CHECK POINT
YOU DESERVE THE BEST SECURITY

CloudGuard AppSec

Application Self-Protection

Automated Web Application and API Protection (WAAP)

Features & Benefits

- **Precise Prevention** Contextual app analysis for high fidelity AppSec. Prevent known & unknown cyber attacks.
- **Automated by Design** Auto-deploy, hands-off management and AI powered short learning cycles
- **Flexible deployment** Protect all applications in any cloud environment built on any architecture

Capabilities

- Web Application Protection
- API Security
- Bot Prevention

Your Applications are Under Attack

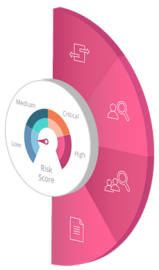
Your applications drive your business and as they evolve and grow, exposing more APIs, your attack surface grows too. Cyber criminals attack web applications and APIs using methods such as SQL injection and cross-site scripting, as well as automatic scripts, known as “bots”. These attacks are damaging and costly and the ability to secure applications has never been so critical.

Legacy Application Security Can't Keep Up

Legacy application security (web application firewalls, or WAFs) relies on threat signature mapping; 20 year old technology which takes a binary decision to either block or permit an application request. WAFs generate a high rate of false positives unless they're maintained with high administration overheads. Coupled with the speed at which applications are evolving, it's clear that legacy appsec can't keep up with DevOps speed and scale.

Applications Must Become Self-Protecting

CloudGuard AppSec represents a new paradigm in application security. Leveraging machine learning and a patent pending contextual AI engine, CloudGuard learns how an application is typically used, profiles the user and the appcontent and scores each request accordingly. This approach has proven to eliminate false positives while maintaining the highest standards of application security. With deployment to protection in a matter of hours, maintain application security with a solution that can keep up even with the fastest Devops teams.

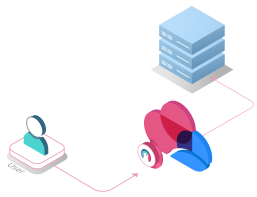


AppSec Powered by Contextual AI

With CloudGuard AppSec every incoming request is analyzed in context. The patent pending AI engine conducts a risk analysis by examining parameters like the user profile, the patterns seen in the user session, and how other users tyically interact with the application. Each request is given a score which will determine how likley it is that the request is malicious. The engine automatically adapts to application changes by continuously profiling the user, application and content.

CHECK POINT
YOU DESERVE THE BEST SECURITY

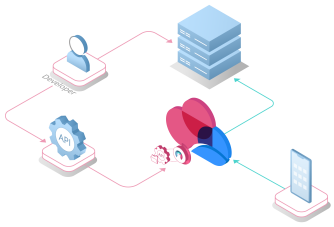
CloudGuard AppSec



Automated Web Application Firewall

Protect Your Applications As They Evolve

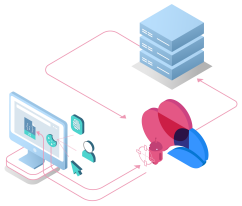
Powered by CloudGuard's contextual AI engine, CloudGuard AppSec stops attacks against applications including: site defacing, information leakage and user session hijacking. By analyzing each request in context and assigning a risk score, the solution provides precise prevention - eliminating false positives and preventing sophisticated attacks against your application, including OWASP Top 10 attacks.



API Protection

Stop Attacks Against YourAPIs

Applications are evolve fingster than ever and as they do, they create and expose more APIs. Ensure that your application's APIs are being used correctly, with CloudGuard AppSec's contextual AI engine, as well as automated validation using OpenAPI schema files. Stop cyber criminals from leveraging your APIs to expose sensitive data, inject commands or to extract API keys.



Bot Prevention

PreventAutomated Attacks

Protect your applications from sophisticated bots. CloudGuard uses JS injections to perform client-side behavioral analysis (including biometric activity like key strokes and mouse movements), in order to distinguish between human and non-human interactions with your application. Stop credential stuffing, brute force attacks and site scraping with advanced bot protection.

Supported Environments

Cloud
- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)
- Microsoft Azure
- VMware

Containers
- Docker
- Kubernetes
- Kubernetes Ingress
- OpenShift

CPUs
- X86 (64 bit)

Operating Systems
- CentOS
- Debian
- Red Hat Enterprise Linux
- Ubuntu

Protection Categories

- Cross Site Request Forgery
- XML External Entity
- Remote Code Execution
- Evasion Techniques
- LDAP Injection
- Path Traversal
- Vulnerability Scanning
- SQL Injection
- Illegal HTTP Methods
- Invalid input to forms and APIs
  Bot Scraping and Brute Force Attacks
- Over 2800 Web Specific CVEs