

▼ **Armorize CodeSecure™ Integrates with art of defence hyperguard to Protect Against Zero-Day Attacks and Crimeware**



Santa Clara, September 22, 2008

In the face of increasingly complex zero-day attacks against web applications, Santa Clara-based Armorize Technologies and art of defence (AOD) from Germany have developed an innovative approach to web security.

Armorize CodeSecure™ pinpoints the root cause of web application vulnerabilities while the AOD hyperguard Web Application Firewall (WAF) specifically blocks exploits targeting these weaknesses at the web application perimeter. By integrating their flagship products, these industry leaders have provided a means for enterprises to address web application security throughout the system life cycle.

The New Attack Paradigm - Drive-by Downloads

This year has seen a rise in the number of zero day attacks targeting web applications. With increasing frequency, attackers are compromising web sites and directing them to attack the end-user computers browsing them. This new paradigm, supported by research from the Google Malware Analysis Team[1,2] has resulted in increased “drive-by downloads” and has been adopted by organized crime worldwide. This research points to a significant rise in the number of web pages containing malware designed to steal information from the end-user.

Since January of 2008, there have been coordinated mass-SQL injection attacks emanating from computers in China[3]. Utilizing complex Google queries, attackers locate vulnerable websites, injecting them with malware which then targets client operating systems and web browsers. The result is theft of information such as stored passwords, banking details, and personal or corporate data.

The generation rate of new attacks makes it extremely difficult to protect web applications through signature-based means such as Antivirus, etc. Instead, it is crucial to ensure that applications are built securely from the outset based on code that is resistant to exploits such as Cross Site Scripting (XSS) and SQL Injection.

Secure Web Development with CodeSecure™

Armorize CodeSecure™ provides the integrated secure coding environment necessary to ensure that web applications are not vulnerable to attacks. This web-based, automated static source code analysis and verification platform analyzes Java, PHP, ASP and .NET web application source code, detecting vulnerabilities and offering guidance on remediation.

As an appliance-based solution, CodeSecure™ ensures minimum installation and configuration overhead with maximum scalability across the enterprise.

By deploying CodeSecure™ early in the Software Development Life Cycle (SDLC), vulnerabilities are identified, understood and remedied by the developers with minimal cost and impact on project progress.

▼ **Armorize CodeSecure™ Integrates with art of defence hyperguard to Protect Against Zero-Day Attacks and Crimeware**



Secure Web Operations with hyperguard Web Application Firewall (WAF)

CodeSecure™ is also extremely useful in locating vulnerabilities in already-deployed web applications. However, remediation steps such as rewriting code may not always be practical due to resource constraints and an unwillingness to take running applications offline. hyperguard offers the perfect solution for this situation.

Hardening and regulating access to web applications, hyperguard protects against attacks such as XSS and SQL Injection that network and system-level security controls typically miss.

A host-based solution, hyperguard is installed as a software plug-in on the web server facilitating rule creation on a page or application-specific basis. Unlike appliance-based WAF solutions, it does not introduce a single point of failure or bottleneck which can be detrimental for complex web services environments.

By integrating with CodeSecure™, hyperguard can be fine-tuned to protect vulnerable applications. Importing the source code analysis results from CodeSecure™, hyperguard dynamically modifies its rules to explicitly block attacks targeting the vulnerabilities identified in the source code analysis process. This integration offers customers a choice in remediation, ensuring optimum protection with zero down-time and minimum cost.

CodeSecure™ and hyperguard integration in practice

art of defence and Armorize clients are already seeing the benefits of this integration. Where code-level vulnerabilities leave the enterprise open to attack, businesses can now choose whether to remediate through code modification or to immediately mitigate risk by deploying specific application firewall controls to protect not only the vulnerable application but also the specific vulnerable page.

For clients seeking compliance with the Payment Card Industry (PCI) standard, web application security is mandatory. Specifically, under Requirement 6.6[4], web-facing applications must undergo source code analysis or be protected by a WAF. While the high-level PCI standard offers this as a choice, the detailed information supplement[5] states that the web application should be protected by a combination of these technologies.

By deploying CodeSecure™ and hyperguard, our clients have chosen an integrated solution that provides dual protection for their web applications, ensuring minimum exposure to attack and a cost-effective strategy for compliance.

About Armorize Technologies

Armorize Technologies is a leading provider of next-generation Web Application Security Solutions. From static source code analysis with CodeSecure™ to dynamic malicious code detection with HackAlert™, Armorize's award-winning solutions are the culmination of years of research and innovation.

Led by numerous internationally acclaimed security veterans and financed by top Silicon Valley investors, Armorize was formed in 2005 with its headquarters in Santa Clara, CA, and its R&D center in the Nan Kang Software Park in Taipei, Taiwan. Armorize has a global customer base with clients from among financial, telecom, government and technology sector leaders.

For more information, visit <http://www.armorize.com>.

▼ **Armorize CodeSecure™ Integrates with art of defence hyperguard to Protect Against Zero-Day Attacks and Crimeware**



About art of defence

art of defence (AOD) is the only European provider of software to secure web applications over their entire life cycle. Leading banks, financial service providers and e-commerce businesses rely on art of defence to protect their internal and external web applications, ensuring compliance with legal requirements or industry standards such as the Payment Card Industry Data Security Standard (PCI-Compliance).

hyperguard, the company's second generation Enterprise Web Application Firewall (WAF), protects web applications in operation. The software blocks illegal access to the application database back-end and operating systems with critical company, customer and product information - even during transactions, when systems are open and vulnerable to attacks.

For more information, visit <http://www.artofdefence.com>

Contact:

Armorize Technologies
John Linehan
Phone: +1-408-216-7893 ext 401
Email: info@armorize.com

art of defence
Dr. Georg Hess
Phone: +49 (0) 941 604 889 58
Email: presse@artofdefence.com

References

- [1] The Ghost in the Browser, Neils Provos et al [May 2007];
http://www.usenix.org/events/hotbots07/tech/full_papers/provos/provos.pdf
- [2] All Your iFrames point to us, Neils Provos et al [February 2008]
<http://research.google.com/archive/provos-2008a.pdf>
- [3] Mass SQL injection attack hits Chinese Web sites, IDG News Service [May 19, 2008]
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9086658&source=rss_news50
- [4] Payment Card Industry (PCI) Data Security Standard, Version 1.1, Requirement 6.6 [September, 2006]
https://www.pcisecuritystandards.org/security_standards/download.html?id=pci_dss_v1-1.pdf
- [5] Information Supplement: Requirement 6.6 Code Reviews and Application Firewalls Clarified [April 15, 2008]
https://www.pcisecuritystandards.org/pdfs/infosupp_6_6_applicationfirewalls_codereviews.pdf