

CHECK POINT PROTECTOR

A WINNING CYBER SECURITY SOLUTION



Solution Benefits

Protect Installed Base by Blocking Competition

Secure Check Point existing accounts by providing a complete end-to-end solution to prevent competitors from initiating with those accounts and reduce customer churn.

Differentiate and Win New Logos against Competition

Win with a broader, more complete solution set that satisfies an array of security use cases.

Protect Check Point Cloud Customers and Expand Offering

Help Check Point protect their cloud customers and expand Check Point's cloud offering with DDoS, WAF and bot protection solutions from a single source.

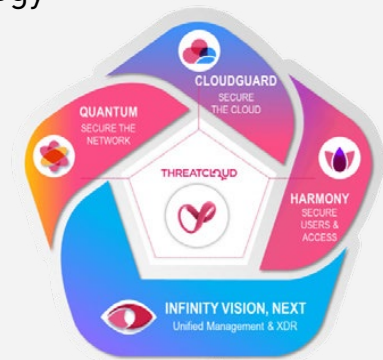
Sell New Products and Significantly Grow Pipeline

Establish Check Point as a superior, comprehensive solution and bolster existing customer opportunities while attracting new customers.

End-to-End Solution Strategy

Check Point Protector Series

- ✓ DDoS Protection
- ✓ SSL Inspection
- ✓ Web Application Firewall
- ✓ Bot Manager Protection
- ✓ ADC



DDOS PROTECTOR: ON-PREMISES AND CLOUD DDOS

An award-winning, automated, real-time mitigation solution that secures organizations against emerging network and applications threats while protecting infrastructure against network and application downtime, application vulnerability exploitation, malware spread, anomalies, information theft and more.

- Faster more accurate behavioral-based DDoS protection
- Rate-invariant behavioral analysis for lower false-positives under attack
- Machine learning real-time signature generation for zero-day attacks protection
- Full protection against emerging network threats
- Maintains network performance even when under high PPS network attacks
- On-premises, cloud-based and hybrid deployment options

APSOLUTE: UNIFIED PROTECTOR MANAGEMENT

Deploying and managing global distributed application delivery and security services that span multiple devices and form factors can be complicated. Check Point APSolute Vision provides a highly available, single point of access for network and security administrators to centrally manage distributed Check Point DDoS, Web App and SSL Protector devices and monitor the health, real-time status, performance, and security of enterprise-wide application delivery infrastructures.

Built to Protect against Advanced, New Generation DDoS Attacks



CARPET BOMBING ATTACKS

Amplification & reflection attack protection



DNS ATTACKS

Automated behavioral DNS protection for authoritative & recursive DNS



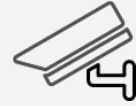
BURST ATTACKS

Behavioral-based burst attack protection



ENCRYPTED ATTACKS

Integrated 0-latency multi-layer SSL- flood protection



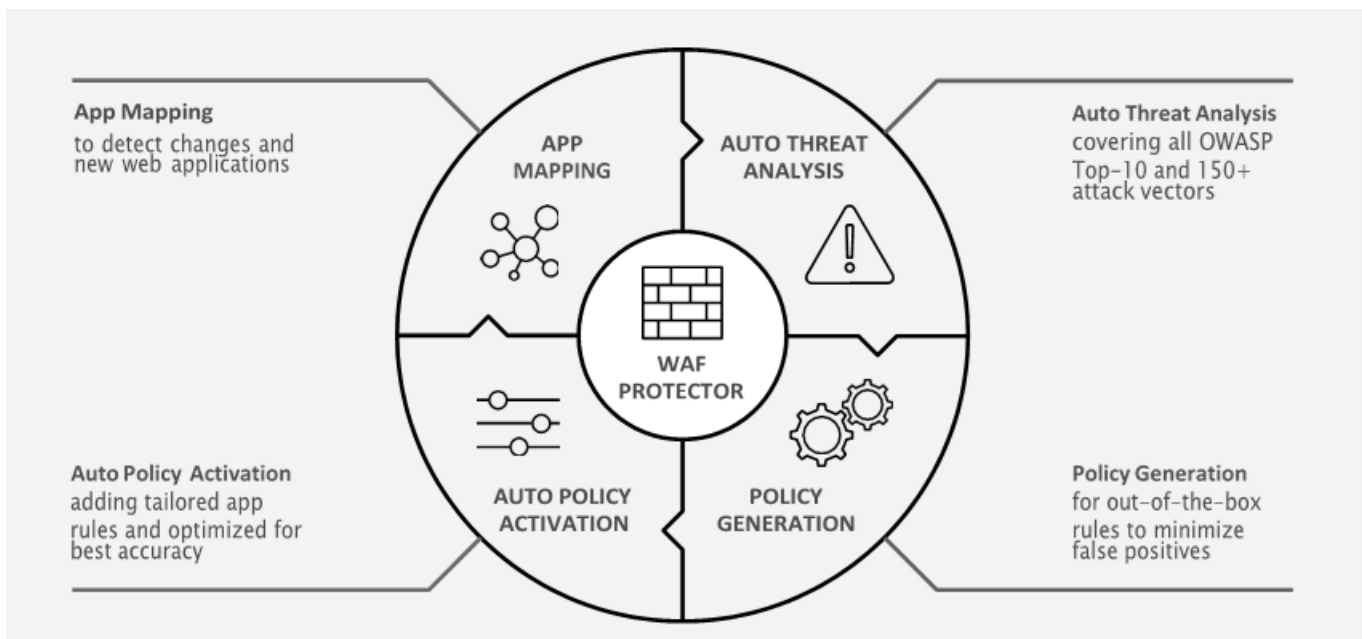
IoT BOTNETS

Real-time intelligence feed to block active attackers

WEB APP PROTECTOR: WAF, CLOUD WAF, API AND BOT PROTECTION

Enterprise-grade, continuously adaptive web application security protection through a web application firewall that provides full coverage of OWASP Top-10 threats for Web and API protection. Automatically adapts to evolving threats as well as a bot manager that provides protection from automated threats like bots by combining behavioral modeling for granular intent analysis, collective bot intelligence and fingerprinting of browsers, devices and machines.

- Automatic adaptive web application security with low false positives
- IP-agnostic fingerprinting for bot protection
- Learning application baseline for zero-day attacks protection
- Machine-learning for dynamic protection
- Flexible deployment modes
- Non-intrusive approach



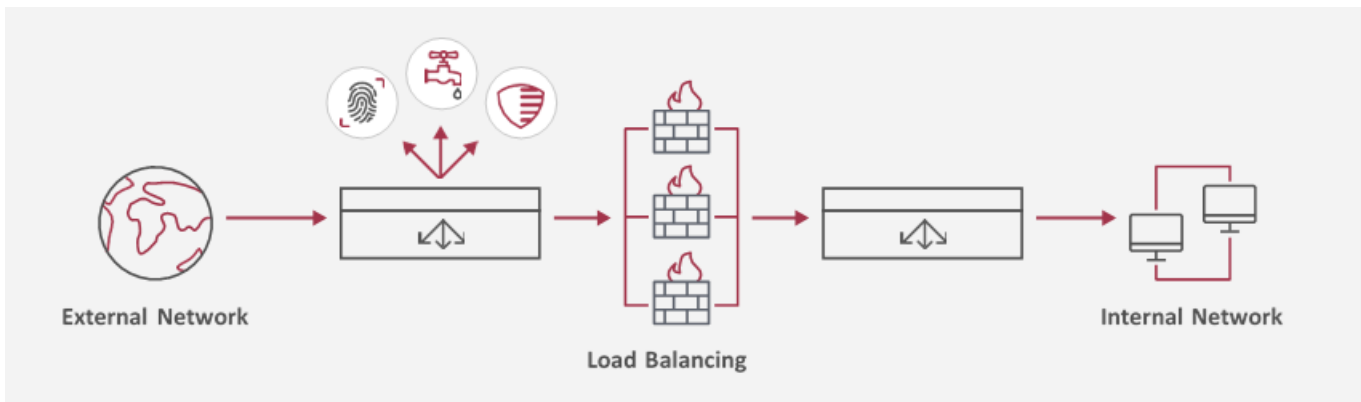
BOT PROTECTION

A comprehensive bot protection for websites, mobile apps, and APIs against OWASP automated threats including Account Takeover, API Abuse, Carding, Scraping, Ad Fraud, and Form Spam. With non-intrusive API-based approach, the bot manager detects and blocks highly sophisticated human-like bots in real-time. The detection engine also collects 250+ parameters like browsing patterns, mouse movements, keystrokes and URL traversal data points from the end user's browser to build a unique digital fingerprint of each visitor. Collective bot intelligence gathers bot signatures from our global client base to build a database of bot fingerprints and proactively stop bots from infiltrating your Internet properties. Additionally, the comprehensive analytics dashboard gives a granular classification of the different types of bots along with their sophistication levels. Protector Bot Protection provides unmatched API protection from automated threats for enterprises in a diverse range of industries including eCommerce, Media, EdTech, Real Estate, FinTech and Legal Services.

SSL PROTECTOR: DEEP SSL INSPECTION AND OFFLOADING

A simple one-box solution for high-performance visibility into enterprise SSL/TLS traffic, removing the blind spots introduced by the rising use of SSL/TLS and allows security tools to inspect all traffic for possible breaches and leaks.

- High-performance platforms
- Best price performance
- Single decryption/encryption point
- Full control over the inspected traffic flow while ensuring uninterrupted traffic
- Smooth scalability for security infrastructure



APPLICATION DELIVERY CONTROLLER (ADC) AND FIREWALL LOAD BALANCING

A next-generation, best-of-breed application delivery controller (ADC) and the only network load balancer that delivers proactive SLA management via on-going monitoring of real-user transactions, visibility via powerful reporting, and web optimization. It provides advanced, end-to-end local and global load balancing capabilities for all web, cloud, and mobile-based applications.

- One solution for any environment
- High level of flexibility to lower costs and simply management
- Single pane of glass for insightful analytics