Press release
Paris, July 16, 2015

DenyAll recognized by Gartner as visionary WAF vendor

DenyAll is positioned in the visionaries' quadrant in the second revision of Gartner's Magic Quadrant for Web Application Firewall (WAF), published yesterday. DenyAll's Next Generation WAF sets the stage for more innovation, centered on user reputation and security efficiency.

In the new edition of the Magic Quadrant for Web Application Firewalls, published yesterday, the leading market analyst firm identified DenyAll as one of the most innovative vendors in a fast growing market. DenyAll is one of two vendors in the visionaries' quadrant.

This confirms the recognition the company has been receiving from customers and partner around the world. Upcoming innovations are centered on evaluating user behavior in context and increasing WAF effectiveness, two of DenyAll's key competitive advantages today.

Users are the new perimeter

Controlling how applications are being accessed and used by people, whether 'insiders' (empoyees) or 'external' contributors, such as customers, partners and suppliers, is essential to effectively securing modern IT. In a Web-enabled and mobile world, the network perimeter doesn't mean much anymore. Understanding what users are doing with the rights they have been granted is the key to successfully preventing attacks targeting the data, brand and reputation of organizations.

In addition to preventing application-layer attacks, such as injections and scripts, modern WAFs must include behavior analysis capabilities, to identify bots and block valid, yet malicious user actions, potentially resulting in denial of service or data leakage incidents. WAFs must also be able to take into account the context of the user's actions, such as geolocation, time, device or reputation of the IP address. These can indeed help make more effective decisions from a security perspective.

The next frontier though is to make decisions based on the level of trust the organization has in the users connecting to its systems. That confidence may vary depending on profiles and it may fluctuate over time, depending on how people actually use the apps and services. Any deviation from normal behavior may not be a security issue, but it may require additional vigilance. During such as period, it may be a good idea to restrict the level of access granted to a user, in a specific context. Any definitive wrong doing should be stopped, logged and further investigated. Upcoming releases of DenyAll's NextGen WAFs will include a user reputation scoring mechanism, which will increase the relevance of WAFs in the fight against online fraud and identity theft.

WAF efficiency requires new approaches

DenyAll has been advocating that efficiency is the real measure of the quality and value of application security tools, such as WAFs. The company takes pride in delivering time-tested products, used by customers to filter live, often mission critical web applications and services, thus effectively protecting IT systems from real-world attacks, without generating false positives.

A new breed of products is required to meet that challenge. The basic negative and positive security technologies used in first generation Web Application Firewalls and Application Delivery Controllers are ineffective. Application-layer attacks can be written in so many different ways, it is impossible to

rely solely on a set of signatures. Even smarter, generic signature systems can be bypassed. The risk of blocking legitimate requests is such that some customers – especially in North America, a market DenyAll hasn't fully invested in yet – shy away from using WAFs in blocking mode, using them instead as mere intrusion detection systems. Web application learning and white listing remain quite effective techniques, if one can afford to re-train the WAF every time new versions of web applications and web services are released. This is not exactly practical in agile environments, where DevOps teams attempt to optimize code quality and time to market.

DenyAll's Next Generation WAFs are ahead of competition in both ease of administration and security, the two functional areas which impact WAF efficiency. A visual, workflow representation of policy is an innovative breakthrough from a usability and productivity perspective. Combined with the industrialization capabilities provided by APIs', it ensures a reduced cost of ownership. When it comes to the ability to block modern day attacks and counter evasion techniques, DenyWall WAFs use alternative techniques, providing administrators with choice and the ability to customize policies based on the exact nature and importance of the applications they seek to protect. For example, content interpretation combined with a field-tested and fully customizable weighting mechanism, blocks known and unknown attacks, while limiting the occurrence of false positives. Advanced engines use grammatical analysis and sandboxing techniques to identify real-world attacks and avoid blocking legitimate requests that embed words that would have been identified as attacks by traditional filters. These approaches are essential when protecting modern web applications, where application logic can be complex, requests can embed comments or be encoded.

About DenyAll
DenyAll is a software vendor and an expert in application security. Building on 15 years of experience securing web applications and services, the company keeps on innovating to meet the needs of organizations of all sizes, worldwide. Its products **detect** IT vulnerabilities, **protect** infrastructures against modern attacks targeting the application layer and **connect** users to the applications which allows them to create and share information. The company leverages an ecosystem of value-added resellers, outsourcers, hosters and cloud providers. A member of the Hexatrust alliance, DenyAll partners with other vendors to deliver innovative, integrated solutions. Look for more information on www.denyall.com.

About the Magic Quadrant
Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Press contacts:		
Oxygen	**Kafka Kommunikation**	**DenyAll**
Laure Mazzesi / Tatiana Graffeuil	Ursula Kafka	Stéphane de Saint Albin
Tél. : +33 1 41 11 37 77	+49 89 747470-580	Tél. : +33 1 46 20 96 21
charlinek@oxygen-rp.com	info@kafka-kommunikation.de	sdesaintalbin@denyall.com
www.oxygen-rp.fr		www.denyall.com