PRODUCT SHEET

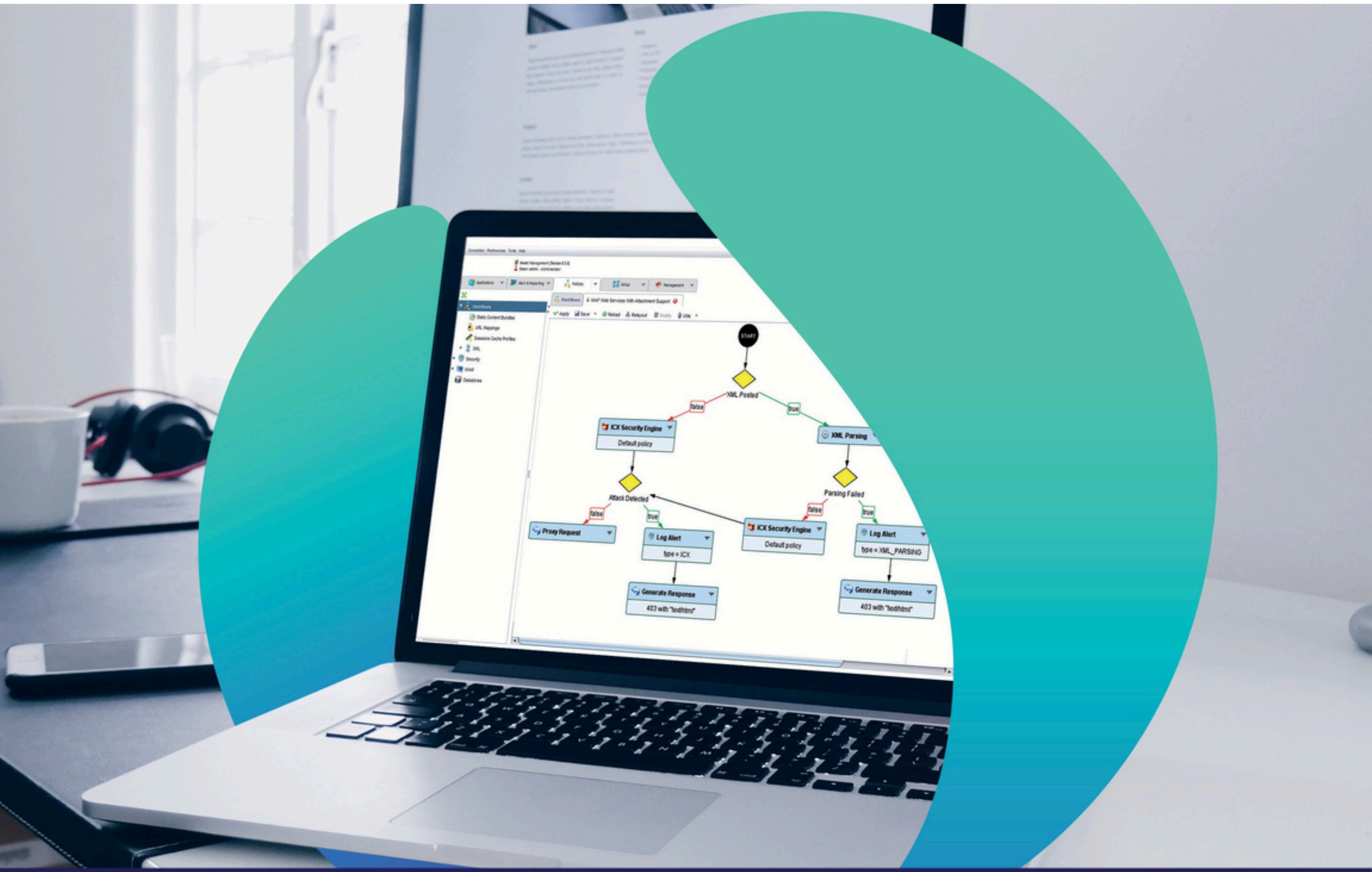
UBIKA WAAP GATEWAY

A complete solution to meet your security needs

UBIKA WAAP Gateway is a comprehensive solution offering a full range of features for managing enterprise-level application security. Designed to protect critical business applications, including legacy applications and custom APIs, from complex attacks while meeting data privacy requirements, it is suitable for any customer environment and supports global high-performance web applications and continuous development of new software.

Key Benefits

- Recognized as a “Strong Performer” by Gartner Peer Insight in 2022 for WAAPs - web application and API protection solutions - UBIKA WAAP provides a powerful all-in-one solution designed for public and private sector companies that value innovation and flexibility to meet their specific needs.
- Software version 6.11 CSPN first level certified by ANSSI.
- Helps organizations in DevOps mode by reducing security risks and total cost of ownership, while improving application performance.
- Fully scalable and technology-independent, it enables consistent management of applications deployed in multi-cloud or hybrid cloud environments, avoiding vendor lock-in and rising costs. Compatible with Cloud Providers Google, AWS, Microsoft, as well as sovereign clouds OVHcloud and Outscale.
- Flexible, powerful graphical workflow for creating security policies tailored to your needs.
- Capable of meeting the most stringent compliance and auditing requirements: PCI DSS, PSD2, NIS2 directive, DORA, RGPD.



Main features

- Proactive protection against known and unknown 0-day threats that can lead to data loss/theft, sabotage, application denial of service (L7 DoS).
- Proven effectiveness against OWASP Top 10 attacks.
- Encryption and signature management, modification of all or part of the request and response.
- Security core based on a combination of several engines for enhanced security, including a generic patterns engine detecting attacks in request content and a scoring engine.
- Detection of attacks even in encoded content.
- Query replay for policy testing and forensic analysis.
- Proactive detection and mitigation of bots.
- Handling of JSON and XML content.
- Easy integration with third-party ICAP file scanners.
- Application learning mode for enhanced protection and better performance during the software development cycle.
- IP geolocation.
- Powerful log analysis to drill down to a specific security problem.
- Redis datastore enables interaction between different elements to create security mechanisms.

Graphical workflow configuration

- Accessible and intuitive graphical workflow editor.
- One-click switching from blocking mode to observation mode for all or part of the security policy.
- Visualization of traffic processing and inspection flows.
- Customization of the response page according to the attack context.
- Ability to combine multiple security engines via the workflow editor for more accurate detection.

Services & Support

- Expert technical support team, in French or English, based in France.
- 24/7 portal for managing support tickets for all types of incident.
- 24/7 telephone support available as an option.
- Product certification training for partners and administrators.

Deployment

- Wide range of physical and virtual appliances selected and tested for maximum performance (from 21,000 to 100,000 transactions per second).
- Multi-cloud provider compatible:
  - Available on AWS (Amazon Web Services), Microsoft Azure, GCP (Google Cloud Platform) and Outscale marketplaces.
  - Generic cloud image compatible with private and sovereign clouds: OVHcloud, Outscale and Cloud Temple.
- Active-passive deployments for high availability.
- Supports distributed architectures: Multiple DMZs for high-security deployments.
- Rapid deployment and automation via API, thanks to Ansible and Terraform.

Optional modules

Advanced Package

Advanced API Security

Enhanced API security for proprietary API-based applications and machine-to-machine communications.

- XML encryption and signing
- Analysis and generation of JSON Web tokens
- JSON, XML and OpenAPI3 schema validation for enhanced whitelist security - without false positive management.

Advanced Web Security

- WebSocket message content protection
- Improved and easier management of false positives, with logging of excepted requests to detect security exceptions that could expose applications.

Authentication Package

- Web Access Manager
- Simplified user authentication via Web Single Sign On (SSO)
- Authentication adapted to user context
- Integration with LDAP, AD, Radius
- Packages for SAML and OAuth authentication.

IP Reputation

- Enhanced security with the addition of IP reputation from Threat Intelligence sources.
- Optimize performance by filtering requests from malicious IP sources.
- Flexibility in the level of security required.

Version 01.00 | juin 2022
Données sous réserve de modification
Image : Adobe Stock

UBIKA

UBIKA
9-11 rue Jeanne Braconnier - 92366 Meudon | France
Tel +33 (0)1 46 20 96 00 | www.ubikasec.com