CHECK POINT™

CloudGuard WAF

WAF as a Service Provides Fully Managed Application Security Within Minutes

A product becomes truly great when it can do the best job in the simplest way possible. Meet CloudGuard WAFaaS.

Our Most Powerful WAF to Date is Now Available as a Service

Ranging from AI-based threat detection, API discovery and bot prevention to file security and rate limiting, CloudGuard WAF as a Service, offers a complete suite of Application and API protection for multiple cloud and modern architecture.

Web application firewalls are challenging for security teams, Traditional WAFs rely heavily on signatures, rule creation and exception handling which make them too time consuming for security teams and too slow for cloud development.

CloudGuard WAFaaS is an entirely automated offering that provides the superior advantages of a high-quality Web Application Firewall with minimal manual input.

DEPLOY ONCE, WITHIN MINUTES

WAF as a Service (WAFaaS) delivers a non-agent Web application Firewall, deployable within minutes. Only a one-time DNS configuration is necessary for Cloud-Guard to start routing traffic securely to applications in the cloud.

PREVENT DDoS AND AUTOMATED ATTACKS

We utilize CDN delivery to guarantee continuous service. and defense against Denial of Service (DDoS) attacks and bot-driven assaults.

NO MORE AGENT DEPLOYMENTS

By routing your traffic through Check Point servers, CloudGuard's web application firewall will automatically be deployed in any cloud environment and will automatically provide and renew SSL certificates.

Ponemon INSTITUTE

According to the Ponemon Institute, an average company needs **2.5 full time** security administrators working **45 hours** per week on WAF alerts and an additional **16 hours** on rule creation, with costs over **$500,000** yearly.

**Any Cloud, Every Architecture**

One-time Agentless Deployment Within Minutes

In order to take ownership of your domain and start using of Check Point's WAF as a Service in a few simple steps, you'll need to add a CNAME record to your domain's DNS settings and point it to Check Point.

Begin Securing Your Traffic Immediately

The CNAME record must indicate a unique identifier provided by Check Point. Once this record is added, you will need to modify your DNS settings and direct them to Check Point's cloud.

This will ensure that when users type in your domain name, the DNS server will promptly search for and return the IP address of Check Point's cloud to their respective web browsers.

ADD A CNAME TO YOUR DNS
1

ROUTE YOUR DNS TO CHECK POINT CLOUD
2

YOU'RE ALL SET
3
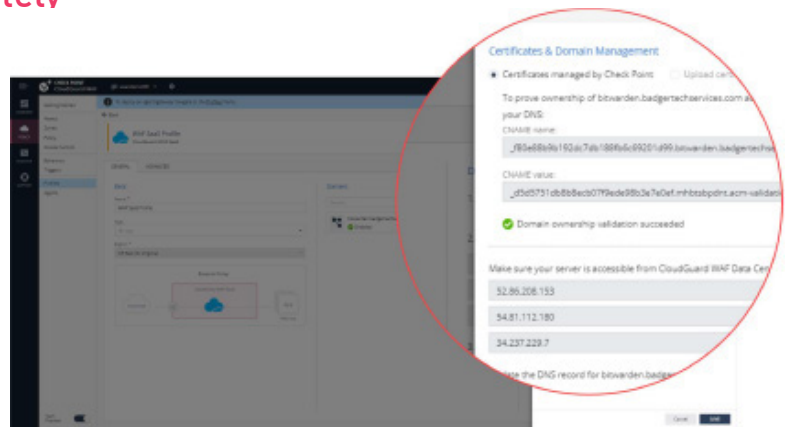
## How Cloud Distributed Networks Provide Greater Security

A Content Delivery Network (CDN) minimizes the physical distance between users and a website by storing cached content in multiple locations, known as points of presence (PoPs), which accelerates content delivery and provides continuous security availability.

CNDS ARE FASTER, SAFER AND SIMPLER
When a user requests content from a web application, the CDN redirects the request to the closest PoP. The cached content is then delivered, resulting in faster delivery and scalability.

CDNS PREVENT DENIAL OF SERVICE ATTACKS (DDoS)
By distributing content across various servers, CDNs safeguard websites against malicious attacks such as DDoS, ensuring higher traffic management and improved resilience to hardware failures.
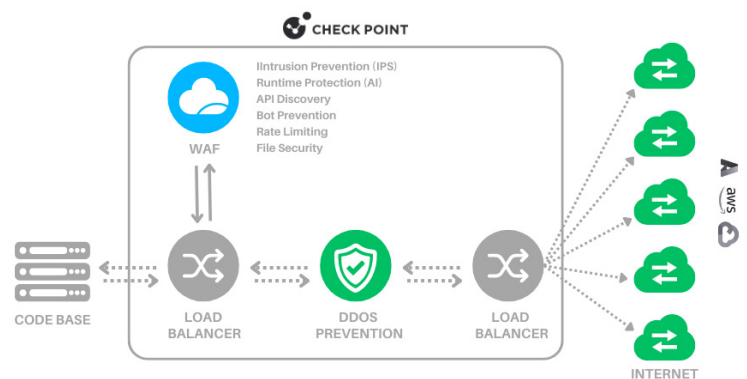
Did you know?

DDoS protection works by detecting and mitigating DDoS attacks in real-time. It involves a combination of techniques such as traffic filtering, rate limiting, and traffic redirection to protect the target resource from being overwhelmed by malicious requests.
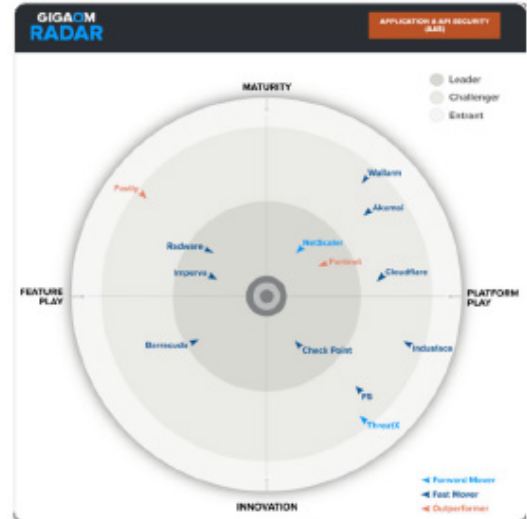
Available in AWS Marketplace

CHECK POINT™

Unified, Prevention-First Cloud Security Platform

CloudGuard CNAPP serves as a unified platform dedicated to securing your cloud environment. With it's prevention-forst approach, it allows for consistent and repeatable enforcement across cloud providers. We cover you from risks, regardless of theur origin, before they reach production and at runtime, known and unknown alike.