WEB APPLICATION FIREWALL

KAAPAGAM

MSC MALAYSIA Status Company

Kaapagam Technologies Sdn. Bhd. (1015448-T)

Unit No:9, 1st Floor, Resource Centre, Innovation Incubation Centre (IIC), TPM, 57000 Bukit Jalil, Kuala Lumpur

Tel : +603 8992 3172 Fax : +603 8998 4010 Email : sales@kaapagamtech.com Web: http://www.kaapagamtech.com

Web applications, are the most vulnerable elements of an organization's IT infrastructure today. According to a research by the **Gartner Group** :

- **Almost three-fourths of all Internet assaults are targeted at Web applications**.
- Estimated 80% of all security breaches are due to vulnerabilities within the web application layer (attacks exclusively using the HTTP/HTTPS protocol) **leading to the theft of sensitive corporate data such as credit card information and customer lists.**
- Traditional security mechanisms such as **firewalls and IDS provide little or no protection against attacks on your web applications**

Insecure web applications provide easy access to backend corporate databases. Firewalls, SSL and locked-down servers are futile against web application hacking! Web application attacks, launched on port 80/443, go straight through the firewall, pass through operating system and network level security, and right in to the heart of your application and corporate data. Tailor-made web applications are often insufficiently tested, have undiscovered vulnerabilities and are therefore easy prey for hackers.

Web applications are vulnerable to long list of attacks due to the practical difficulty of following Secure Coding / Secure Programming practices on a business oriented IT software development eco system. For example, source code review on thousands of lines of codes incur substantial amount of time and cost for each application. Furthermore, source code review & audit must be done on the entire code base every time when there are changes or additions to the application code. As this creates burden on the project timelines as well as budgets, most of the organizations do not follow the secure coding and auditing practices.

In addition to the vulnerabilities from the application itself, vulnerabilities from operating systems, firmware's, web server software's, web application language platforms, database platforms, etc. introduce more entry points and attack vectors for attackers to party on the infrastructure.

The vast majority of web applications have inadequate security, hence a Web Application Firewall (WAF) is necessary. According to Web Application Security Consortium, A Web Application Firewall is an intermediary device, sitting between a web-client and a web server, analysing OSI Layer-7 messages for violations in the Application security policy. A web application firewall is used as a security device protecting the web server from attack.

VALARI is a Web Application Firewall & Security Management System designed to secure your web applications from attacks and provide a layer of security by proxy-ing all HTTP(S) traffic and shield web servers and databases from direct access of the attackers irrespective of the underlying application vulnerabilities.

- VALARI can **detect and block all the OWASP Top 10 Vulnerabilities** and many more Web application threats:

  HTTP Distributed Denial of Service (DDoS), HTTP Flooding and Slow HTTP DoS Attacks, Brute Force Login, OS Command Injection, Parameter / Form Field Tampering, Data Disclosure, Phishing Attacks, SQL Injection, Cross Site Request Forgery (CSRF), Cross Site Scripting (XSS), Drive-by-Downloads, Directory Traversal, Buffer Overflow, Cookie Injection, Cookie Poisoning, Site Reconnaissance, Data Destruction, Remote File Inclusion Attacks, Google Hacking, Anonymous Proxy Vulnerabilities, HTTP Response Splitting, HTTP Verb Tampering, HTTP Parameter Pollution Attack, Malicious Encoding, Malicious Robots, Known Worms, Web Services (XML) attacks, Session Hijacking, Site Scraping, Sensitive Data Leakage (Social Security Numbers, Cardholder Data, PII, HPI), Web server software and operating system attacks, Zero Day Web Worms, Forceful Browsing of Website Content, Automated Botnet Attacks, Manipulation of Query String Parameters and many more ……

- **Full Web Traffic Logging** : contents in the web Request bodies are not logged by the web servers and hence attackers use POST requests to delivery exploits and it goes completely blind on the web server logs. With full HTTP transaction logging in VALARI, it is possible to log all requests and responses. This Logging feature can be controlled on what and when a log is created. VALARI can be configured to mask the sensitive data in the request and/or response fields before they are written to the audit log.

- **Web Intrusion Detection with Just-In Time Monitoring and Detection** : Web Traffics are monitored real time to detect attacks and react on suspicious events / data that hit your web applications.

- **Built-in Anti-evasion and Encoding validation mechanisms**.

- **Protected protocols: HTTP, HTTPS (SSL), XML, Web services, SOAP and AJAX**

- **Facilitates compliance with PCI DSS requirement 6.6**

- **Attack Prevention and External Patching / Virtual Patching** : VALARI acts immediately to prevent attacks from reaching your web applications. With more than 20,000 specific rules, VALARI is an ideal external patching tool. External patching (referred to as Virtual Patching) is about reducing the window of opportunity as the time needed to fix / patch application vulnerabilities often take weeks to months. With VALARI, application vulnerabilities can be patched from the WAF Layer without patching the application source code making your applications secure until a proper patch is applied to the application by your development team or vendors.

- **Flexible Rule Engine** : The Heart of VALARI is made up of our flexible rule engine with more than 20,000 specific rules covering all sorts of application vulnerabilities, signature patterns and evasion patterns. Our Rule engine is implemented with hardening, protocol validation and detection of web application security issues and is kept updated on regular basis as and when vulnerabilities and attack vectors evolve.

- **Geo-location Blocking** : VALARI allows Geo-location blocking to block request originated from specific countries

- **Integrated Security Rules** from various public vulnerability data signature sources and VALARI correlates data from all these numerous sources to generate the Flexible – Scalable – Reliable rules, automatically updating daily and as needed. Various vulnerability data signature sources include :
    - Kaapagam Tech Rule Set
    - Public vulnerability data such as the Open Source Vulnerability Database (OSVDB)
    - Honeypot systems

- **High Availability Deployment option** with Active & Passive VALARI Units with identical rule sets and configurations. The Passive VALARI unit can be put-in action if the primary VALARI unit is down for any unforeseen circumstances.

TESTIMONIALS

" VALARI, an indigenous product of Kaapagam Technologies have been successfully protecting our Web Assets for more than 3 years now with NO intrusion incident. We are happy with the auto-updates on the rule sets and prompt support. Furthermore VALARI give us good support in term of testing and vulnerabilities on current attack at our Web. Base on good support we are able to minimize the risk. WAF also give us good protection on the Web and we confident on the capabilities of the protection. Thanks for all response and support to MiCare. "

- Mr. Fu Chwan Jye, CIO, MiCare

" Kaapagam Technologies is our Security Partner for the last 4 years and we have selected to use VALARI after POC session with other competing products and VALARI passed our tests with flying colors. We are using VALARI for 2 years now with NO incidents. Our Load is around 650K requests a day and the appliance handles it with breeze. We recommend VALARI for anyone who needs to protect web applications "

- Mr. Gary, IT Head, Monash University

" Golden Screen Cinemas, has been working with Kaapagam Technologies Sdn. Bhd. to assist us with various IT initiatives since 2012. We engaged Kaapagam for Pentest and IT Consultancy services. During this time we have found Kaapagam to be very professional, technically knowledgeable, helpful and willing to go the extra mile in delivering its services to meet our IT Security needs. It is because of this well-established trust and confidence that we have in Kaapagam, we are now using their VALAI Enterprise IPS/IDS, at our headquarters to protect our IT network. We have decided to use VALARI for our E-Payment systems after the product cleared all our POC tests. Kaapagam will continue to be our partner and we see them as an integral part of our IT team. "

- Mr. Lye, IT Manager, Golden Screen Cinemas

COMMON CRITERIA CERTIFICATION

VALARI has successfully completed PreCC and Currently submitted for Common Criteria Certification (ISO /IEC 15408).

VALARI is supported by Cyber Security Malaysia, An agency under Ministry of Science, Technology, and Innovation (MOSTI).

Common Criteria Certification for VALARI is funded by MOSTI

With Common Criteria Certification, VALARI will be the only WAF in APAC certified with CC

SUPPORT & MAINTENANCE

- Standard Support :

  VALARI will be deployed with 1 year Maintenance and Standard Support on Software components and rule sets. Customer will be provided with a telephone number and email to make Service / Support Request. The Support number operates during business hours, 9:00 a.m. to 5:00 p.m. (GMT +8), Monday through Friday, excluding legal holidays. All Software related supports will be done remotely via Team Viewer or VPN access. The Support is inclusive of any patches and upgrades to the existing system.

- Premium Support :

  Premium Support of VALARI includes 24 x 7 x 365 email and phone support. All Software related supports will be done remotely via Team Viewer or VPN access. The Support is inclusive of any patches and upgrades to the existing system.

OUR CONSULTANTS

Seasoned Consultants Deliver . . .

Kaapagam Technologies is committed to deliveringthe highest quality consultancy to help you achieve your business goals and eliminate issues. No matter which technology or devices you use, you can count on our consultants—with years of hands-on experience—to be your teammate.

At Kaapagam Technologies, we select only the experts in their respective field who can pass our rigorous selection process. Each consultant is an acknowledged subject matter expert who is dedicated to customer's requirements

List of Certifications achieved by our consultants

Certified Information System Security Professional (CISSP)
Certified Ethical Hacker (CEH)
Computer Hacking Forensic Investigator (CHFI)
EC-Council Certified Secure Programmer (ECSP)
EC-Council Certified Incident Handler (ECIH)
EC-Council Certified Security Analyst (ECSA)
EC-Council Certified Licensed Penetration Tester (LPT)
EC-Council Certified Disaster Recovery Professional (EDRP)
EC-Council Certified VoIP Professional (ECVP)
EC-Council Certified Instructor (CEI)
Open Source Wireless Integration Security Professional (OSWiSP)
Offensive Security Certified Professional (OSCP)
GIAC Certified Security Essential (GSEC)
GIAC Certified Penetration Tester (GPEN)
GIAC Certified Incident Handler (GCIH)
GIAC Certified Forensic Analyst (GCFA)
GIAC Reverse Engineering Malware (GREM)
SCSAS (Sun Certified Solaris Associate)
CCDA (Cisco Certified Design Associate)

CCNA (Cisco Certified Network Associate)

Microsoft Certified Systems Engineer (MCSE)

Microsoft Certified Professional Developer (MCPD)

Microsoft Certified IT Professional – Business Intelligence

Microsoft Certified IT Professional – Enterprise Messaging

Microsoft Certified Technology Specialist – Web Applications

Microsoft Certified Technology Specialist – Virtualization

Microsoft Certified Technology Specialist – Database

Microsoft Certified Trainer (MCT)

Microsoft Most Valuable Professional (MVP) - Security

CONTACT US

At **Kaapagam Technologies,** customer service is everyone's responsibility. Our goal is to provide "High Calibre" service to our customers.

For further details, please contact: Clement Arul @ clementarul@kaapagamtech.com

Unit No: 9, 1st Floor, Resource Centre, Innovation Incubation Centre (IIC),
Technology Park Malaysia, 57000 Bukit Jalil, Kuala Lumpur
Tel : +603 8992 3172
Fax : +603 8998 4010
Email : sales@kaapagamtech.com
Web: http://www.kaapagamtech.com