rules and signatures. There is a list of more than a dozen security filters focusing on different aspects and dimensions of web application security. Some are targeted to detect and block injection attacks, while others are defining restrictions on parameter values.

For instance, one such filter is protecting against data leakage by identifying and then blocking or masking sensitive information transmission such as a credit card number (CCN) or social security number (SSN). Masking CCNs is an actual requirement of the PCI standard and is achieved with Cisco's WAF Service without an application modification.

Another example is a security filter that addresses session management attacks such as session fixation, cookie poisoning, and session hijacking through encryption or signing of cookies to avoid manipulation on the client side.

Positive and Negative Security Model

The best security coverage with minimal impact on legitimate traffic is made possible by Cisco's combination of negative (defining what is forbidden and accepting the rest) and positive security models (defining what is allowed and rejecting the rest). Combining the two models allows granular and accurate policy definitions, therefore avoiding false positives and false negatives.

The negative security model protection is based on up-to-date signatures against known vulnerabilities that provide the most accurate detection and blocking technology of application vulnerability exploits. The positive security model is useful in stopping zero-day attacks. The positive security rules and mechanisms allow definition of value types and value ranges for all client-side inputs, included encoded inputs and within structured formats as XMLs and JSONs. The positive security profiles limit the user input to only the level required by the application to properly function, thus blocking zero-day attacks.

Automated Application Protection Policy Generation

Building an optimized, application-specific security policy covering both negative and positive security rules typically demands intensive work on the part of the administrator while still leaving a system open to attack due to inherent human error.

Cisco Secure WAF leverages machine learning algorithms to automatically generate optimized security policies for each specific application. These algorithms enable organizations to:

- Reduce the amount of human resources required to generate such extensive security policies
- Eliminate human errors in the process
- Leverage negative and positive protection models
- Reduce false positives and false negatives
- Remain accurate as the application evolves by automatically adjusting the policy for each new version introduced

By leveraging machine learning algorithms, auto-policy generation secures a web application with as little human intervention as possible. There are different attributes of the secured application, the environment needs that impact the process of policy generation. The system automatically discovers the structure of a web application, while at the same time, auto-policy generation sets the relevant security filters, analyzes traffic properties from the production environment, and builds a dynamic network profile for a specific site according to which the auto-policy generation module automatically builds the policy.

Four Automated Steps to Secure Applications

Auto-policy generation has four distinct steps for generating an optimized security policy for an application.

Step 1 – Application mapping

Each application would naturally have different sections and zones, where each require a different set of security rules. There might be an admin zone with specific operations and URLs that only admins are allowed to access. There could also be a zone for users, with a different set of rights and URLs they can access. The first step of the algorithm is to automatically learn and map the application sections it protects with the different types of users and rights they might have.

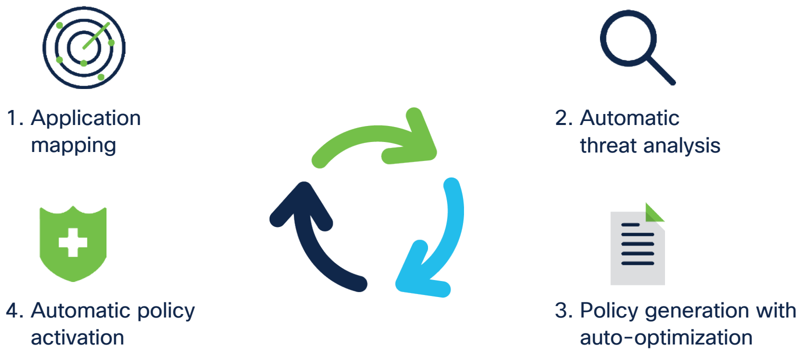

1. Application mapping
2. Automatic threat analysis
3. Policy generation with auto-optimization
4. Automatic policy activation

Figure 5. Auto-policy generation algorithm

Step 2 – Auto-threat analysis

For each of the application zones, it analyzes which threats are relevant based on the OWASP Top 10 application vulnerabilities list of threat categories and another 150 attack vectors already programmed into the algorithm.

Step 3 – Policy generation with auto-optimization

Based on the aforementioned threat analysis, the algorithm will generate an optimized security policy with both negative and positive sets of rules to provide comprehensive protection while minimizing false positives.

Step 4 – Auto-policy activation

Once the security policy is generated, the algorithm will apply the security policy to start and protect the application. This is when manual fine-tuning of the security policy can take place to further minimize false positives and false negatives. This tuning can also be done by the Radware Emergency Response Team[2] (ERT) for customers that purchase the ERT premium managed service.

How Auto-Policy Impacts the Quality of Protection

Another important value of the auto-policy generation is quality of protection.

The fact that different levels of protection can be automatically learned and optimized by the auto-policy generation system allows enabling ALL RULES and activates various security filters. With this capability, the rules and filters are being optimized and updated automatically, thereby removing the risk of generating false positives.

If we take a simple example of the Always-True Expression type of SQL Injection such as “OR 1 = 1,” we can easily understand that rules that are aimed to block such inputs will have a high tendency to generate false positives. If there is no automatic mechanism to create such policy exceptions, it will not be reasonable to define such rules that may block legitimate traffic. Many cloud WAF vendors do not define such risky rules.

Cisco’s auto-policy generation technology allows all rules to be enabled while automatically creating the exceptions for areas where these rules generate false positives while properly securing the rest of the application. All HTTP RFC rules are enabled, and all injections rules are applied and being optimized automatically. This alone offers a dramatically higher quality of protection even if a positive security model is not involved.

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, semi-supervised 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 non-intrusive, 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.

[2] Provided through Cisco’s OEM partnership with Radware.

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

Full coverage of OWASP automated threats
Protection from all forms of account takeover, denial of inventory,distributed denial of service (DDoS), card fraud, and web scraping

Secure all channels: web, mobile, and APIs
Proects against bots that target digital assets, including sophisticated bots designed to attack multiple targets

Flexible integration options
Non-intrusive 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

Figure 6. Comprehensive bot protection

Detection and Mitigation with High Accuracy

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 builds upon Radware's bot management research findings in semi-supervised machine learning and leverages the latest developments in deep learning.

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 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.

Easy Integration

Flexible deployment options include integration through our JS tag, cloud connectors, or web server plug-ins. Alternatively, a virtual appliance is also available for the entire web app or selected sections. Using an API-based approach, Domain Name System (DNS) redirection is not mandatory, so deployment into the existing application stack is easy and seamless.

Designing a Secured API Environment

While APIs bring tremendous benefits, they also introduce new security risks, including service disruption and data theft. Many APIs process sensitive personally identifiable information (PII). Additionally, known application security risks with HTTP/S apps are as relevant for APIs as they are for web applications. Communication with APIs usually follows known structures and protocols. The most common protocol is REST-JSON, which has a schema format definition called OpenAPI.

Because threats vary, API security requires a combination of access controls (such as authentication and authorization mechanisms), injection prevention, bot management, and DoS mitigation. In addition, hackers may try certain API-specific attacks such as using invalid schemas, parameter tampering, or token manipulations.

This is why providing comprehensive protection against API-related attacks and a combination of several technologies are required, such as application and API vulnerability protection, bot protection, and behavioral analysis, all with positive and negative security models.

Attack category	Example of attacks / risks	Protection technology
API1:2019 Broken Object Level Authorization	• Unauthorized Access to APIs: IP / Token / Role / Customer Based	**WAF:** - Quota - API catalog
API2:2019 Broken User Authentication	• Authentication: OAuth2, JSON Web Token • Session Hijacking (e.g., steal token) • Token manipulation (e.g., privilege esc.)	**WAF:** - Token Protection
API3:2019 Excessive Data Exposure	• Environment Fingerprinting: • 5XX Internal Server Errors • HTTP response headers	**WAF:** - Data Masking - Replace 500 messages
API4:2019 Lack of Resources and Rate Limiting	• ATO: Credential Cracking / Stuffing, … • Scraping / Data Harvesting • Denial of Inventory • Token Cracking: Coupons Enumeration	**WAF:** - Quota - Activity Tracking **BOT Management** with intent-based behavioral analysis
API5:2019 Broken Function Level Authorization	• Unauthorized Access to APIs IP / Token / Role / Customer Based • Access to restricted APIs	**WAF:** - API catalogue validation - IP and GEO policies
API6:2019 Mass Assignment	• Unauthorized Access to APIs • Access to restricted APIs	**WAF:** - API catalog validation - IP and GEO policies
API7:2019 Security Misconfiguration	• Incomplete or ad-hoc configurations • Misconfigured HTTP headers • Unnecessary HTTP methods	**WAF**: - Data Masking - Replace 500 messages - Auto-learning
API8:2019 Injection	• SQL Injections • XSS • Command Injection • Directory Traversal	**WAF:** - Positive Security model - Negative Security model - API catalog validation
API9:2019 Improper Assets Management	• Overexposed API end points	**WAF:** - Positive Security model - Negative Security model - Auto-learning
DoS, Availability	• Volumetric Application DDoS on APIs • Low and Slow Attacks (TCP \ HTTP)	**WAF:** - TCP low and slow detection - Behavioral low and slow detection **BOT Management**

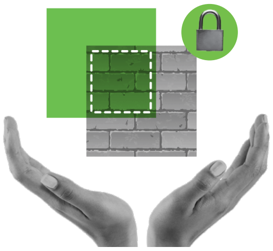
Cisco's API Protection Solution

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.

Managed Application Protection

Cisco customers have the option of purchasing a fully managed WAF and bot protection service through Cisco's global OEM partnership with Radware. Radware's emergency response team (ERT) is comprised of security experts available 24x7x365 who provide proactive security support services for customers facing an array of application- and network-layer attacks. Powered by Radware's Threat Research Center, ERT



engineers combat attacks and provide customers with industry-leading expertise and intelligence, enabling customers to benefit from industry-leading application security even if the customer lacks in-house application protection expertise.

- Radware's ERT managed service assumes full responsibility to configure and update security policies as well as actively monitor, detect, alert, and mitigate attacks in real time.
- Fastest attack mitigation – The ERT maintains a 10-minute SLA to provide organizations under attack with access to battle-proven security experts.
- Preemptive attack Intelligence allows access to threat alerts, advisories, and attack reports provided by Radware's Threat Research Center.
- Consulting and reporting features provide a monthly analysis of cyberattacks against your organization and others to identify attack trends, how your organization's network can be impacted, and defense recommendations.
- Technical account management includes a dedicated and proactive consultant who serves as a focal point for configuration, tuning, integration upgrades, and attack mitigation.

Overview of Cisco Application Protection Capabilities

The table below highlights some of the key features necessary for effective WAF and DDoS protection and analyzes Cisco's WAF and Cloud WAF Service offerings.

Feature	Description	Cisco's Advantage and Benefits
Positive security model	A positive security model is one that defines what is allowed and rejects everything else. This should be contrasted with a negative security model, which defines what is disallowed while implicitly allowing everything else.	Secure WAF technology automatically learns the web application structure and appropriate requests or responses using a combination of auto-policy generation and security filters. This allows Cisco to maintain an effective positive security model that can help block well-known and zero-day attacks. With regards to API traffic, WAF technologies define the allowed actions while blocking all access attempts to nonlisted API end points or paths. API catalogs, definition of headers, path parameters, and query parameters with a strong schema validation are all great examples of a positive security model. The value of such an approach is a tighter, more-effective security policy, including the ability to define a positive security model immediately without any learning process to effectively secure the APIs.
Machine learning-based auto-policy generation	Leveraging machine learning algorithms, auto-policy generation helps automatically generate a security policy tailored to the specific application. The auto-policy helps create a positive security model for the application and configure the negative security policy while automatically correcting false positives.	Secure WAF automatically maps the application structure, performs threat analysis process, auto-generates a tailored policy for the secured app, and automatically updates policy with application changes. With regard to the API traffic and for the undocumented approach, Secure WAFs propose the API Discovery module to automatically learn the API traffic and create the rule based on a positive security approach.

Feature	Description	Cisco's Advantage and Benefits
Cross-site request forgery (CSRF)	CSRF is a type of malicious website exploit where unauthorized commands are transmitted from a user that the website trusts. Unlike cross-site scripting (XSS), which exploits the trust a user has for a particular site, CSRF exploits the trust that a site has in a user's browser.	Cisco offers CSRF protection based on a reference header validation. This mechanism allows robust CSRF protection by blocking requests if they are not coming from the trusted referrer.
Server-side request forgery (SSRF)	SSRF is a web security vulnerability that allows an attacker to induce the server-side application to make HTTP requests to an arbitrary domain of the attacker. The attacker might cause the server to make a connection to internal-only services where they may be able to force the server to connect to arbitrary external systems, potentially leaking sensitive data such as authorization credentials.	Cisco host protection protects SSRF by avoiding unvalidated redirect with support of such attacks into different locations of the attack payload, including XML format.
Tailored granular policies for custom applications and protection from session or cookie hijacking	Effectively protecting custom applications requires granularity in application mapping and policy development. The lack of granular policies limits the tailoring of policies for particular parts of the applications and means the entire application needs to be scanned for new policies based on changes to the application. Session hijacking involves the exploitation of a valid computer session to gain unauthorized access to information or services in a computer system.	Cisco offers granular application mapping down to the folder or file level. This enables more tailored protection for different parts of the application and speeds up the time to protection following changes to the application. The configuration can also be delivered using the management API for CI/CD integration. Cisco provides session and cookie hijacking protection by validating that users do not modify cookies and that those user-sensitive cookies, such as session cookies, are not being sent by different devices.
Mitigation platform stability	The ability of a cloud-based DDoS provider to deliver service is only as reliable as the availability of its mitigation platform. Outages of these platforms result in performance impacts or event unavailability of customers' websites.	Cisco's OEM partner Radware maintains a separate infrastructure for handling large volumetric DDoS attacks. This eliminates the impact on legitimate traffic running through Radware's cloud services when there is an attack. Additionally, Radware has maintained its cloud DDoS mitigation platform without an outage since its inception in 2013.
Data leak prevention (DLP) for sensitive data	DLP features protect against the loss of sensitive data through application attacks that exploit vulnerabilities to force applications to reply to malicious requests with sensitive data (for example, CCNs).	Cisco offers DLP features that mask or block sensitive information in application replies including CCN, SSN, and server error messages. Policies for specific data can be applied globally to the application or on specific folders.
Device fingerprinting	Advanced security systems are using device fingerprints as a more accurate means of attacking traffic sourcing or malicious behavior tracking. IP address-based bot or attack detection has become insufficient due to the various ways that IP addresses can be masked (for example, through anonymous proxies or global NATs) or spoofed.	Secure WAF offers a web client fingerprint being generated on every new session to allow IP-agnostic attack source detection and mitigation. This delivers unique protection from continuous attack vectors such as web scraping, brute-force attacks on login pages, and advanced availability threats such as HTTP Dynamic Floods and low and slow, where the correlation across multiple sessions is essential for proper detection and mitigation.?

Beyond all the required protections discussed above, including SQL injection, broken authentication, XSS, CSRF, DDoS, and more, Cisco's web application security technology features additional attack correlation capabilities. These capabilities allow blocking of repetitive attack sources by managing a penalty score for security violations per source. Once an attack source reaches a predefined score threshold, it will be blocked.

Cisco Secure WAF performance per Alteon[3] platform series

	Alteon D - 4208	Alteon D - 5208	Alteon D - 5820	Alteon D - 6024	Alteon D - 7612	Alteon D - 8420
BW (Mbps) up to	2000	4000	5000	7500	15,000	12,000
CPS up to	6300	20,000	15,000	45,000	70,000	64,000
RPS up to	14,300	41,000	34,000	60,000	130,000	92,000

[3] Alteon is a registered trademark of Radware, Inc.

This paper is published by Cisco based on content originally authored by Radware, Inc.

For More Information

CCisco offers the industry's most comprehensive solutions for application and API security, bot management, network protection, and application delivery control.

Speak with your Cisco representative to learn how Cisco can help ensure the resilience, availability and security of your digital organization.

For information about Cisco application security solutions, go to: www.cisco.com/go/security