

Application Activity Monitoring - Web Application Firewall Services

CGI's Web Application Firewall service (WAF) provides a centralized policy enforcement point for the web tier of multi-tiered applications. Security supervision is required by many IT policy and risk management frameworks such as Payment Card Industry Data Security Standard.

Traditional network firewalls can be easily subverted by attacks hidden within the application layer, often rendered inaccessible by encryption, lack of analysis depth, or lack of contextual awareness. Web client logon sessions can be easily taken over by malicious techniques and advanced persistent threats (such as cross-site scripting and bot-net malware) that abuse the trust model in most web browser clients.

Often web application designers trust that security issues are solved solely with authentication and encryption. However, web applications often inadequately inspect the appropriateness of messages destined for web applications. Anonymous logons, unauthorized data modifications, and unexpected data sequences can easily ruin the integrity of web applications and the underlying databases without even "hacking the server" which host these components.

Web Application Firewall Services Description

The WAF service looks inside the encryption and spots unexpected data sequences and blocks them gracefully, and provides a compensating control to manage the risks from weak software applications while they are being repaired. CGI deploys, administers and monitors client premise equipment for repeatable, measurable smooth operations, allowing your organization to leverage expensive infrastructure and skill-sets which would be otherwise unattainable.

The CGI WAF service integrates into your change management processes, and is supported by a service level agreement, delivering 24x7 vigilance and enforcement, without the loss of government policy control. As an integral part of the CGI Managed Security Services group, the Security Operations Center (CGI MSS SOC) provides 24x7 monitoring, identification of exceptional events, and notification that includes recommended containment countermeasures.

Basic Services

- Affirmative Application Service Policy Enforcement
 - Enforce baseline security policy at the web-application layer
- Vulnerability Identification, Masking and Exploit Containment
 - Identify exploits of web application vulnerabilities
- Authorized Containment / Intrusion Prevention
 - Owner-authorized web application transaction impact
 - Graceful prevention and negative acknowledgements
- Security Exception Monitoring and Handling
 - Vigilant coverage 24x7
 - Identify gross exceptions
 - Low-latency response
 - Notification and recommendation of appropriate containment activities to application owner or CIRT.
- Compliance Information Support
 - Support compliance audit trails and reporting.
- Design and Implementation Assessment to identify application and implementation security gaps