

CloudGuard AppSec

Preemptive Web Application & API Protection (WAAP)

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.

RADAR REPOR

LEADER

CloudGuard

Secure the Cloud

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With modern applications being developed and deployed at breakneck speed, it is becoming increasingly clear that this outdated approach is unable to keep up with the pace and scope of DevOps practices.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

THREAT PREVENTION	BEHAVIORS EXCEPTIONS	EVENTS			
• S WEB APPLICATION SECL	JRITY BEST PRACTICE Mode:	Prevent 👻	>		
		Learn / Detect			
WEB ATTACKS	Mode: As Top Level 👻	Prevent			
Activate when Confidence is:		Disabled			
High and above Advanced	ł				
✓ Cross Site Request Forgery	 Evasion Techniques 	✓ Vulnerability Scanning			
✓ XML External Entity	✓ LDAP Injection	✓ SQL Injection			
 Remote Code Execution 	Remote Code Execution 🗸 Path Traversal		✓ Other		



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 clientside 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.

Objects • O Install Policy Logs General Overview ×	NewTab +											CHECK POINT	1
												Q. Search	
* Queries C Q @ All	Time • Enter sear	ch query (Ctrl+F)											· ·
											Query Synta	Object Categories	
← General Overview >	Critical Attack	Types Not prevented	by policy								E Optic	ons - A Network Objects	
												Services	5
Attack Types by Blades						Activity Timeline						1 Applications/Categorie	
						Critical High						VPN Communities	
1 7 IPS	1	Anti-Bot		2 Threa								An Data Types 424 Users	
				🖤 🗲 Emula	ation							Servers	
						ifeel						Time Objects	
Anti Mari			tostor		• Eutraction							& UserCheck Interactions	
😵 3 Anti-Viru	IS T	0 DDoS Pro	tector	U Threa	t Extraction							🔁 Limit	
-	-												
						Feb 13, 201	19 1:00 AM	1:00 AM 1:0	AM 1:00 AM	Dec 10, 2019 Fe	6 8, 2020		
Top Attacks				Top Sources				Top Destinations					
Protection Name	Severity •	Blade	L	Source	Severity	* Blade	Logs	Destination	Severity	• Blade	Logs		
MIT Kerberos kadmind RPC	Critical	1 IPS	100	10.132.5.65	Critical	Multiple Blades	57	10.226.111.43	Critical	Threat Emulation		×	
Backdoor.Win32.Taidoor.A	Critical	Anti-Bot	11	192.168.9.78	Critical	1 PS	25	10.225.243.132	Critical	1 PS	10		
Microsoft Windows RASMA	Critical	1 IPS	8	III 10.132.5.50	Critical	Threat Emulation	12	192,168,72,71	Critical	1 PS	10		
Exploited pdf document	Critical	C Threat Emulation	6	= 10.226.111.7	Critical	1 B	10	192.168.72.40	Critical	1 15	8		
Exploited doc document	Critical	C Threat Emulation	6	30 10.132.5.213	Critical	1 PS	6	28 10.7.98.85	Critical	1 IPS	8		
Malicious Binary,balmbij	Critical	Anti-Virus	2	10.82.92.88	Critical	10 PS	5	192.168.72.190	Critical	1 PS	7		
Microsoft Windows Remote	Critical	IPS	1	B 10.132.5.101	Critical	10 PS	4	10.82.92.147	Critical	10 IPS	6		
Alt-N Technologies Security	High	1P5	7	192.168.9.59	Critical	🔮 IPS	4	192.168.72.162	Critical	10 PS	6		
Novell eDirectory HTTP Hea	High	1PS	6	10.132.5.42	Critical	1 PS	4	192.168.20.92	Critical	🖤 IPS	6		
Microsoft WINS Local Privile	High	🔮 IPS	6	10.82.92.4	Critical	🔮 IPS	4	I0.23.147.5	Critical	🔮 ins	6		
EICAR-Test-File	High	2 Anti-Virus	4	= 10.226.111.88	Critical	🔮 IPS	2	192.168.72.87	Critical	🕲 Anti-Bot	4		
Virus.WIN32.Eicar-Modified	High	😨 Anti-Virus	4	10.82.92.56	Critical	🔮 IPS	2	I0.23.147.132	Critical	🔮 ins	4		
Multiple Vendor SNMPv3 H.,	- High	1PS	1	192.168.35.16	Critical	10 PS	1	10.225.243.64	Critical	🔮 IPS	4		
13 Protections	Critical	4 Blades	162	10.23.147.157	Critical	🖤 PS	1	192.168.72.129	Critical	🔮 IPS	4		
			_	192,168,9,56	Critical	10 PS	1	I0.23.147.159	Critical	🖤 iPS	4		
				192.168.20.30	Critical	V Anti-Virus	1	10.23.147.92	Critical	🔮 IPS	4		
No tasks in progress +						Cloud Demo Sen							

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

Web Application	•			Web Server	₩¥	Kubernet
	Security will be enforced using Existing Profile: Select	a Reverse Proxy and	Nano Agent	Reverse Proxy		POD
2 USERS	New Profile				pod	
3 PRACTICES	I want a pre-packaged VM w			API Gateway		
	aws	🔥 Azure	vm ware [*]			Service M
5 summary	I will manage my own NGIN	X or NGINX Kubernetes I	Ingress	Linux VM		Serverless
	G + 🙆		N + 🙆		Λ.	Serveriess
	Nano Agent for Linux	N	lano Agent Docker			
			BACK NEXT			
		9				

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/