

Leading Analyst Firm report on WAF market highlights trends that play to DenyAll's competitive advantage

A Competitive Landscape published on June 29, 2012, highlights some key trends in the Web Application Firewall market. The report points out the importance of Web fraud detection and browser security, the need for event correlation and continued innovation.

The [Gartner report](#), Competitive Landscape: Web Application Firewall Market, Worldwide, 2012, suggests that a combination of preventive and defensive measures is required to protect an IT infrastructure from application-layer attacks, beyond what is dictated by PCI DSS or HIPAA. Organizations investing in developer training and source code analysis, performing regular penetration tests and deploying Web Application/Services Firewalls are more likely to prevent web fraud, denial of service and data leakage than those who don't.

Extending the perimeter to connecting browsers

Even in such a context, connecting browsers are weak components of the infrastructure. Many users connect to Web applications from a potentially insecure client. Be it a PC, tablet or smart phone, the device may be infected by a key-logging malware, capturing all session data and sending it to botnet controllers, such as Zeus or Spyeeye.

Here's what [Gartner's report](#) reads on the subject: *"Web fraud in the financial sector and mobile applications, combined with the adoption of the bring your own device (BYOD) concept, has highlighted customer interests in WAF technology extensibility to the endpoint device. Some WAF products now provide additional client-side browser evaluation and malware detection capabilities and are driving interest in their technology. This is achieved by injecting client-side specific code, such as Java or ActiveX, to inspect or protect the browser and Web session."*

DenyAll's Client Shield extends the application security perimeter to connecting browsers, preventing "Man-in-the-Browser" attacks from compromised clients. By triggering the launch of a new browser window and controlling its safe execution, rWeb's Client Shield ensures that a valid SSL authenticated connection will not be used by resident malware to reach, capture or destroy data hosted by the protected application. DenyAll is the only WAF vendor to offer such an innovative approach.

Innovation to advance web protection capabilities

Gartner recommends that WAF vendors keep innovating to differentiate vs. Application Delivery Controller vendors and defend against future competition from services offered by Content Distribution Network companies. DenyAll believes that its security expertise and ability to innovate are key differentiators. As an example, the company advocates that a new breed of security engines is required, which natively understand modern languages and new content types used in Web 2.0 applications, and can dynamically filter them in spite of their embedded and cascading nature (SQL within JSON within HTTP, for example).

The DenyAll Application Security Platform (DASP) is the foundation on which DenyAll has been delivering innovative security technologies. Among those, a set of XML/SOAP-specific security features, a User Behavior Tracking module, and a unique Scoring engine. The latter performs an agnostic analysis of the data and identifies unknown threats while minimizing false positives, thanks to a field-tested weight calculation technique. New security modules will be added to the platform shortly, which canonize complex data structures in order to perform an in-depth analysis.

Moving towards Application Security Intelligence

DenyAll shares Gartner's perspective that the correlation of application security events and its presentation to the right decision makers is needed to raise "context awareness" and help organizations manage application-layer attacks more effectively. Application security intelligence will ensure that all stakeholders become aware of the issues as soon as they arise and can cooperate in their resolution. DenyAll recently announced a Splunk-based Application Security Dashboard which will be a great operational foundation for enabling that information sharing. The upcoming integration of DAST scan results into DenyAll's platform will also contribute to the realization of that vision.

More information

The report also includes a profile of key vendors, and highlights some of DenyAll's key differentiators. DenyAll invites its customers and partners to read the report, or purchase it if they are not Gartner customers, at <http://www.gartner.com/resId=2067715>.

About DenyAll:

DenyAll is an innovative software leader in the growing application security market. The company was one of the pioneers in the Web Application Firewall market. Building on +10 years of experience securing and accelerating large customers' Web, XML and FTP application-layer flows, DenyAll keeps innovating to respond to the needs of organizations of all sizes. Against modern threats, its products protect transactional Web sites, the Web front-ends of critical applications, Web Services-based custom applications, as well as social and collaborative tools, both in traditional and SaaS/cloud environments. DenyAll's firewalls leverage the DenyAll Application Security Platform (DASP), a modern and modular platform based on proven reverse proxy technology. The company builds an ecosystem of partners, distributors, integrators, outsourcers and application hosters, and works with other vendors to offer comprehensive solutions, dedicated to securing and accelerating modern applications. More information can be found on www.denyall.com.

Press contacts:	
OXYGEN Tatiana Graffeuil / Sandrine Mahoux Tél. : +33 1 41 11 37 89 tgraffeuil@oxygen-rp.com www.oxygen-rp.fr	DENYALL Stéphane de Saint Albin Tél. : +33 1 46 20 96 21 sdesaintalbin@denyall.com www.denyall.com