Web App Protector

More Than Just a Web Application Firewall

Add Value to your Business

Best Security Coverage

- Attack mitigation with no performance impact or risk
- Secure availability of web applications
- Audit ready and visibility into application security
- Data loss prevention

Fast to Deploy

- Fast, reliable, and secure delivery of mission-critical web applications

Allows Secured, Continuous Web Application Delivery

- Integrated with DAST solutions for real time web security patching

Easy to Maintain

- Low maintenance costs and post deployment peace of mind
- Improved risk management

As cyber-attacks and mitigation techniques continue to evolve, enterprises need to be on alert and keep time to protection as short as possible.

Enterprises are migrating business-critical functions to web applications in an effort to increase productivity, improve business agility and reduce costs. While the migration to web applications provides economic advantages and enables increased business agility, it also creates new security risks and compliance requirements that need to be addressed. The complexity of attacks and the speed in which new mitigation tools and techniques are being bypassed require a more robust and comprehensive solution that provides faster protection and reduced maintenance costs.

By targeting the application layer, attackers exhaust server and application resources using stealth attack techniques that go undetected by traditional security tools. It is no longer just about http floods and downtime. Advanced methods and the use of multiple vectors during attacks present new challenges in securing an organization.

ADVANCED WEB APPLICATION SECURITY

Web App Protector, Check Point's Web Application Firewall (WAF), ensures fast, reliable and secure delivery of mission-critical Web applications. Web App Protector is an ICSA Labs certified and PCI compliant WAF that provides complete protection against web application attacks, web application attacks behind CDNs, advanced HTTP attacks (slowloris, dynamic floods), brute force attacks on login pages and more.

Web App Protector is the only web application firewall that provides complete web application security. It blocks attacks at the perimeter and ensures fast, reliable and secure delivery of mission-critical web applications. It is the best performing application security solution for web security, mitigation and compliance.

Comprehensive and Accurate Security Coverage

Web App Protector delivers comprehensive and accurate security coverage of known and unknown web application threats. It provides full security coverage out-of-the-box of OWASP Top 10 threats, including injections, cross-site scripting (XSS), cross-site request forgery (CSRF), broken authentication, leakage of sensitive information and session management. It offers security coverage for additional attacks and threats beyond the OWASP Top-10 list such as Web Application Security Consortium (WASC) threats. Web App Protector terminates TCP connections and normalizes client encoded traffic to block various evasion techniques and guarantees that out of the box negative security is much more efficient, accurate and difficult to evade.

Automated Protection from Zero-Day Web Attacks

The best security coverage with minimal impact on legitimate traffic is made possible by Check Point'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 allow granular and accurate policy definitions, therefore avoiding false positives and false negatives.

By using both negative and positive security models - Web App Protector features not only the lowest false positives and minimal operational effort, but also robust protection against known and unknown (Zero-day) threats.

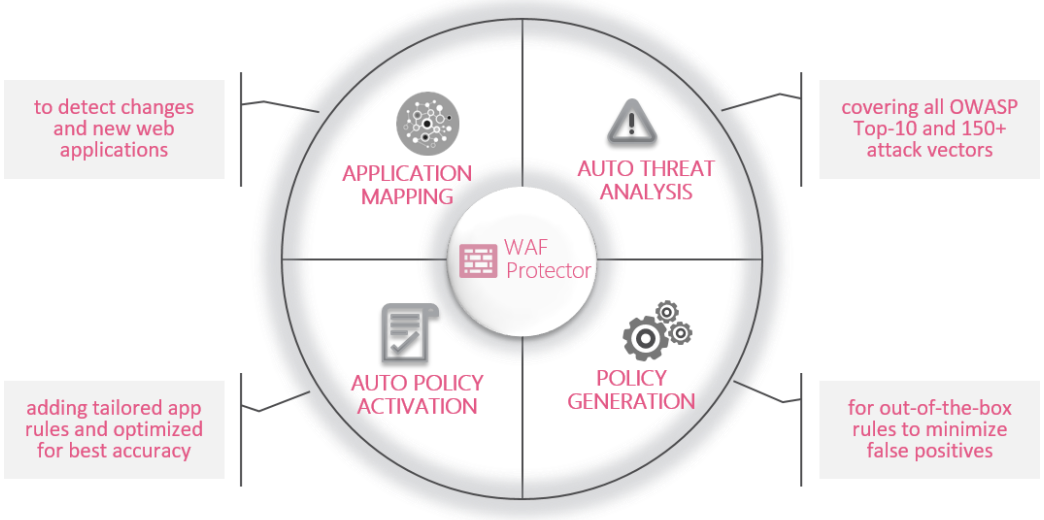
Leveraging Machine-Learning Algorithms for Auto Policy Generation

Web App Protector incorporates machine-learning algorithms to keep Web assets protected always, even while applications constantly change and threats rapidly evolve, assuring web security is future proof. Web App Protector's unique Auto Policy Generation mechanism provides the best tool for automatically generating security policy to secure Web applications.

The Auto Policy Generation module will automatically use the required security filter, create security filter rules and switch the security filters into active mode. These operations would normally require many manual refinements.

By leveraging machine-learning algorithms, Auto Policy Generation is designed to secure a web application as automatically as possible with little or limited user interaction and offers the following benefits:

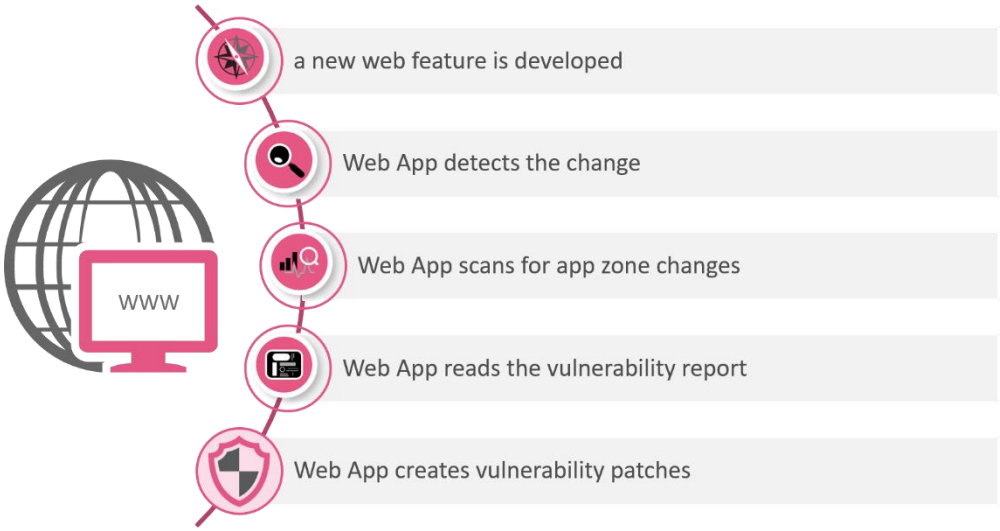
- Shortest time to protection, requiring only one week for known attacks – 50% faster than other leading WAFs
- Best security coverage by performing auto threat analysis, with no admin intervention – covering over 150 attack vectors
- Lowest false-positives achieved through auto-optimization of out-of-the-box rules – close to zero false positives
- Automatic detection of web application changes assuring security throughout the application's development lifecycle – post deployment peace of mind



Continuous Security Delivery

Web App Protector is the first WAF to provide a real-time security patching solution for Web applications in continuous application deployment environments. This is accomplished via tight integration with Dynamic Application Security Testing (DAST) solutions.

As Web applications are continuously introducing new features and resources, Check Point's Web App Protector automatically detects any changes in the Web applications (1) in real time and invokes (2) DAST tool to explicitly scan (3) the specific application zones that have been changed. This scan is accomplished in minutes versus a complete web application scan that can take hours. Web App Protector then reads (4) the DAST vulnerability report, and uses it to automatically update the application security policy (5) by creating the applicable virtual patches. Following that, a second vulnerability scan is invoked to test whether the application security was indeed successfully patched.



IP-agnostic Device Fingerprinting for Bot Protection

Web App Protector's Device Fingerprinting and Activity Tracking modules offer IP-agnostic source tracking to help address the threats posed by advanced bots, such as web scraping, Web application DDoS, brute force attacks for password cracking and clickjacking. Web App Protector can detect sources operating in a dynamic IP environment and activity behind a source NAT, such as an enterprise network or proxy. Even if the bot dynamically changes its source IP address, its device fingerprint does not change. Web App Protector tracks the device activity and correlates the source security violations across different sessions over time.

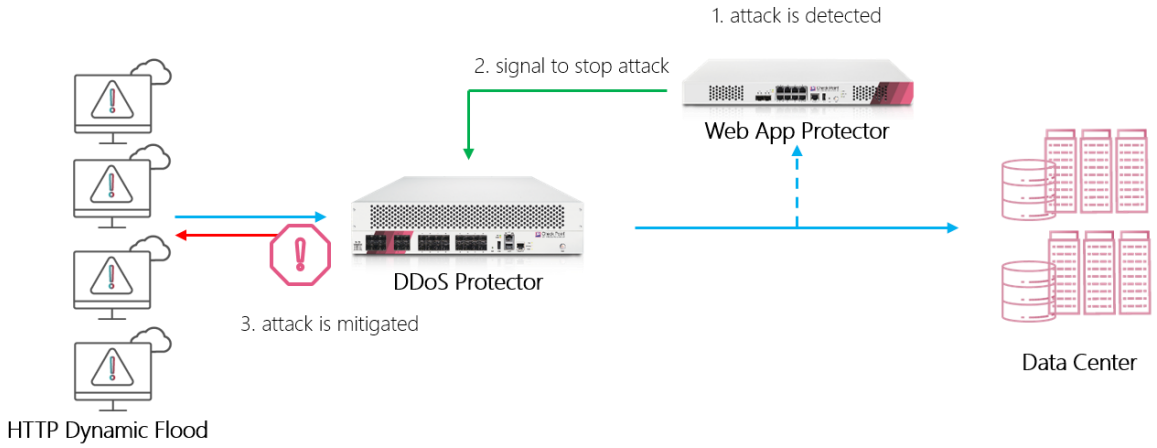
Unique Out-of-Path Deployment with Full, Line-Speed Mitigation

Web App Protector is the only WAF that can be deployed out-of-path while still providing full mitigation. As part of Check Point's integrated Attack Mitigation Solution, a unique defense messaging mechanism enables Web App Protector to signal Check Point's perimeter attack mitigation device, DDoS Protector, when a web application attack is detected, block it at the perimeter and protect the rest of the network.

Once Web App Protector detects a web-based attack, it automatically sends a message to DDoS Protector which is deployed at the perimeter to mitigate and block attacks in real-time.

This unique defense messaging mechanism can be leveraged when Web App Protector is deployed inline as well as out-of-path to assure line speed web based attack mitigation with no additional latency, performance impact or risk. This includes:

- Mitigating at line speed– up to 400 Gbps, 330M DDoS PPS at 60 micro-seconds latency.
- Mitigating cyber-attacks targeting web applications behind CDNs.
- Blocking advanced HTTP DDoS attacks (Slowloris, Http Dynamic Floods), Brute Force attacks on login pages and SSL based attacks.
- Blocking the attack source at the perimeter, before it enters the organizations' network, securing other applications and services.
- Enabling multi-layered detection and mitigation



All-in-One Application Delivery and Security

When Web App Protector is deployed as part of Check Point's Application Delivery Controller the solution provides a comprehensive set of availability, acceleration, and security services designed to ensure fast, reliable, and secure delivery of mission- critical web applications. Resources of Web App Protector instances can be dynamically allocated according to enterprise needs and deliver fault isolation, SLA assurance and high platform density. The solution supports both out-of-path and inline deployment modes and can be delivered on a variety of platforms that support up to 80 Gbps.

Fully Managed Web Application Protection

Understanding the challenges organizations face in managing and maintaining web application security solutions, Check Point offers solutions that are fully managed by security experts. In addition to Check Point's fully-managed Cloud Web App Protector Service, Check Point's Web App Protector customers can also get the managed service provided by Emergency Response Team (ERT) security experts that includes the ongoing management, monitoring and configuration of the on premise WAF device.

Authentication Gateway

Web App Protector's user authentication and single sign-on offering functions as an authentication tier in front of the web applications. It applies two factor authentication, authorizes and enforces. Web Access Control policy, and enables access to premise-based applications from outside the enterprise network. Various authentication schemes are supported among of which are the FBA (Form Based Authentication), NTLM, and KCD (Kerberos Constrained Delegation).

Multi-Vector Role Based Security Policy

By leveraging Web App Protector's authentication and SSO, application or organizational web role (employees, partners, customers etc.), and security policies (such as application access, data visibility and web security) can enforce segregation of duties that ensure access to data is based on business needs.

Compliance

Web App Protector enables organizations to fully comply with PCI DSS section 6.6 requirements and includes the most advanced security graphical reports to convey visibility into the application security and detected attacks. Its detailed PCI compliance report analyzes the security policies, provides automatic compliance status and a mandatory action plan for compliance.

CLOUD WEB APP PROTECTOR CLOUD SERVICES

The Check Point Cloud Web App Protector Cloud Service provides the same feature set available in our on premises Web App appliances. This is the industry's best web application security that uses a positive security model based on machine-learning technologies to provide comprehensive protection coverage against OWASP Top 10 threats and other vulnerabilities. You also get dynamic security policies with automatic false-positive correction, built-in DDoS protection, integrated bot mitigation and many other features to help protect organizations against the risk of data loss.

HOW CHECK POINT KEEPS YOU AGILE AND SECURE

Automatic Traffic Learning

Check Point uses advanced machine-learning algorithms that to analyze and learn what constitutes legitimate behavior and automatically block malicious traffic

Application Mapping

Check Point automatically maps protected applications, detects code changes whenever new features are added or modified, and identifies potential vulnerabilities

Continuously Adaptive Policies

Check Point continuously adapts security policies to optimize coverage to the application's threat profile in order to maximize security coverage and reduce false positives

THE ONLY CLOUD WAF FOR FULL PCI COMPLIANCE

Check Point Web App Protector Cloud Service is the only cloud WAF service which fully implements all 10 recommended security mechanisms of PCI DSS Requirement 6.6, including Enforcing a Positive Security Model and implementing Data Leakage Prevention (DLP) controls. Check Point's cloud WAF service is also PCI DSS v3.2 certified and based on NSS Labs and ICSA certified technology, meaning customers can deploy Check Point's Web App Protector Cloud Service with full confidence and attain maximal compliance.

PCI DSS COMPLIANT

Global Presence, Right Next to Your Origin Server

Check Point's Web App Protector Cloud Service is based on a global network of distributed WAF Points of Presence (PoPs), making sure that you are always protected from the closest point to your origin server. Check Point's Web App Protector Cloud PoPs are located at major traffic hubs with connections to Tier 1 ISPs, ensuring low latency and minimal impact on web application performance.

EASY MANAGEMENT AND CONTROL

Vision is a unified management and monitoring system that provides a rich centralized dashboard to display threats and manage your configuration. Granular alerting capabilities include 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 provide situational control. Centrally manage Web App and DDoS Protector and get reporting for both.

THE PREMIUM SUPPORT SERVICE ADVANTAGE

Want a higher priority response to service issues? Our Premium cloud WAF service may be the choice for you. The standard WAF service best effort. With our Premium Managed WAF Cloud Service you get pre-attack alerts, post-attack reports and recommendations, two Forensics Reports per year, a Technical Account Manager (TAM), and a dedicated Emergency Response Team (ERT) expert. Your cases get priority with a 10 minute wait time to a Security Expert, direct "Hot-line" access, weekly calls during Onboarding stage and a yearly Proactive Security Policy Review to optimize your security policy.

ORDERING WEB APP PROTECTOR

PROTECTOR SECURITY APPLIANCES [1]	SKU
Protector AL5208 Security Appliance	CPAP-AL5208-S
Protector AL5208 Security Appliance with a DC power supply	CPAP-AL5208-D-S
Protector AL6024 Security Appliance	CPAP-AL6024
Protector AL6024 Security Appliance with a DC power supply	CPAP-AL6024-D
Protector AL6024 Security Appliance	CPAP-AL6420-S
Protector AL6024 Security Appliance with a DC power supply	CPAP-AL6420-D-S
Protector AL8420 Security Appliance with a DC power supply	CPAP-AL8420-D-S
Software Upgrades	
SSL Protector AL6024S - Upgrade S to SL SSL Acceleration	CPSB-AL6024S-UPG-SL
SSL Protector AL8240 S - Upgrade S to SL SSL Acceleration	CPSB-AL8420-S-UPG-SL
SSL Inspection and WAF Upgrades	
License upgrade For Protector AL5208 to include WAF and SSL Inspection	CPSB-AL5208-WAF-SSL
License upgrade For Protector AL6024 to include WAF and SSL Inspection	CPSB-AL6024-WAF-SSL
License upgrade For Protector AL6420 to include WAF and SSL Inspection	CPSB-AL6420-WAF-SSL
License upgrade For Protector AL8420 to include WAF and SSL Inspection	CPSB-AL8420-WAF-SSL
Hardware Accesories	
SSL Protector AL6024 - Upgrade to S SSL Acceleration - Factory installed	CPAC-AL6024-UPG-S
SSL Protector AL6024 Memory Upgrade to 64 GB - Factory installed	CPAC-AL6024-UPG-64G
SSL Protector AL6420 Memory Upgrade to 64 GB - Factory installed	CPAC-AL6420-UPG-32G-TO-64G
Single AC Power Supply - SSL Protector AL5208	CPAC-PSU-AC-AL5208
Single AC Power Supply - SSL Protector AL6024	CPAC-PSU-AC-AL6024

[1] GBICs must be purchased separately

Web App Protector Cloud Services

PREMIUM CLOUD WAF SERVICE	SKU
Web App Protector Enterprise Premium Service up to 5 or 1 Gbps or 500, 100, 50, or 10 Mbps and 1 Application for 1 year	CP-CG-WAF-PREM-xxBPS-1-MS-1Y
Web App Protector Enterprise Premium 1 Gbps or 500, 200, 100, 50, or 10 Mbps Traffic Add-On for 1 year	CP-CG-WAF-PREM-xxBPS-ADD-1Y
ENTERPRISE CLOUD WAF SERVICE	
Web App Protector Enterprise Service up to 5 or 1 Gbps or 500, 100, 50 or 10 Mbps and 1 Application for 1 year	CP-CG-WAF-xxBPS-1-MS-1Y
Web App Protector Enterprise 1 Gbps or 500, 200, 100, 50, or 10 Mbps Traffic Add-On for 1 year	CP-CG-WAF-xxBPS-ADD-1Y
High Capacity Add-on	
High-capacity SSL protection add-on up to 240,000 sessions per second and 12,000,000 concurrent sessions for 1 year	CP-CG-WAF-SSL-ADD-240K-12M-1Y
High-capacity SSL protection add-on up to 100,000 sessions per second and 5,000,000 concurrent sessions for 1 year	CP-CG-WAF-SSL-ADD-100K-5M-1Y
High-capacity SSL protection add-on up to 60,000 sessions per second and 3,000,000 concurrent sessions for 1 year	CP-CG-WAF-SSL-ADD-60K-3M-1Y
High-capacity SSL protection add-on up to 20,000 sessions per second and 1,000,000 concurrent sessions for 1 year	CP-CG-WAF-SSL-ADD-20K-1M-1Y
Additional Services	
Volumetric Cloud DDoS Protection Add-on for Web App Protector Unlimited DDoS Traffic for 1 year	CP-CG-WAF-DP-ADD-UL-1Y
Volumetric Cloud DDoS Protection Add-on for Web App Protector Up to 10Gbps Attack Traffic for 1 year	CP-CG-WAF-DP-ADD-10GBPS-1Y
Web App Protector Unlimited Applications Add-On for 1 year	CP-CG-WAF-UL-ADD-1Y
Web App Protector 100, 50, 20, 10, 5, or 1 Application(s) Add-On for 1 year	CP-CG-WAF-xx-ADD-1Y

CONTACT US
Worldwide Headquarters | 5 Shlomo Kaplan Street, 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 | Fax: 650-628-2117 | www.checkpoint.com