

Cool Vendors in Application Security, 2010

Ray Wagner, Joseph Feiman, Neil MacDonald, John Pescatore, Earl Perkins

Technological advances in application security continue to move very rapidly — in some cases, outpacing the market's ability to adopt and integrate them. Nonetheless, information security professionals, application developers and other stakeholders should consider the innovations offered by Gartner's 2010 Cool Vendors as a way of understanding the directions application security may take in the future. For Gartner's Cool Vendor selections in three other important security market segments, see "Cool Vendors in Cloud Security Services, 2010," "Cool Vendors in Data and Infrastructure Protection, 2010" and "Cool Vendors in Identity and Access Management, 2010."

Key Findings

- Many of this year's Cool Vendors in application security offer highly advanced technologies — in some cases, technologies that are well ahead of the market. These offerings are not necessarily appropriate for all enterprises or all implementations. They are likely to be suitable for Type A Gartner clients (technologically sophisticated early adopters), but much less so for more-risk-averse Type B or Type C clients.
- A recurring theme among the technologies provided by the 2010 Cool Vendors is the attempt to find new ways to meet the challenges of a rapidly evolving threat environment, including sophisticated, targeted attacks.

Recommendations

- Consider innovative products and services — including those from Gartner's 2010 Cool Vendors — when considering solutions to address application security strategies and requirements.
- Don't base product or service implementation decisions for application security or any other security-related area on technological innovation alone. Consider real-world workability, cost-effectiveness and enterprise-specific requirements, in addition to vendor capability and viability, as key selection criteria.

TABLE OF CONTENTS

Analysis	3
1.0 What You Need to Know	3
2.0 ActiveBase.....	3
3.0 Checkmarx	4
4.0 Engiweb Security	4
5.0 HBGary.....	5
6.0 Mykonos Software	6

ANALYSIS

This research does not constitute an exhaustive list of vendors in any given technology area, but rather is designed to highlight interesting, new and innovative vendors, products and services. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

1.0 What You Need to Know

Application security technologies continue to change rapidly — more rapidly, in fact, than in many other areas of information security — in response to changes in application development models and the threat environment. Many of the Cool Vendors Gartner has identified in application security for 2010 address niche markets or are, otherwise, not yet ready for widespread market adoption. Nonetheless, chief information security officers (CISOs) and other security decision makers need to familiarize themselves with the emerging technologies and approaches presented by Gartner's Cool Vendors and other leading-edge providers. These vendors and their technology offerings offer, at minimum, an important set of indicators of possible future directions for application security.

2.0 ActiveBase

Ramat-Gan, Israel; and Phoenix, Arizona (www.active-base.com)

Analysis by Joseph Feiman

Why Cool: ActiveBase is one of the pioneers of an emerging dynamic data-masking technology.

Data masking is not just another form of data manipulation, but rather an essential part of the testing and operation phases of the software life cycle. Data masking, which can be static or dynamic, aims to prevent the abuse of sensitive data by hiding it from users. This is accomplished by such techniques as replacing some fields with similar-looking characters, replacing characters with masking characters (for example, "X"), replacing real names with fictional names and reshuffling data in database columns.

Static data masking — the only approach offered by most vendors — primarily aims to deter the misuse of data by users of test databases (typically programmers, testers and database administrators) by masking data in advance of testing. Dynamic (real-time) data masking typically masks data in production databases (for example, from client service personnel working in credit-card call centers).

ActiveBase's dynamic data-masking technology installs on a relational database management system (RDBMS) server or a dedicated server, becoming the RDBMS' listener port. All traffic to the RDBMS passes through it, enabling traffic analysis and modification. ActiveBase intercepts SQL SELECT requests from RDBMS' clients, analyzes clients' access and role entitlements, and modifies requests so that they return to the requestor's data records with masked sensitive fields. The result is that database users can access only those data fields that they are entitled to.

This technology does not require any changes in applications that access the database, or to the database itself. A caching mechanism minimizes performance effects.

Challenges: ActiveBase dynamically masks only relational database data. The company should add support for nonrelational data sources, such as Virtual Storage Access Method and queued sequential access method on mainframes.

Who Should Care: Business data owners, chief security officers (CSOs), CISOs, compliance officers, auditors and other enterprise decision makers concerned about the security of their sensitive data should consider ActiveBase.

3.0 Checkmarx

New York, New York; and Tel Aviv, Israel (www.checkmarx.com)

Analysis by Joseph Feiman

Why Cool: Checkmarx is a vendor of static application security testing (SAST) technology. The Checkmarx product's key distinction is that it converts programming languages' code into a single common-language format and holds it in persistent storage. That storage makes an application security intelligence repository, which enables repeatable queries and impact analysis.

There is no need to run additional application tests if the applications have not changed. Applications can be tested for vulnerabilities to new attacks simply by modifying queries with patterns from new attacks.

Queries, unlike traditional reports, enable specific answers to specific questions. They can be run across information on multiple applications, and can have security, business and compliance context. This is a step beyond the current common security testing approach, which is based on the execution of repeatable security tests that produce reports with limited search capabilities and limited analysis capabilities.

Checkmarx's approach simplifies parallel analysis of fragmented, distributed composite applications, making it suitable for outsourced and crowdsourced application security testing and emerging cloud-based security testing. Checkmarx analyzes code written in Apex (used by salesforce.com), Java, Ajax, C#, Visual Basic and ASP, and it has an early release for C and C++ analyses.

Checkmarx mainly sells software security testing services through a security-testing-as-a-service business model, but it also offers product licenses. Checkmarx technology uses proprietary repository and proprietary query language.

Challenges: Checkmarx needs to increase its name recognition — namely, by gaining more clients. The company should also increase offering its analyzer as a product, not only as a service.

Checkmarx's position as a thought leader would be even stronger if it offered a standard repository (for example, RDBMS) with a standard query language (for example, SQL).

Who Should Care: The Checkmarx approach should interest CSOs, CISOs, compliance officers, internal auditors and application security, development and maintenance specialists. Software vendors and service providers concerned about product security should also investigate Checkmarx's offerings.

4.0 Engiweb Security

Rome, Italy (www.engiweb.com)

Analysis by Earl Perkins

Why Cool: European identity and access management (IAM) vendors have been experiencing something of a renaissance, particularly in entitlement life cycle management (role and entitlement management). Engiweb Security — a privately held vendor founded in 2001 by the

Italian system integrator, Engineering Ingegneria Informatica — has delivered products that can best be described as an "entitlement-aware" platform for configuring an entitlement life cycle environment. In the hands of knowledgeable enterprises or skilled system integrators, Engiweb solutions can deliver detailed, granular role and entitlement administration, and entitlement resolution functionality.

Engiweb's Identity and Access Management Suite (IDEAS) solution straddles the role life cycle and entitlement management markets, with features of each, and provides a detailed development and configuration environment to link these features to compliance requirements, particularly in SAP applications. The product provides some provisioning and privileged user management functionality as well. The Engiweb team is highly skilled and has published a number of detailed academic papers for the security community on the conceptual model used in the IDEAS solution.

Challenges: Engiweb does face some challenges. Some functionality is possible straight out of the box, but IDEAS is primarily an IAM development environment, best used in the hands of system integrators or capable clients that can establish a model for authorization in an existing IAM deployment. It does have functional capabilities that span several products within the traditional IAM market, which makes marketing to potential clients a challenge, particularly when trying to compare with role management or entitlement management competitors. However, the company does understand the key deficiencies in the IAM market today, and is taking technology steps to give clients a chance to take their IAM solutions to the next level, as a business enabler.

Who Should Care: Enterprises that have evaluated entitlement life cycle management tools (both role life cycle and entitlement) from existing IAM vendors and found them inadequate for their needs will be interested in evaluating Engiweb IDEAS. Gartner recommends that developers and security specialists validate IDEAS' capabilities in IT security architecture.

Recommended Reading:

"Adaptive Access Control Emerges"

"Entitlement Life Cycle Management: Authorization through Entitlement Resolution"

"Entitlement Life Cycle Management: The Evolution of Role Life Cycle Management"

5.0 HBGary

Sacramento, California (www.hbgary.com)

Analysis by John Pescatore

Why Cool: For several years, the most damaging attacks have used targeted custom malware that evades traditional antivirus and Web security gateway controls. HBGary provides a set of products for analyzing executables and system configurations to detect, inspect and analyze advanced malware, based on its patent-pending Digital DNA technology. The company's Responder platform offers advanced tools for preserving and analyzing system to memory to detect and investigate compromises. Other products provide software agents to place on critical servers and PCs to limit the impact of malware and preserve runtime forensic information. The combination of these capabilities can provide visibility into target attacks, botnet compromises and other forms of what the U.S. Department of Defense (DoD) now calls "advanced persistent threats."

Challenges: Malware analysis tools require deep expertise and continual use to be effective. The enterprise market for such "lean-forward" approaches is limited and — much like the overall digital forensics market — dominated by the DoD and other government agencies. Another

challenge is presented by dynamic and static analysis software testing tools. These more-general-purpose tools do not provide the same capabilities as HBGary, but they could evolve to meet mainstream market needs. Larger security firms with significant threat research and reverse-engineering teams could also offer products to compete with HBGary at the high end of the market.

Who Should Care: HBGary's technologies should interest consulting service providers that perform incident response and forensic engagements, and high-security-profile enterprises that have the budget and personnel necessary to take a proactive approach to targeted malware.

6.0 Mykonos Software

Burlingame, California (www.mykonossoftware.com)

Analysis by Neil MacDonald

Why Cool: Mykonos Software officially came out of "stealth mode" in 2Q09 with an Ajax framework for developing and operating secure Web 2.0 applications (specifically, Ajax-enabled applications). Ajax applications, like other Rich Internet Applications (RIAs), place a significant amount of code onto end-user machines. This code, like all arbitrary executable code, may be malicious or may have been tampered with. To address this problem, the Mykonos Ajax development framework supports encryption and digital signatures all the way down to the component layer to ensure that the application code has not been tampered with (directly or via code insertion). The Mykonos framework focuses on enterprise — not consumer — applications, and requires changes to the application and plug-ins at the application server to support its increased security.

The Mykonos framework brings stronger security to Ajax applications, but changes to the applications are required. To address the problem of applications that can't be changed, and using its expertise in protecting vulnerable applications, Mykonos developed an innovative physical and virtual appliance-based implementation called the Mykonos Security Appliance, which it delivered early in 2010. The Mykonos Security Appliance functions as an in-line gateway-based solution to shield potentially vulnerable Web applications. The application-level gateway is conceptually similar to a Web application firewall (WAF) and can protect from the Open Web Application Security Project's top 10 application security flaws. Optionally, the gateway can deliver counterhacking capabilities by injecting code (like a honeypot) into the application tier and dynamically changing how the application interacts with a hacker to track how the hacker is trying to inspect the site. The gateway can also implement more-active response measures that extend well beyond traditional firewalling, including the ability to "fingerprint" individual hackers based on patterns of attack.

Challenges: Mykonos faces multiple challenges:

- The company's original framework approach required changes to applications and plug-ins at the application server to work, which slowed market adoption.
- Attacks on Ajax haven't yet caused significant damage, so doing nothing remains an option. Moreover, Ajax development tools and frameworks will likely come to support stronger security capabilities, including component-level digital signatures and tamper protection, over time, potentially reducing the need for the Mykonos framework.
- The Mykonos framework is focused on Ajax Web 2.0 RIAs, and needs a similar value proposition for Adobe Flash and Microsoft Silverlight applications.

- The Web application protection and counterhacking capabilities of the security appliance overlap conceptually with the WAF approach, and Gartner expects WAF vendors to extend their capabilities to include the ability to alter responses to attacks using code injection techniques.
- Enterprises may be reluctant to use security services from a lesser-known provider such as Mykonos.
- The buying center for Mykonos' solutions is ideally the head of the application security team, but not all enterprises have designated such a role or team. In these enterprises, Mykonos's offering spans buying centers — sometimes including IT security and application engineering — making targeting more difficult.

Who Should Care: IT security professionals looking for innovative ways to secure their internally developed Web 2.0 Ajax applications and infrastructure should consider the Mykonos framework. To secure existing or third-party Web applications, they should consider the Mykonos Security Appliance solution for protection from attacks on vulnerable applications, as well as to deliver insight into hacker behavior, or pressure their WAF vendors to deliver counterhacking capabilities as well.

REGIONAL HEADQUARTERS

Corporate Headquarters

56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters

Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters

Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters

Gartner do Brazil
Av. das Nações Unidas, 12551
9º andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509