CHECK POINT

APPLICATION & API PROTECTION
GIGAOM RADAR REPORT
LEADER

CloudGuard AppSec

Preemptive Web Application & API Protection (WAAP)

CloudGuard
Secure the Cloud

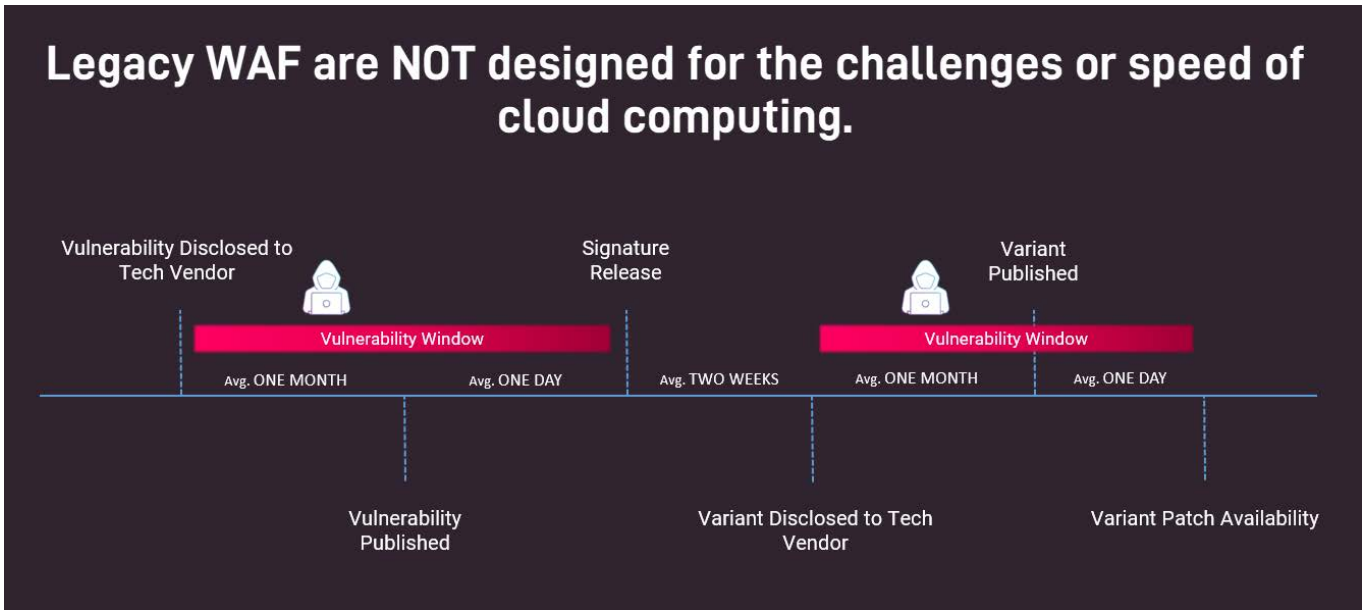
Don't Get Caught Off-Guard

As your cloud based web applications expand, so does your vulnerability to cyber threats. Attackers exploit your Web Applications and APIs using nefarious techniques like SQL injection, cross-site scripting and automated scripts a.k.a "bots." The fallout from such assaults can be highly detrimental and financially devastating, making application security an absolute priority for any business, big or small.

Traditional WAF Just Can't Cut It!

Web application firewalls (WAFs) have traditionally relied on threat signature mapping to reactively fend off attacks. This approach is both reactive (takes and avg of 1 month for initial rememdy) and is limited in its effectiveness because it can only make a binary decision: block or permit. This leads to a high number of false positives, causing headaches for security teams who must constantly monitor and maintain them.

With modern applications being developed and deployed at breakneck speed, it is becoming increasingly clear that this outdated approach is unable to keep up with the pace and scope of DevOps practices.



Eliminate Risks, Reduce Overheads, Accelerate Development

CloudGuard AppSec is the ultimate solution for organizations looking to mitigate risks and speed up development. This advanced cloud native platform streamlines Application security management and re-imagines threat prevention, effectively blocking known and unknown threats and significantly reducing operational overheads.

Real-time Premptive Protection

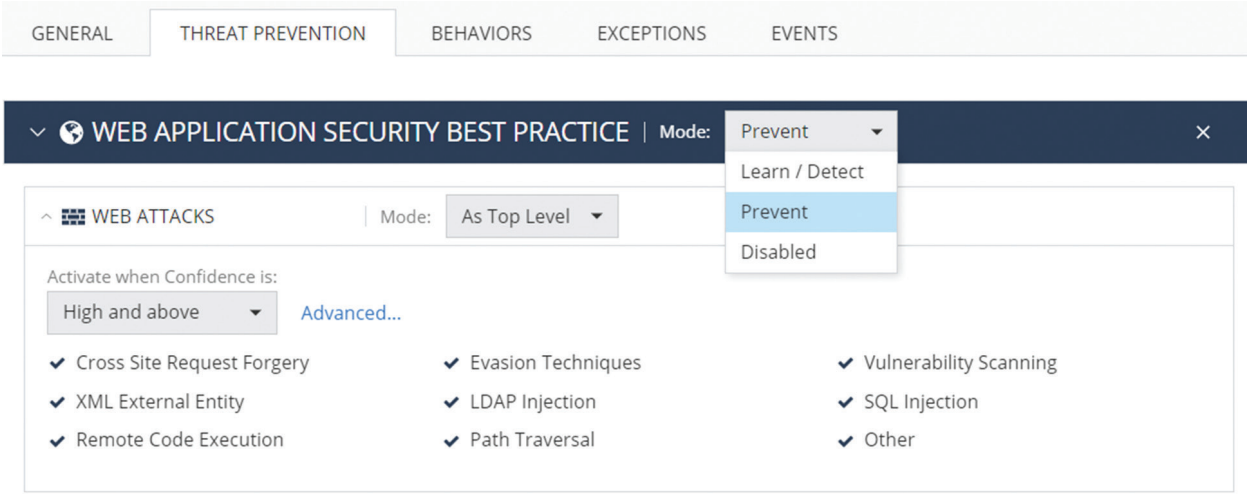
CloudGuard AppSec preemptively blocks attacks, based on patented contextual AI/ML. AppSec embeds security testing directly into the development pipeline, providing real-time protection. The result is enhanced security, accelerated time-to-market, and greater development efficiency, all achieved without compromising on quality or safety.

Precise Prevention

CloudGuard AppSec accurately eliminates false positives by examining various contextual parameters and determining a final risk score with input from multiple ML engines. Using multiple engine risk analysis provides more accurate decision-making eradicating manual tuning and enabling security admins to operate confidently in Prevent Mode without blocking legitimate requests.

Business Specific Protection

Web apps enter learning mode to gather environment-specific data and business cases, with multiple CPUs storing and synchronizing information hourly. The system identifies the source, HTTP method, HTTP requests, and every key/value pair, quickly completing its learning before users switch to prevent mode.

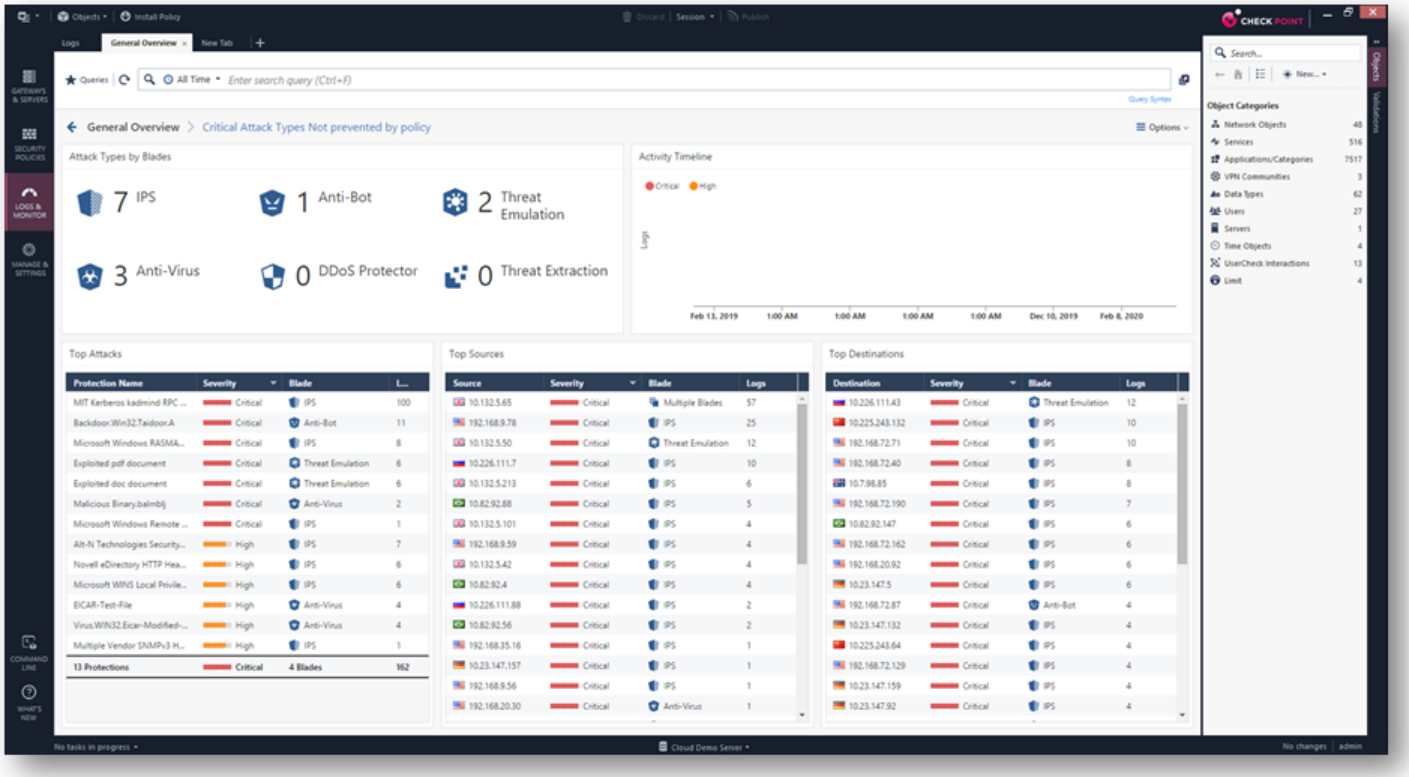


Open Schema API Protection

Applications are evolving faster 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.

Prevent Automated 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.



AUTOMATED WEB APPLICATION AND API PROTECTION (WAAP)

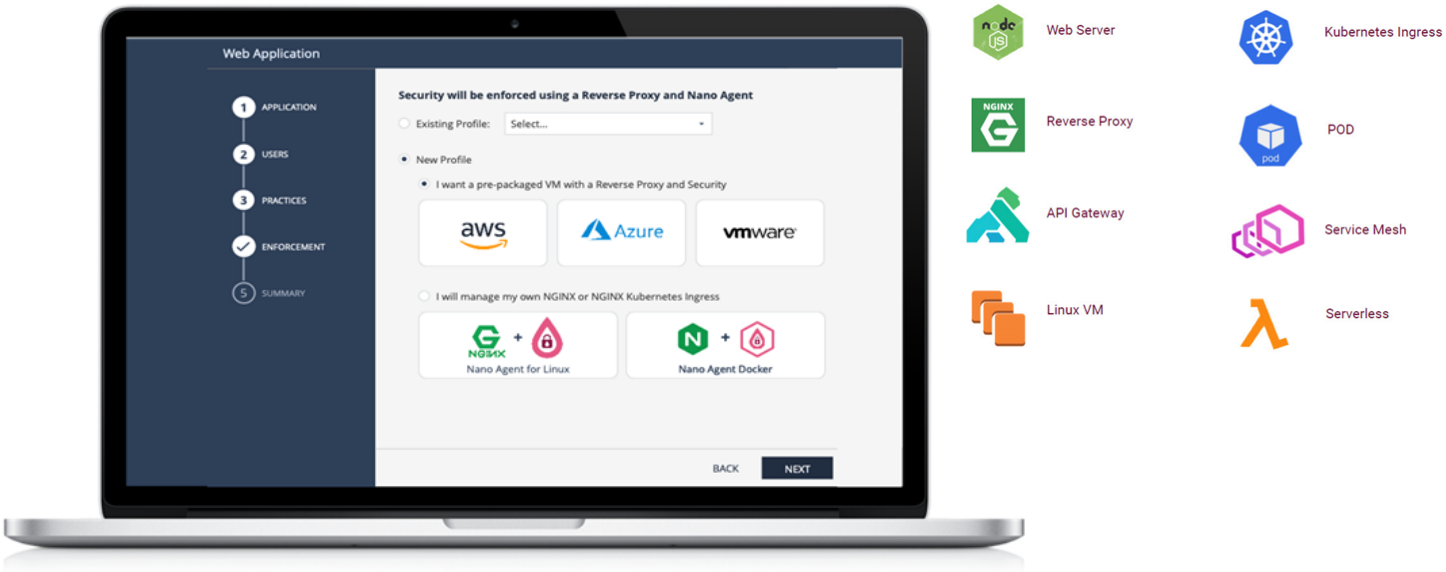
- Web Application Protection
- API Security
- Bot Prevention
- Intrusion Prevention (IPS)
- File Security

KEY PRODUCT BENEFITS

- **Preemptive Protection:** Contextual machine learning provides precise analysis, preventing known and unknown cyber attacks.
- **CI/CD Automation:** Auto-deploy on any cloud, hands-off management, DevOps friendly by design.
- **Utmost Efficiency:** No Signiture Update, No False Positives, No Manual Tuning

Cloud Distributed WAF

Instead of securing your application perimeter, CloudGuard WAF is deployed across all of your application components, providing complete cloud coverage



SUPPORTED ENVIRONMENTS

CLOUD

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

CONTAINERS

- Docker
- Kubernetes
- Kubernetes Ingress

CPU'S

- 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

Dec 2022 - CloudGuard AppSec Recognized as the Only WAF to successfully block a penetration test by Team82

Claroty Team82 has developed a generic bypass for web application firewalls (WAF). Major WAF products including: AWS, F5, CloudFlare, Imperva and Palo Alto were found to be vulnerable. CloudGuardd AppSec pre-emptively blocked the attack/bypass, within seconds.

Licensing Model	Description	SKU
CloudGuard (part of Workloads)	100 workload units, 1Y subscription 1 unit = 10M requests (or serverless / containers)	CP-CGWL-SL-100-1Y
Stand-Alone	100M requests 1Y subscription	CP-CGAS-100-1Y
	100M additional requests 1Y subscription	CP-CGAS-100A-1Y
PAYG	1M yearly requests	Use Marketplace Listing

Worldwide Headquarters
5 Ha'Solelim 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: 650-654-4233
www.checkpoint.com/cloudguard/appsec/