

# DenyAll 2014 Newsletter

Based on 2014 Gartner Magic Quadrant  
for Web Application Firewalls

June 2014



NEXT GENERATION APPLICATION SECURITY

# Summary

<b>1. Editorial</b> .....	<b>3</b>
Innovating for Next Generation Application Security .....	3
<b>2. Main messages</b> .....	<b>5</b>
2.1 Why DenyAll? .....	5
2.2 Innovation through Integration .....	5
2.3 Delivering Next Generation Application Security .....	6
2.4 Leveraging the Cloud.....	6

## 1. Editorial

### **Innovating for Next Generation Application Security**

Gartner's first MQ for Web Application Firewalls illustrates the growth in the application security market. WAFs and vulnerability scanners are "must have" security controls now. The WAF market is open, as illustrated in the Magic Quadrant by the fact that 11 of the 16 are vendors placed in the Niche Player Quadrant. DenyAll is well positioned in the MQ in terms of "completeness of vision", thanks to its innovation in security. Now forming one company with BeeWare, we will continue to innovate in years to come, delivering Next Generation Application Security solutions and expanding from our European base. [Click here for more](#) and read below for details.

### **DenyAll recognized in first Gartner Magic Quadrant for WAF**

We believe that Gartner publishing a Magic Quadrant for Web Application Firewalls (WAFs) shows that demand is high for application-specific security controls. The technology has matured. WAFs and Dynamic Application Security Testing (DAST) are "must have" security controls for many organizations nowadays.

In a web-enabled world, these tools complement network security controls to effectively secure modern IT. Businesses and governments around the world are coming to grasp with the notion that applications are vital and require specific investments, beyond network security, especially as they embrace the cloud. This trend was previously highlighted in the report "Web Application Firewalls Are Worth the Investment for Enterprises" published by Gartner analysts Jeremy D'Hoinne and Adam Hills on February 28, 2014.

The WAF market is growing fast, according to Gartner. It is still young and open, with 11 "niche players", 4 "challengers" and only one "leader" in the MQ.

### **BeeWare and DenyAll are among the 16 vendors listed in the MQ.**

Our vision is that our combined company will be one of the leading vendors in that space in years to come. We have been placed furthest along the "Completeness of Vision" axis for the Niche Players, and believe that is due to our innovation in security.

At DenyAll, we are experts in application security, with a proven track record of securing the applications of +600, very demanding customers in the last 15 years. Most of our competitors are load balancing or network security generalists. They don't know application security the way we do.

By acquiring BeeWare in May 2014, DenyAll reached critical mass and boosted its ability to lead the market from a technology innovation perspective. By leveraging the cloud and further integrating our WAF, WAM and DAST products, we will deliver superior Next Generation Application Security solutions.



Read more in this newsletter about our differentiators and vision for application security. And [contact us](#) to find out why some of the largest organizations in Europe have been trusting us with the security of their most critical applications.

**Stéphane de Saint Albin**

Chief Marketing Officer

DenyAll

## 2. Main messages

### 2.1 Why DenyAll?

The following are the differentiating features of DenyAll and BeeWare's now combined portfolio:

- Advanced security engines, providing accurate protection for modern languages and against anti-evasion techniques;
- Browser lightweight engine for end-to-end protection of web application sessions, protecting applications and data from man-in-the-browser attacks;
- Superior protection for Web services;
- Workflow interface for superior traffic and security policy configuration;
- Integrated Web Access Management;
- Integration with DenyAll Detect vulnerability scanners and Qualys;
- Ability to deploy on the cloud platforms of Amazon, Microsoft and more.

Find out why DenyAll and BeeWare have been recognized in the Magic Quadrant by reading the report.

### 2.2 Innovation through Integration

DenyAll's advanced web application security and vulnerability management capabilities are complemented by BeeWare's advanced workflow, XML filtering and Web Access Management features. DenyAll's ability to innovate is enhanced by the ongoing integration of these technologies.

Our flagship WAF products, **rWeb** and **i-Suite**, will continue to evolve and be supported over the long run. They will gradually come to share the same components, and DenyAll will eventually maintain a unified platform. For now, the focus is on delivering tangible improvements to both WAFs in coming quarters. The cross-pollination process will see DenyAll's Dynamic Application Security Testing (DAST) tool integrated with i-Suite and an intelligent Web SSO interface added to rWeb, among other things. These and future innovations will be delivered through incremental patches, requiring no migration.

- Modular architectures and APIs
- Advanced filtering
- Flow-based policy
- Web SSO and vulnerability assessment

DenyAll masters the key technologies required to turn application security into shared services which meet the growing demand for simplicity combined with security effectiveness.

### 2.3 Delivering Next Generation Application Security

Traditional, linear filtering techniques based on signatures and endless learning phases are not up to the task of securing modern applications. Effective application security requires a paradigm shift towards intelligent filtering, based on identifying the nature of the requests and taking the context of users and their actions into consideration. DenyAll's Next Generation Application Security solutions will offer the following capabilities:

- Automatically discover unprotected applications, profile them, identify their vulnerabilities and provision ad hoc policies, to ease the burden of administrators.
- Use grammatical analysis and sandboxing technologies to identify the nature of incoming requests, ahead of eventually interpreting their content, in order to block complex attacks and evasion techniques.
- Analyze user behavior and evaluate user reputation to detect and block abnormal activity.
- Ensure in-session browser security to prevent compromised devices from becoming attack vectors.
- Automatically scale as demand grows, using APIs and workflow management technology.

### 2.4 Leveraging the Cloud

Both rWeb and i-Suite are available on the cloud platforms of Amazon and Microsoft (Azure). We are also working with select cloud providers to ensure their OpenStack platforms can host DenyAll WAFs and offer application security as valued-add service to their customers.

A new WAF-as-a-service, powered by DenyAll's proven technology, is currently in beta phase at [www.cloudprotector.com](http://www.cloudprotector.com). A cloud-native solution, it delivers unprecedented levels of simplicity and security performance for professional bloggers, small business owners and line of business teams willing to secure their web applications and the data it hosts, without necessarily having the skills to administer a full-blown professional WAF. Test-drive it for free today!



NEXT GENERATION APPLICATION SECURITY

**Germany**

An der Welle 4  
D-60322 Frankfurt  
Deutschland

Tel: +49 (0)6233 66 75 39  
Fax : +49 (0)6975 93 82 00

**Montpellier**

501 rue Denis Papin  
34000 Montpellier  
France

Tel: +33 (0)1 46 20 96 01

**Headquarter**

6 avenue de la Cristallerie  
92310 Sèvres  
France

Tel : +33 (0)1 46 20 96 00  
Fax : +33 (0)1 46 20 96 02

Email : [info@denyall.com](mailto:info@denyall.com)

[www.denyall.com](http://www.denyall.com)