

# An Application Security Strategy Guide

---

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper  
Prepared for Cenzip

February 2009



IT MANAGEMENT RESEARCH,  
INDUSTRY ANALYSIS AND CONSULTING

## Table of Contents

Introduction .....	1
Education.....	1
Application Assessment.....	2
Application Monitoring.....	4
What Works.....	5
About Cenzip .....	5

## Introduction

Attacks, incidents and compliance regulations, in combination with difficult-to-automate processes, a steep learning curve, and highly charged political environments, are only a few of the factors that have made application security possibly the most difficult to address aspect of a security strategy. Indeed, application developers as well as security practitioners are struggling within this arena, while malicious attackers thrive unabated from application security failures. One primary difficulty is that ensuring application security requires a higher level of understanding and knowledge than many other aspects of a security strategy.

While the definition of this difficulty may be simplistic in nature, the complexities that it creates in both the security process cycle and the software development lifecycle (SDLC), including applications going through development or quality assurance and the existing deployed applications, are anything but simple. In fact, compliance measures that attempt to simplify exactly what is needed to ensure application security often leave organizations who abide by those compliance measures vulnerable and insecure. In many ways, application security has shown that a compliant organization may not be the equivalent of a secure one.

Of course, this begs the question, “How does an organization address application security in a manner that both complies with regulations and secures its applications?” Unfortunately, there is no widely accepted assessment, monitoring, or auditing model that professionals can use as simply as a checklist. Moreover, the dynamic threats and vulnerabilities faced by applications often require the teamwork and collaboration of multiple departments within an organization.

It is imperative for organizations who attempt to solve application security issues to engage multiple stakeholders in an effort to create a security aware culture.

For this reason it is imperative for organizations who attempt to solve application security issues to engage multiple stakeholders in an effort to create a security aware culture. Within this culture, each stakeholder must have a vested interest in securing and protecting Web applications. The difficulty in this strategy is selecting the proper technology that can be utilized as a catalyst to cultivate the culture necessary to not only create more secure applications in development, but to also remediate the security issues within the production environment.

This ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) white paper is meant to serve as a summary guide for decision-makers who must address the challenges of application security. The pain points and issues surrounding a lack of understanding in application security are examined. This is followed by a discussion of how assessment technologies can be utilized as a catalyst to create better understanding of application security issues as well as enhance the capabilities of other security countermeasures.

## Education

It is impossible to discuss application security strategies without first addressing the issue of education. Gaining the necessary level of understanding and expertise is a primary challenge for organizations in implementing application security programs. Application security challenges are amongst the most dynamic, complicated, and sophisticated issues that any IT organization will

face. The general lack of understanding within this arena has created a seemingly infinite number of possible targets for malicious attackers.

Complicating matters is the unfortunate reality that the majority of IT security professionals currently come from backgrounds in systems administration or infrastructure architecture. Moreover, most development teams are heavily focused on functionality as opposed to security. This means that security is a mere afterthought for these critical stakeholders in application security.

As a result, security professionals struggle to implement a strategic assessment program or properly monitor application firewall solutions because of an inadequate awareness of the underlying technical issues. Meanwhile, development teams consider security as an afterthought rather than as an integral aspect the Software Development Lifecycle (SDLC)—which, in turn, has resulted in practices such as insecure coding.

Further complicating matters, most security strategies currently rely on security countermeasures that do not fully educate security professionals of the issues about which they are attempting to detect. To the untrained eye, application attacks, especially those detected in typical security countermeasures, often resemble regular application traffic. In some cases, such as cross-site scripting, detection systems will merely catch any anomalous JavaScript statements and sound an alarm. The problem with this type of alarm is that the professional monitoring the application must know its intended use and technical details, such as the application's coding language, well enough to determine if the alarm was or was not a false positive. When the security professional monitoring these issues is not fully educated on the matter, the impact of these alarms is often not fully understood, and as a result, there is no response.

---

Application vulnerability assessment allows organizations to discover their vulnerabilities, educate themselves on the impact of those vulnerabilities, and research the proper solutions to resolve the vulnerabilities they've discovered.

---

## Application Assessment

In situations such as this it is imperative that security teams within an organization possess the proper utilities and capabilities to educate themselves. In many ways, this is the major benefit of application vulnerability assessment. Application vulnerability assessment allows organizations to discover their vulnerabilities, educate themselves on the impact of those vulnerabilities, and research the proper solutions to resolve the vulnerabilities they've discovered.

In this manner, application security assessments are the foundation of the process of addressing application security. However, performing application assessments is no easy task. In fact, application assessments are possibly the most difficult process for a security organization.

The first difficulty is selecting an appropriate assessment methodology. Decisions are often made based on who within an organization is the most vocal evangelist of application security. If the loudest voice comes primarily from a development team, then a “white box” solution for scanning the application from the “inside” (i.e., assessment of the application code itself), is likely to be selected. If the loudest voice comes from a security team—particularly if they are outside the development organization (the most common case) or they have no backing for implementing

security processes into the system development lifecycle—then a “black box” assessment methodology is likely to be used, meaning assessment from the “outside,” or from the user’s perspective as it were, without knowledge of the application system’s internals, hence the “black box” sense of the term.

There are benefits and drawbacks to each methodology. Ideally if the customer has enough budget and resources they should try to implement both technologies. If not, black box testing provides the biggest bang for the buck since it is easier to implement and truly emulates a hacker.

Of course, it must be noted that in terms of creating a culture that engages the interests of multiple stakeholders in an effort to create more security within applications, that black box technology is usually the best bet. In many cases the operation of black box technology is typically not within the responsibility of developers because the assessments are run after the application has been developed. However, the developers are still responsible for the remediation of the actual vulnerabilities found. This means that the teams conducting assessments and the teams responsible for application development need to work collaboratively. A collaborative effort and productive culture can be created by deploying role-based solutions where the information security teams can define expectations while the QA and development teams perform the assessments. Black box solutions (also known as Dynamic Application Security Assessment Solutions) are still an important aspect of the application security assessment process, as the capabilities of these solutions are still needed to assess production applications and function as an auditing utility. One of the shortcomings of black box technologies is that they do not pin-point the exact location within the application code where an error occurs; however, most organizations are able to use the specific url of the vulnerabilities provided by the major black box assessment solutions to trace to the line of code. White box solutions are often needed to catch certain kinds of vulnerabilities early in the cycle; however, due to the effort and resources required to implement these solutions, many organizations are focusing on black box solutions for now. Also, white box testing solutions often do not address security assessment of production applications, which in some cases can be the vast majority of a company’s total application portfolio.

---

Unfortunately, in many instances, even with both white box and some black box solutions in place, many applications will still be vulnerable to dynamic issues that may not have been detected by either scanner.

---

Unfortunately, in many instances, even with both white box and some black box solutions (the ones that take a signature-based approach) in place, many applications will still be vulnerable to dynamic issues that may not have been detected by either scanner. Issues such as logic vulnerabilities and vulnerabilities related to the relationships between an application, users, and databases are only a few examples of where this could occur. This is why manual testing of applications is an essential aspect of an application security assessment. Many companies are starting to use a hybrid approach of using an automated solution, but also using a Software as a Service (SaaS) and a managed service from the same vendor so they can supplement their own resources and also address additional vulnerabilities. While an automated solution will address multiple issues within a small amount of time, it might not fully address the

nuances of each individual application in detail. The primary benefits of these types of solutions are the advantages they offer in addressing the issues of resource drain and a steep learning curve. They will identify many security issues in a specific application—and they must also be kept up-to-date in the face of a continually evolving threat environment. Performing a manual assessment requires a large amount of time and education but can address certain issues like social engineering that cannot be addressed by any automated solutions. .

Thus in high-risk applications, a manual test for certain tests in addition to an automated solution might be necessary. Unfortunately, comprehensive manual tests are time consuming and require the efforts of highly skilled professionals, and they are typically the most expensive to conduct. The decision to pursue a complete manual test should therefore be subjected to a cost-benefit analysis, in correlation with a risk assessment, to more accurately gauge the need. This is where the SaaS offering can be cost effective and efficient.

## Application Monitoring

With all these issues surrounding assessment, it seems as though a monitoring solution is the best option for an organization. However, monitoring an application for security issues is not a simple task. Again, the major issue here is the learning curve with which a security professional must progress in order to properly ensure a reasonable level of security.

There are several options for monitoring an application to determine whether an attack is taking place or has already taken place. Either way, a high level of network visibility is required to make the necessary distinctions between a real threat and a false positive—as well as distinctions between false negatives and activity that *appears* to be legitimate, but in fact may conceal a threat. This implies that an additional solution must be in place between the typical security countermeasures in a layered security model. In particular, an application firewall or full packet capture solution should be in place to give security professionals an accurate view of network traffic.

There are several solutions for blocking attacks, such as inline application firewalls, that do everything from detecting types of SQL injections to blocking users from multiple attempts to exploit a particular input field. There is a high return on investment for implementing these types of solutions. The automatic blocking features can easily ensure a base level of security. However, because the firewall does not have a full understanding of the application itself, it must be customized to fit the application in order to prevent cutting off critical availability or worse yet, missing attacks all together.

When utilizing black box technology, organizations can proactively determine vulnerabilities and application functionality to essentially educate the monitoring solution. This education can be utilized to enhance the Web application monitoring capabilities to truly protect dynamic Web applications as well as allow organizations to remediate production application vulnerabilities without the scrutiny of malicious attackers. It is for this reason that black box technology is an essential component in the monitoring of Web applications.

## What Works

Effective security strategies must be comprehensive in nature. Organizations must embrace education, automation, manual testing, and monitoring. While it must be noted that each of these areas have distinct gaps, together they create a climate and culture that addresses application security.

Education is possibly the most significant of these focus areas. Developers must be educated on secure coding standards in order to substantially reduce the possible attack vectors that a malicious attacker could exploit. Beyond developers, security assessors and auditors must be educated on the application security issues affecting a wide range of programming languages and coding techniques. These professionals must be trained on how to identify serious issues in a security assessment or audit of an application. This understanding must be well beyond that of a “top ten” or other checklist of issues. Finally, professionals monitoring application security must be educated on plausible avenues of attack as well as what an attack might look like. This knowledge should be obtained through analysis of application attack patterns and vectors.

---

The key is to implement an application security technology that can be utilized as a method for creating collaboration amongst multiple teams and stakeholders.

---

While these education efforts may seem fairly daunting, they can thankfully be simplified by utilizing automated and SaaS solutions to raise awareness, create a central point for education, and enhance the capabilities of other security countermeasures. The key is to implement an application security technology that can be utilized as a method for creating collaboration amongst multiple teams and stakeholders. Resolving application security woes in this manner enables organizations to leverage technology as a catalyst toward the solution as opposed to attempting to leverage the technology itself as the solution.

## About Cenizic

Winner of numerous awards and independent product reviews including SC Magazine’s Best Buy, Cenizic provides software (Cenizic Hailstorm®) and SaaS products (Cenizic ClickToSecure®) to protect Web sites against hacker attacks. Unlike network security and SSL solutions, Cenizic tests for security defects at the Web application level where the majority of attacks occur.

Cenizic’s patented technology goes beyond a signature-based approach by emulating a true hacker with a Stateful Assessment™ approach that maintains the state while attacking the application at the browser level. This approach allows Cenizic’s solutions to find critical vulnerabilities including application logic tests like session hijacking, privilege escalation, strong passwords, privacy policy validation, and many others that are typically missed by other vendors. Cenizic solutions provide details of all vulnerabilities, pinpointing the location, including URLs and forms, and comprehensive remediation information.

Furthermore, Cenizic can test for vulnerabilities across a multitude of applications including commercial and proprietary applications, Web infrastructure, and across multiple stages of a Web application. Cenizic supports testing of applications throughout the Software Development Lifecycle (SDLC) including deployed applications in production. Customers can test their live Web sites using Hailstorm’s built-in algorithms or by using Hailstorm’s integration with VMWare Lab Manager and Virtual Center without corrupting the database.

Cenzic's SmartAttack™ library is among the most open and configurable in the industry. This allows customers to customize the attacks to fit their own environment and for assessment zero day vulnerabilities. Also, through its CIA (Cenzic Intelligent Analysis) Lab team, Cenzic provides weekly updates to the attack library to help customers stay ahead of the recent attacks.

Hailstorm's Web-based intelligent and dynamic dashboard allows enterprise-wide visibility based on roles, and gives users control to manage the work flow of assessments from one central console. The reporting module provides a comprehensive set of reports that are customizable and can be exported in different formats to share with others in the organization.

Additional features in the Cenzic product line include prioritization of vulnerabilities using a quantitative score called HARM (Hailstorm Application Risk Metric), a proprietary algorithm, which can be configured by customers. This score better enables users to sort their vulnerabilities by HARM, and decide which ones to focus on first.

Organizations can use the Cenzic solutions to achieve compliance with a myriad of regulations including PCI, California AB1950, GLBA, HIPAA, FISMA, and many others.

Cenzic offers clients a flexible suite of products including software (for organizations that have internal expertise), Software as a Service (for organizations with limited expertise or internal resources), and a hybrid of both Software and SaaS (for organizations that want to deploy the software in-house but want to supplement their resources due to a large number of Web applications).

## **About Enterprise Management Associates, Inc.**

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst and consulting firm dedicated to the IT management market. The firm provides IT vendors and enterprise IT professionals with objective insight into the real-world business value of long-established and emerging technologies, ranging from security, storage and IT Service Management (ITSM) to the Configuration Management Database (CMDB), virtualization and service-oriented architecture (SOA). Even with its rapid growth, EMA has never lost sight of the client, and continues to offer personalized support and convenient access to its analysts. For more information on the firm's extensive library of IT management research, free online IT Management Solutions Center and IT consulting offerings, visit [www.enterprisemanagement.com](http://www.enterprisemanagement.com).

---

This report in whole or in part may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Enterprise Management Associates, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice. Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. "EMA" and "Enterprise Management Associates" are trademarks of Enterprise Management Associates, Inc. in the United States and other countries.

©2009 Enterprise Management Associates, Inc. All Rights Reserved. EMA™, ENTERPRISE MANAGEMENT ASSOCIATES®, and the mobius symbol are registered trademarks or common-law trademarks of Enterprise Management Associates, Inc.

**Corporate Headquarters:**  
5777 Central Avenue, Suite 105  
Boulder, CO 80301  
Phone: +1 303.543.9500  
Fax: +1 303.543.7687  
[www.enterprisemanagement.com](http://www.enterprisemanagement.com)



1833.022309