

# CORISECIO - WAF - Service

*Security Automation across the SOA Lifecycle*

Brute Force, DoS attacks as well as SQL injections in SOA environments also are daily threats. Therefore, the use of Web Application Firewalls (WAF) is necessary but not sufficient for adequate protection of services and message exchange. Conventional Web Application Firewalls quickly meet their limits when handling Web Services. Especially when dealing with SOAP messages these solutions are not able to identify resp. repel attacks. The XML Schema validation turns out to be difficult because of message transformation and addition of further security features (SAML, Token etc.) on message level. Also the transfer of assumedly invalid data (e.g. encrypted SOAP messages) would lead to an error and the result would not be reliable.

Furthermore a SOA infrastructure creates questions regarding distribution and scaling of individual WAF hierarchies. In many cases an implementation in front of each service is not advisable for financial reasons.

### SECURITY AS A SERVICE

In a SOA infrastructure it is wise to provide security mechanisms as services themselves. Via standardized interfaces Security Services may be provided domain wide and used by all services. Functionality itself does not have to be installed in front of or in each application. Even license and operating costs may be decreased significantly with central resp. domain wide Security Services.

### CORISECIO - WEB APPLICATION FIREWALL SERVICE

CORISECIO provides a WAF Service for SOA infrastructures. The Content Filter analyses the data stream and forwards appropriate parts for testing to the Web Application Firewall. The CORISECIO securityRunTime integrates the powerful Deny All Web Application Firewall in the SOA environment and protects web applications against any attacks. Threat scenarios from Brute Force, Cross-Site- Scripting via Session Manipulation up to entry of invalid parameters are reliably prevented with high performing real-time scanning technologies. For the user all scans occur completely transparent and without changing of workflows. Existing applications do need not to be adjusted.

### MODELING AND ORCHESTRATION

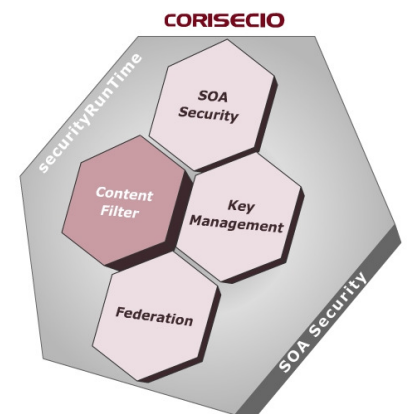
The modeling function of the CORISECIO securityRunTime allows use of the Web Application Firewall as system wide or local service.

### FACTS

- Protection against any web attacks
- Web Application Firewall for SOA
- Security as a Service implementation
- Use of existing WAF-solutions for SOA

### BENEFITS

- Low administration and configuration effort
- Low migration and license costs
- Future proofness
- Decreasing costs for maintenance and operations





Encrypted Web Services may so be tested reliably as only decrypted data is forwarded to the WAF. The administration is completely integrated. So the Deny All Web Application Firewall is configurable with preconfigured settings as well as individually via the CORISECIO administration.

### SOA SECURITY INFRASTRUCTURE

The CORISECIO solution provides a Security Basis for SOA infrastructures. Security Standards, implementation, administration and automation are the basis. The solution may easily be enhanced with security mechanisms because of the flexible adapter concept.

## KEY FEATURES

### ■ CORISECIO securityRunTime

System and platform independent run time environment for security applications.

(see Factsheet - securityRunTime)

### ■ Adapter - Content Filter

- *Data stream & message filter*
- *Supports:*
  - *http/https*
  - *FTP*
  - *XML/SOAP*

### ■ Adapter - WAF Deny All

- *Web Application Firewall Function (modelable)*
- *Integration of Deny All rweb WAF*
- *Administration via CORISECIO— Security Administration*

