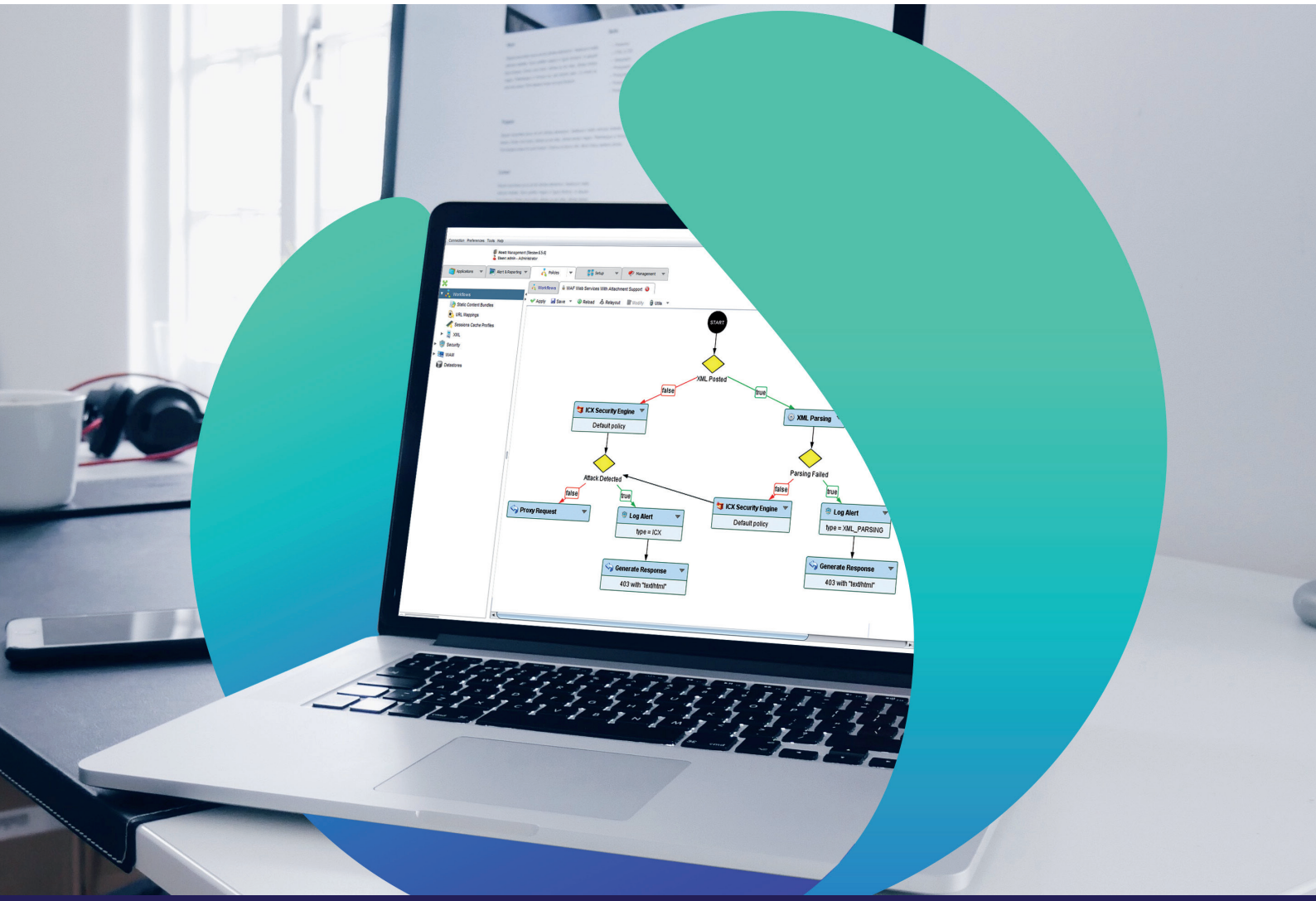
PRODUCT SHEET

UBIKA
WAAP GATEWAY

UBIKA WAAP Gateway is a comprehensive solution offering a full range of features to manage application security at the enterprise level. Designed to protect critical business applications, including existing legacy applications and custom APIs from complex attacks while respecting 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 2022 Gartner Peer Insight "Strong Performer" for Web Application and API Protection solutions, UBIKA provides an all-in-one powerful solution designed for public and private sector enterprise customers who value innovation and flexibility to meet their specific needs
- Helping organizations in a DevOps mode of operation by reducing security risk and TCO while improving application performance
- Fully scalable and technology agnostic, allowing to consistently manage applications deployed in multi-cloud or hybrid cloud environments avoiding vendor lock-in and escalating costs
- Able to address the most stringent compliance and audit requirements: PCI DSS, PSD2, NIS Directive, GDPR, OZG



Deployment

- Range of physical and virtual appliances selected and tested for maximum performance
- (from 21,000 to 100,000 transactions per second)
- Available on AWS (Amazon Web Services), Microsoft® Azure marketplaces and GCP (Google Cloud Platform)
- Preconfigured policy templates for standard applications: e.g. Microsoft® SharePoint, OWA365, Exchange, SAP®, WordPress, Drupal
- Active-passive and active-active deployments for high availability
- Supports distributed architectures: multiple DMZs for high security deployments
- Fast deployment and automation using Terraform /Ansible

OPTIONAL MODULES

Extended API Security

- Securing API-based custom applications and Machine-to-Machine communications
- XML / JSON ciphering and signature
- JSON Web Token parsing and generation

Web Access Manager

- Streamlining user authentication via web SSO
- Adaptive authentication based on user context
- Integration with LDAP, AD, Radius

IP Reputation

- Adding current, comprehensive and actionable threat intelligence feed into security policy
- Guaranteeing performance optimization by filtering out requests originating from malicious IP sources
- Reducing the risk of false positives by adjusting the policy based on the origin of request
- Disregarding requests from unwanted robots

Management Console

- Dedicated platform for centralized provisioning and management of all devices and applications
- Automated deployment of application security policy across all instances, including cloud-based Monitoring of web applications in real time
- Role-based access for distributed management tasks
- Customizable dashboard with drill down capability

Core product capabilities

- Proactive protection against known and unknown threats that can lead to data loss, sabotage, L7 denial of service (DoS)
- Proven effective against OWASP Top 10 attacks
- Ability to sign, verify signature, encrypt, decrypt, modify any part or entity of request or response
- Standard security based on generic patterns and scoring mechanism complemented by advanced security engines for more granular and accurate detection
- Log replay for policy testing and forensics analysis
- User reputation scoring to prevent online fraud and theft deterring illegitimate users
- Proactive bot detection and mitigation
- JSON Firewall and XML parsing and validation
- Seamless integration with third party file scanners
- (ICAP)
- Application learning for stronger protection and improved performance during the software development cycle
- OpenAPI Import / Export for API security and DevOps
- IP Geolocalization
- Powerful log analysis allows drilling down to a specific security issue
- Redis datastore creates real time security mechanisms

Graphical workflow configuration

- Accessible and intuitive management interface
- With a click, switching from blocking / logging mode on all or specific parts of a security policy
- Visualization of traffic processing and inspection flows
- Configurable attack response based on context
- Ability to chain multiple security engines via the workflow for accurate detection and reduced rate of false-positives

Services & support

- Expert technical support team based in Europe
- 24/7 portal to log support tickets for all types of incidents
- 24/7 phone support available as an option
- Product certification training for partners and administrators

UBIKA is a registered trademark from UBIKA company.
All other trademarks mentioned in this document belong to their respective owners.
Version 01.00 | June 2022
Data subject to change
Image : Adobe Stock
©2022 UBIKA | France

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