

DenyAll enables faster, virtual patching of application vulnerabilities

A new commissioned study conducted by Forrester Consulting on behalf of DenyAll highlights the benefits of application vulnerability patching in terms of scalability and timely response to modern threats. Virtual patching is at the heart of DenyAll's integration strategy between its Web Application Firewall and Dynamic Application Security Testing tools, delivered through new releases of its Protect and Detect product lines. New security engines in DenyAll rWeb 4.1 feature pack 1 also deliver unprecedented levels of protection against modern attacks.

A new Forrester survey highlights important application security trends

In the first quarter of 2013, DenyAll commissioned Forrester Consulting to conduct a survey of 50 European organizations (based in Germany, UK and France) regarding their approach to securing web applications. The report highlights the following:

- Because of security expertise and time to market pressures, **only 40%** of organizations say that they have **mature and extensive application security processes**;
- **Developer training** is perceived by **60%** as being a long term proposition, unable to ensure code security in the short term, or not sufficient in itself;
- Web Application Firewalls (WAFs) are the most popular mechanism for securing applications, with **75% of respondents having deployed or planning to deploy WAFs** in the near term.

The survey shows that application security professionals assign the following benefits to WAFs: effective protection against application-layer attacks, scalability, and the ability to patch application vulnerabilities faster, thanks to the integration with Dynamic Application Security Testing (DAST) tools. The full report will be available on the DenyAll website (www.denyall.com) shortly.

An innovative solution for patching application vulnerabilities

Application virtual patching is the process by which WAF settings are modified based on the outcome of a vulnerability scan, to prevent vulnerabilities from being exploited until they can be fully remediated (through code changes or system patches, for example). Virtual patching can drastically reduce the period of time during which sensitive data is exposed to potential attacks.

Since the acquisition of VulnIT in the summer of 2012, DenyAll has been working to combine its WAF and DAST technologies. Newly released products, **DenyAll rWeb 4.1 feature pack 1 (FP1)** and **DenyAll Detect 5.1**, together represent a first step towards the delivery of the integrated application security solution envisioned by the company.

This solution is the first to deliver granular policy adjustment recommendations, helping administrators save time and make decisions that match their organization's priorities. Scan reports can be easily exported from the DenyAll Detect products, and imported into rWeb. From there, the WAF presents the administrator with security policy modification choices. There can be several options, depending on the vulnerability and on the organization's priorities: minimizing false positives, maximizing security or maximizing performance.

Advanced Detection Engines improve protection of modern applications

With feature pack 1, all DenyAll Protect products take advantage of various enhancements and new features, such as log compression, syslog forwarding and a scheduler, for task automation. rWeb 4.1 FP1, the most comprehensive member of this product line, also includes the virtual patching capability and a new group of security engines. These **Advanced Detection Engines** were designed to defeat WAF evasion techniques, improve protection against modern attacks and the security of applications based on new languages. They include:

- A new approach to SQL injection protection based on grammatical analysis of submitted data;
- A scripting language injection detection engine, protecting against nested blocks in Java, PHP, SSI (Server Side Include) and JavaScript;
- Protection against HTTP Response Splitting;
- The ability to identify and block XSS attacks in HTML4/5 tags and attributes;
- Advanced protection against directory traversal confusion attempts.

Improved automation in DenyAll Detect 5.1

DenyAll's vulnerability scanners keep evolving to meet customer demand. The latest 5.1 release of DenyAll Vulnerability Manager includes new features focused on improving asset management, team delegation and performance:

- **Asset management:**
 - Auto-grouping classifies assets based on predefined criteria,
 - One-shot analysis can be launched directly from the inventory, or tickets,
 - Gap analysis reports show how the organization is improving over time.
- **Team delegation** and segregation of duties:
 - Groups of users can be created, that relate to specific groups of assets,
 - A new delegation model allows specific assets and tasks to be assigned to specific people, which is important in larger organizations and hosted environments.
- **Performance:**
 - Improved OpenVAS startup performances,
 - New password triviality test for white box scans on Unix and DBMS,
 - New taskbar notifying the user when a scan is running in the background.

Upcoming Webinars

For more information on rWeb 4.1 FP1's Advanced Detection Engines and DenyAll's virtual patching solution, join the **April 23** Webinar. You can also join the next 'CTO Talk' Webinar focused on HTML5 security issues, on **May 29**. Register here: http://www.denyall.com/news/events_en.

About DenyAll

DenyAll is an innovative leader in the application security market. The company was one of the pioneers of the Web Application Firewall market in Europe. Building on 15 years of experience securing and accelerating web applications and services, DenyAll innovates to respond to the needs of organizations of all sizes. Its products detect IT vulnerabilities and protect infrastructures against application-layer attacks. DenyAll builds an ecosystem of expert security partners, outsourcers and cloud providers, and works with other vendors to offer comprehensive solutions, dedicated to securing and accelerating applications. More info on www.denyall.com.

Press contacts:		
Oxygen Marion Avranche / Tatiana Graffeuil Tél. : +33 6 87 83 97 58 mariona@oxygen-rp.com www.oxygen-rp.fr	Kafka Kommunikation Ursula Kafka +49 89 747470-580 info@kafka-kommunikation.de www.kafka-kommunikation.de	DenyAll Stéphane de Saint Albin Tél. : +33 1 46 20 96 21 sdesaintalbin@denyall.com www.denyall.com