viettel Cloudrity

Comprehensive security solution for your website

Outstanding Features of Cloudrity

✓

Anti DDoS attack – Network Layer (L4)

DDoS attacks are routed to the Cloudrity system and are intercepted by the system/operator before reaching client's server.

✓

Web Application Firewall

Automatically detect and prevent requests to exploit website vulnerabilities of the list of OSWAP TOP 10 attack,etc.

✓

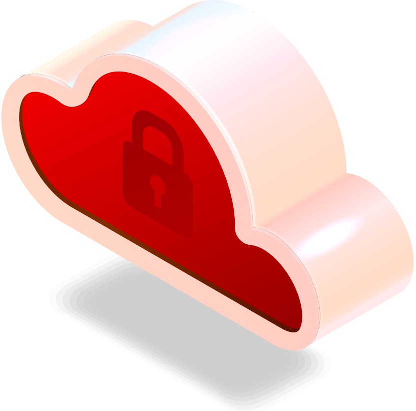
Anti DDoS attack – Application Layer (L7)

Automatically detect and prevent HTTP Flood and Slow attack (Slow POST, Slow loris); block bot request on website using cookie and captcha challenge.

Cyber Security Threats

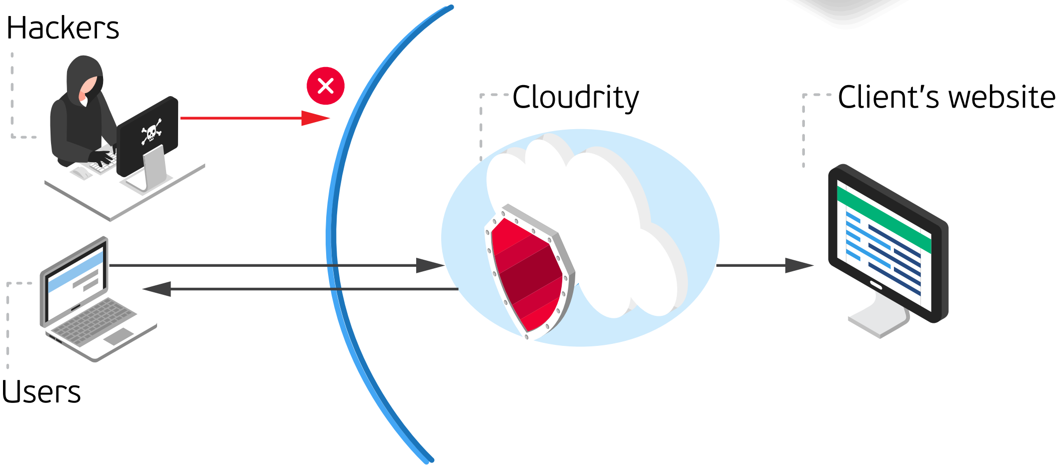
COVID-19 pandemic still takes place extremely complicated, resulting in the growth of demand for digital transformation, many organizations and businesses require to work remotely, but not have fully-security ensured yet, leading to data leaks and account takeover threats. According to Viettel Threat Intelligence, the number of vulnerabilities discovered in the 1st quarter of 2022 increased by 33.31% compared to the same period in 2021. Cloudrity statistics in the 2nd quarter of 2022:

16,933,145	9,152,589	152,328
Website vulnerabilities exploiting attack	Anti DDoS attack (L4)	Anti DDoS attack (L7)



Cloudrity is built with the aims to protect client's website against intentionally external attack, thus maintaining production and business process effectively.

Operating Model



Service Packages of Cloudrity

Feature	Description	Service		
		WP Silver	WP Gold	WP Platinum
Web Application Firewall	Protect against OWASP Top 10 attacks – 10 most common website security vulnerabilities according to OWASP standards. These vulnerabilities allow hackers to exploit,attack and infiltrate data on website.	Basic *	Full *	Full *
	Prevent exploiting 1-day, that are announced of web framework, web server, mail server, etc. Websites using out-of-date versions that have not been patched with vulnerabilities of these technologies are at risk of being exploited by hackers.		✓	✓
	Insert customized block rules as required.	✓	✓	✓
Anti DDoS attack	Protect against network-layer DDoS attack (DDoS L4) - volume based attacks like UDP Flood, SYN Flood.	1Gbps	5Gbps	As required
	Protect against application-layer DDoS attack (DDoS L7) like HTTP Flood, Slow loris.	500Mbps	2Gbps	As required
	Block bot using cookie challenge.	✓	✓	✓
	Maximum access frequency	1000rps	5000rps	As required
	Limit access frequency from each IP address (by the number of request and connection)	✓	✓	✓
Access list	Manage IP blacklist/ whitelist	✓	✓	✓
	Manage URL whitelist	✓	✓	✓
Monitoring	Monitor bandwidth usage (bps, rps, cps, pps)	✓	✓	✓
	Monitor attack events (WAF, DDoS L7)	✓	✓	✓
Report	Periodic report sent automatically	✓	✓	✓
	Customized report			✓
Alert	SMS alerts of website downtime			✓
Other features	IPv6 support	✓	✓	✓
	CNAME support	✓	✓	✓
Commitment to service quality	Uptime commitment (even when attack occurs)		99.99%	99.99%
	Support 24/7		✓	✓
	Urgent support hotline		✓	✓
	Processing request response time level 1*		2-hour maximum	30-minute maximum
	Processing request response time level 2*		4-hour maximum	1-hour maximum
	Processing request response time level 3*		24-hour maximum	8-hour maximum

Note:

Basic*: includes the most basic rules that web application firewall can turn on right away and has a low false-positive error rate.

Full*: includes the most basic rules that web application firewall can turn on right away and has a low false-positive error rate.

Level 1*: serious issues affecting the availability (uptime) of the entire service.

Level 2*: less serious errors, or false positive errors.

Level 3*: requires configuration updates, questions and answers.

For more information, please visit

www.cloudrity.com.vn ☎ +84 971 360 360

viettel security