instartlogic

“Instart Logic’s Cloud Application Security Suite”

Provides comprehensive multi-layered protection for web applications, leveraging a unique client-cloud Software Defined Application Delivery Platform

>> Malicious attacks, denial of service, and data breaches are on the rise. Hackers and thieves are leveraging cloud technologies to launch increasingly larger and more sophisticated attacks. This can significantly impact enterprises, causing costly service disruptions, lost productivity, and irate customers.

Instart Logic’s Security Suite provides protection across the end-to-end delivery path, from device to cloud to origin with DDoS protection, Web Application Firewall capabilities, and origin protection. The security suite is available today with our Software Defined Application Delivery Service and is PCI Level 1 Certified to keep websites operating with confidence.

Our Web Application Firewall inspects your HTTP and HTTPS web traffic for suspicious or malicious activity and detects and blocks any suspect traffic from reaching your web applications across our globally distributed network. Our web application firewall provides always-on protection against the most critical web application security threats including the OWASP Top 10 vulnerabilities – Cross Site Scripting, SQL injection, HTTP Slow Start, Cross-Site Request Forgery, among others. Our professional support team has years of security experience and continuously refines our WAF rules to ensure that your web applications are always protected as new attack vectors emerge.

instartlogic

Key Capabilities:

Network layer protection

- Only accepts valid HTTP traffic and all other traffic types are dropped
- DDoS protection that absorbs distributed denial of service attacks at the edge
- IP, geography, and user agent based rate

Application layer protection

- Inspection of Layer 7 traffic
- Plaintext and SSL-encrypted traffic inspection (available for PCI & non-PCI environments)
- HTTP-awareness (protocol validation, encodings, cookies, etc.)

Signature-based detection

- Based on the respected ModSecurity engine
- OWASP core rule set (OWASP Top 10 coverage)
- Custom rules
- Virtual patching

>> *Layered approach to Application Attack Protection*

		Instart Logic	Akamai
Phase 1	• Proxy-level blocking and throttling • Based on IP, User Agent, or Geo • *Addresses about 75% of attacks*	x	x
Phase 2	• WAF-level request filtering • Based on multiple request features fed into Modsecurity • *Addresses remaining 25% of attacks*	x	x
Phase 3	• Proxy & WAF-based countermeasures remain in place • Neustar scrubbing service activated	x	x