



WHITE PAPER

# The Case for Business Software Assurance

# The Case for Business Software Assurance

## Table of Contents

---

3	<b>Introduction</b>
4	<b>The Vulnerability of Applications</b>
6	<b>The Current Hacking Landscape</b>
7	<b>The Costs of a Data Breach</b>
8	<b>Defining and Implementing a Comprehensive Solution</b>
14	<b>Conclusion</b>
15	<b>References</b>

## Introduction

---

In recent years, the hacking community has shifted its efforts toward a new frontier: the application layer. With most companies spending thousands, if not millions, of dollars securing the perimeter with network firewalls, intrusion prevent systems, and other devices, hackers have realized the lowest hanging fruit lies in the applications themselves. Vulnerabilities that exist in the code are being exploited to steal private data, conduct phishing attacks, deface web sites, and run any range of online scams. These vulnerabilities have lead to breaches exposing over 212 million records over the last 3 years.

How are companies responding? *Business Software Assurance*. This is the capability to address the problem of application risk within an enterprise. It's the goal of ensuring the software that runs your business — whether it's the code you developed internally, outsourced, purchased, or integrated from the open-source community — is secure and able to withstand attack.

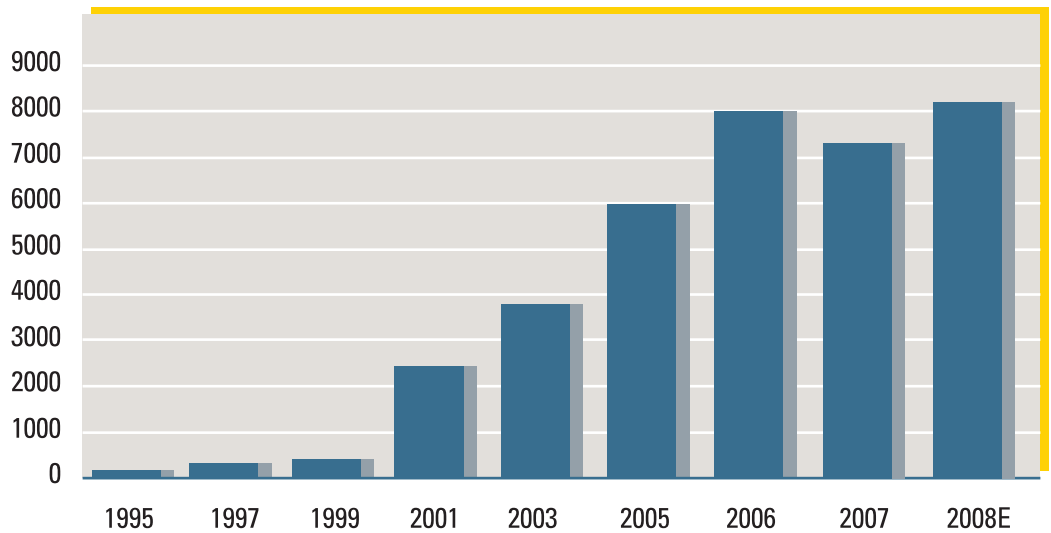
This white paper provides an overview of the severity of the problem, the current hacking landscape, and the people, processes, and technology needed to develop Business Software Assurance in your organization.

Between 1995 and 2007, the number of reported security vulnerabilities increased an average of 37 percent every year.

## The Vulnerability of Applications

With the advent of SOA, AJAX, and other Web 2.0 technologies, applications are becoming increasingly powerful and complex. With this complexity comes an ever-growing risk that security vulnerabilities will be introduced into applications. These vulnerabilities cannot be protected with a firewall, intrusion prevention system, or any other perimeter approach. They lie within the code and can be exploited by anyone who gains access to your Web site or your software. Unfortunately, developers are trained to build complex and feature-rich applications, and not applications that can withstand attack. Increasingly, the software applications that millions of people and businesses depend on every day are being exposed to escalating risks in the form of sophisticated attacks and other threats. Carnegie Mellon University's CERT (Computer Emergency Response Team) tabulates comprehensive data on the number of software vulnerabilities reported each year. Between 1995 and 2007, the data CERT collected and analyzed from numerous sources showed that the number of reported security vulnerabilities increased an average of 37 percent every year.

**Vulnerabilities Reported 1995 – 2007**



Source: CERT [1]

Application developers and their superiors in IT departments too often mistakenly believe that firewalls, intrusion detection systems (IDSs), identity access management (IAM) systems and network traffic encryption are sufficient measures for applications' security. By doing so, they are confusing application security with network security.<sup>3</sup>

Even more frightening are the vulnerabilities that are not reported. To gauge this number, the Web Application Security Consortium (WASC) analyzed 31,373 Web applications for common vulnerabilities. WASC's research shows that these applications contained over 148,000 distinct vulnerabilities and includes the following details about them:

- 7 out of 10 were vulnerable to Cross-Site Scripting
- 1 in 3 aided attackers with Information Leakage
- 1 in 4 was susceptible to Content Spoofing
- 1 in 6 fell prey to SQL Injection
- 1 in 6 employed Insufficient Authentication
- 1 in 6 used Insufficient Authorization
- 1 in 7 allowed Abuse of Functionality
- 1 in 20 permitted Directory Indexing
- 1 in 30 was a victim of XPath Injection

*Source: Web Application Security Consortium [2]*

Despite compelling data to the contrary, many organizations continue to operate under the misconception that securing their networks will block attacks against vulnerabilities in their applications. Joseph Feiman, from the Gartner Group, a leading information technology research and advisory company, writes:

"Application developers and their superiors in IT departments too often mistakenly believe that firewalls, intrusion detection systems (IDSs), identity access management (IAM) systems and network traffic encryption are sufficient measures for applications' security. By doing so, they are confusing application security with network security."<sup>3</sup>

Most of the attackers are aware of this and continue to shift their focus to applications. Many well-respected sources have recognized this change, including:

- Gartner, reporting that 75 percent of breaches are caused by security flaws in software.<sup>4</sup>
- National Institute of Standards and Technology (NIST), reporting that 92 percent of vulnerabilities are in software.<sup>5</sup>
- The United States Air Force, reporting that the percentage of attacks directed at their applications (versus their networks) grew from 2 percent to 36 percent between 2004 and 2006.<sup>6</sup>

*InformationWeek* reported that the number of hackers attacking banks jumped by 81 percent between 2005 and 2006, according to figures released at the Black Hat security conference in July, 2007.

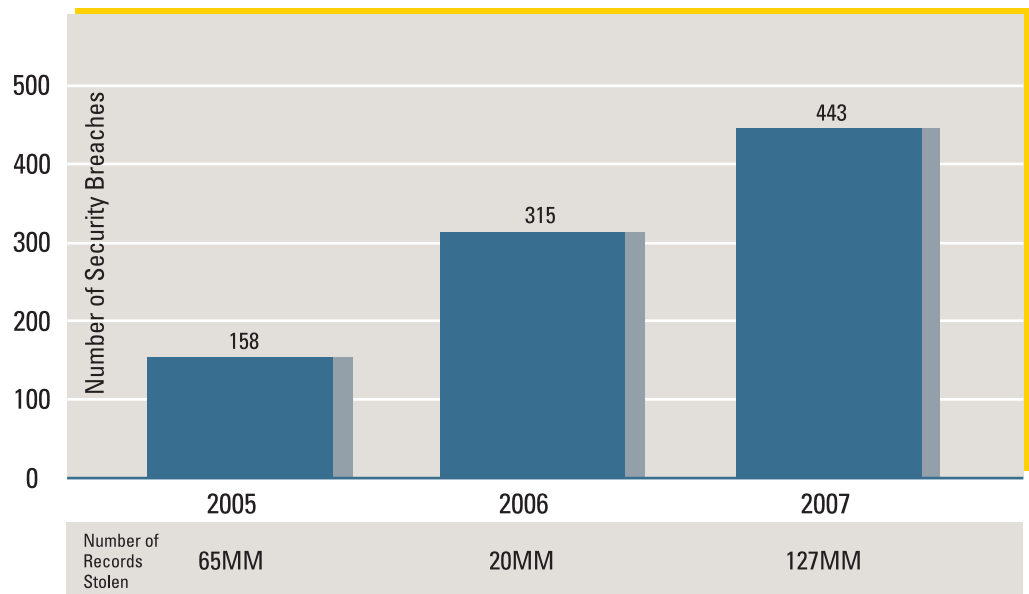
## The Current Hacking Landscape

Since the mid nineties, the number of attacks directed at the application layer has skyrocketed. CERT measured the growth in number of attacks to be, on average, 66 percent every year between 1997 and 2003, at which point they were forced to stop collecting the necessary data due to the sheer enormity of the endeavor.<sup>7</sup> This trend measured by CERT has continued to intensify over the last few years.

*InformationWeek* reported that the number of hackers attacking banks jumped by 81 percent between 2005 and 2006, according to figures released at the Black Hat security conference in July, 2007. *InformationWeek* argues this increase is due to the increased availability of hacking toolkits and malware in the online underground.<sup>8</sup> In addition, underground sites, such as <http://www.xssed.com/>, give attackers a blueprint of how to break into enterprise applications. In 2005–2007, over 212 million private records were reported stolen from American businesses; a significant portion of which was compromised as a direct result of a software breach.<sup>9</sup>

The chart below shows the number of breaches and records stolen between 2005 and 2007.

**Number of Data Security Breaches 2005 – 2007**



Source: *InformationWeek* [10]

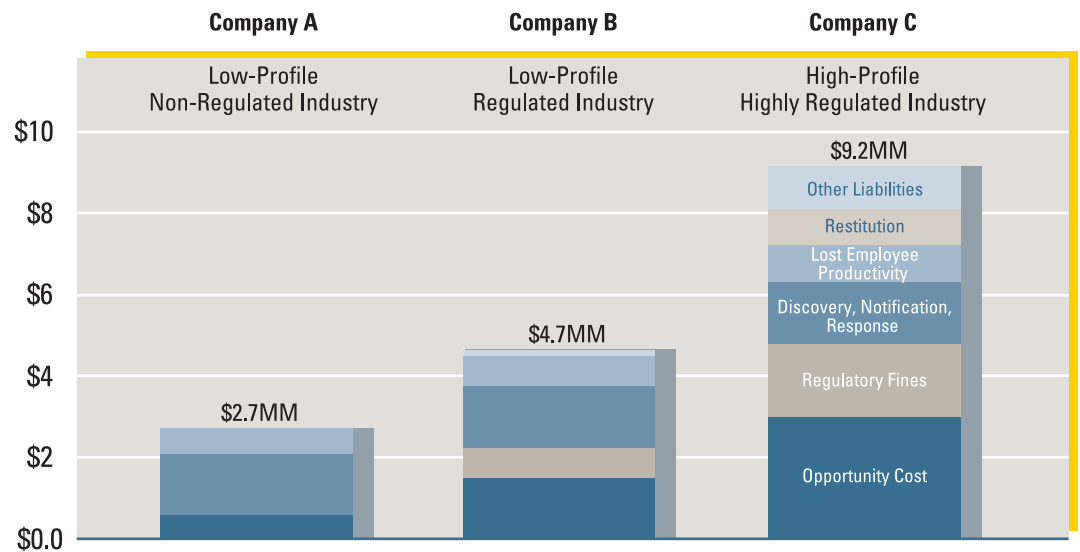
As of August 22nd, 2008, there had already been more breaches (449 total) than in all of 2007.<sup>11</sup> As more companies fall victim to data breaches, an increasingly accurate understanding of the true costs of a breach is being developed. The next section outlines these costs.

As of August 22nd, 2008, there had already been more breaches (449 total) than in all of 2007.<sup>11</sup>

## The Costs of a Data Breach

Various organizations have assessed the cost of a data breach. The estimated cost per compromised record currently ranges from a few dollars to upwards of \$400. The breadth of this range can be attributed to variations in the size of the organization that experiences the breach, the number of customers affected, the nature of the organization’s industry, and the percentage of its revenue derived from online transactions.

The graph below outlines the results of a recent study by Forrester. It shows the average cost of a data breach that impacts between 20,000 and 30,000 record. The study assessed the cost of a breach in three representative classes of businesses: a low-profile company in a non-regulated industry, a low-profile company in a regulated industry, and a high-profile company in a highly regulated industry.



Source: Forrester [12]

The Forrester data readily demonstrates that even a small breach can be extremely costly.

Business Software Assurance is the capability to address the problem of application risk within an enterprise.

# Defining and Implementing a Comprehensive Solution

As the application layer becomes the new frontier for cyber attacks, organizations need to develop an effective plan for securing their applications. The most effective approach entails implementing Business Software Assurance. As mentioned on the previous page, this is the capability to address the problem of application risk within an enterprise. This comprehensive approach outlines a set of actions that helps organizations:

- Establish a baseline where the greatest risk lies in the organization
- Define roles and assign responsibility for each task
- Educate developers on secure coding
- Identify automated solutions that can speed the process of securing applications
- Track metrics to gauge the success of each activity

At the core of Business Software Assurance are 12 Maturity Areas. In order to effectively navigate each area, Fortify has developed a comprehensive framework and set of activities that can be applied to any organization. To illustrate the concepts behind each of the 12 Maturity Areas, we outline below one question that addresses Level 1 Maturity for each area. These questions are intended to spark discussion around the necessary organizational competencies for application security.

Governance and Alignment	
Maturity Area: <b>Education and Guidance</b>	Question: Can your software developers describe the 10 most dangerous application security vulnerabilities and how their programming will mitigate the associated risk?
Maturity Area: <b>Standards and Compliance</b>	Question: Do you have a control statement document mapping compliance drivers to specific software implementations?
Maturity Area: <b>Strategic Planning</b>	Question: What is the software security vision of your organization, and what are the discrete steps you will take to realize that vision?

### Requirements and Design

Maturity Area:  
**Threat Modeling**

Question:  
Which of your applications has the highest associated risk, what type of hacker is most likely to attack it, and how would they attack?

Maturity Area:  
**Security Requirements**

Question:  
Are there security requirements in your application specification, and do they tie directly to specific business functionality?

Maturity Area:  
**Defensive Design**

Question:  
Do you have a document describing the required security principles for each perimeter interface of your application?

### Verification and Assessment

Maturity Area:  
**Architecture Review**

Question:  
Do you have a system architecture diagram annotated with the design features that address each known security requirement?

Maturity Area:  
**Code Review**

Question:  
Do you have a checklist of known security requirements, and do you use it to perform code reviews during the development process?

Maturity Area:  
**Security Testing**

Question:  
Do you have a checklist of known security requirements, and do you use it to create and evaluate a set of security-specific test cases?

Deployment and Operations	
<p>Maturity Area: <b>Vulnerability Management</b></p>	<p>Question: Do you have an established incident response plan? Are the assigned points of contact for security issues clearly documented?</p>
<p>Maturity Area: <b>Infrastructure Hardening</b></p>	<p>Question: Do you have a specification for a secure operational environment, and do you have processes to ensure the specification is followed?</p>
<p>Maturity Area: <b>Operational Monitoring</b></p>	<p>Question: Do you have a documented set of procedures for managing critical and security-related application alerts?</p>

In order to help companies define, develop, and implement these 12 Maturity Areas, Fortify offers extensive services and cutting-edge technology.

### Services to Help Achieve Business Software Assurance

Fortify services include detailed programs around each of the Maturity Models described above. Below is a list of some services available today.

#### Security Awareness and Secure Coding Education

This program provides customers with the ability to increase security awareness and usage of industry best practices within their organization.

#### Software Business Risk Assessment

This program utilizes application testing, validation, and threat modeling to characterize real threats, as well as to identify and quantify the software security risks associated with an organization’s applications.

#### Application Vulnerability Assessment

This program offers a code review using the industry-leading Fortify 360 Suite. A detailed summary of all vulnerabilities is produced along with a description of the underlying code issues and methods to address the vulnerabilities.

### **Third-Party Application Assessment**

This program gives an organization the opportunity to have their third-party applications assessed for security weaknesses.

### **Ongoing Managed Assessments**

If an organization lacks sufficient application security resources, a Fortify consultant can provide the needed application security resources on a regular basis.

### **Application Security Strategy and Planning**

A Fortify consultant works with the enterprise to develop and document a strategy for addressing application security. The strategy is developed through a series of technical workshops with lead technical engineers, architects, business sponsors, testers, and other individuals involved in the software development process.

### **Business Software Assurance Process Design and Implementation**

A Fortify consultant works with project stakeholders to assess the customer's current organizational approach to application security. A gap assessment is performed to determine variance between the customer's current strategy and industry best practices. Current application security policies, guidelines, and specifications, along with existing artifacts and workflow processes within the project management cycle, are all carefully reviewed and considered from an application security perspective.

### **Secure Development Lifecycle Planning**

This service helps an organization integrate best-practice SDL activities into their development strategies. A Fortify consultant reviews existing methodologies, workflows, and processes from an application security perspective. A gap analysis is performed to illustrate the strengths and weaknesses in the current processes.

### **Policies, Guidelines, and Technical Papers**

For this service, a Fortify consultant provides assistance in developing technical guidelines, policies, and white papers that define and communicate these standards.



Fortify offers the number-one market share application security technology, as noted by the Gartner Market Share: Application Development Software, Worldwide 2007 report.<sup>13</sup> With over 400 successful deployments, Fortify has more experience and expertise than any other company.

## Technologies to Help Achieve Business Software Assurance

As a company evolves with Business Software Assurance, it becomes increasingly important to use automated solutions to help expedite the work. Fortify offers the number-one market share application security technology, as noted by the Gartner Market Share: Application Development Software, Worldwide 2007 report.<sup>13</sup> With over 400 successful deployments, Fortify has more experience and expertise than any other company. The flagship product is called Fortify 360.

**Fortify 360** is a suite of integrated applications for identifying, prioritizing, and repairing security vulnerabilities in software and managing the business of assuring application security. It includes 3 analyzers that identify over 315 vulnerability categories across 17 languages and 500,000 APIs.

- Source Code Analysis to identify vulnerabilities throughout the code
- Program Trace Analysis to identify vulnerabilities in a running application during a QA test
- Real-Time Analysis to monitor and protect a deployed application

### Fortify Source Code Analyzer (SCA)

Source code analysis is the most comprehensive solution to the application security problem. It leverages the ability to cover 100 percent of the application to analyze every feasible path that execution and data can follow to identify and help remediate hundreds of categories of vulnerabilities. Fortify SCA is the most deployed source code technology and has won numerous awards for its cutting-edge approach.

Key Benefits:

- Analyzes 100% of the source code
- Provides detailed information on each vulnerability
- Identifies vulnerabilities early in the software development lifecycle, when they are least expensive to fix
- Educates developers about security while they work

## Fortify Program Trace Analysis (PTA)

The Fortify Program Trace Analyzer identifies application vulnerabilities during runtime, while an application is being tested. PTA integrates with any QA test to find security vulnerabilities while a QA test is performed. It reveals vulnerabilities that can be found or more easily identified only when an application is being executed, such as those that become apparent through unpredictable user behavior. With no customization required and zero security expertise needed, PTA enables QA testers and developers to find security vulnerabilities while conducting their typical functional tests.

Key Benefits:

- Enables enterprises to repurpose test suites for detection of vulnerabilities
- Integrates seamlessly into existing QA testing processes
- Provides accurate results with the fewest false positives
- Operates from within an application, providing the best context to determine whether an issue is genuinely exploitable or simply benign
- Provides the exact code location for each vulnerability, enabling more rapid remediation

## Fortify Real-Time Analysis (RTA)

The Real-Time Analyzer (RTA) monitors and defends deployed applications. Uniquely positioned inside an application, RTA provides a real-time view into how a deployed application is being attacked in the real world. At any point in time, IT personnel can see who is attacking (based on IP address and domain name), how the attack is being conducted, and what part of the application is being attacked, down to the exact line of code. RTA can also protect an application against an array of attacks, including evolving logic-based attacks, directed hacking attempts, and data mining.

Key Benefits:

- Provides true application-layer insight and can make use of application logic to make decisions
- Provides results in real time, including email alerts
- Accurately distinguishes between an actual attack and a legitimate request, improving the end-user experience, while greatly boosting protection
- Can accommodate additional logic- and behavioral-based rules that address specific threats for individual Web applications

## Conclusion

---

As our networks become more secure, the application is becoming the new frontier for cyber warfare. The results show that hackers are increasingly attacking vulnerabilities in applications to steal private records, often at great cost to the application's owner. Technology, including the advances commonly referred to as Web 2.0, has enabled applications to provide new levels of functionality, which brings with it added complexity and a related increase in the chance the software will contain security vulnerabilities. Today, attacks against applications impact organizations across nearly every industry, including finance, healthcare, retail, telecommunication, education, ISVs, and government agencies. Every indication is that hackers, organized crime cartels, and foreign entities are increasing their efforts and directing attacks against applications. In order to combat these threats, a comprehensive process is needed. That's where Business Software Assurance can help. It includes the correct balance of processes, people, and technology. Fortify offers the necessary services and products to help any organization achieve Business Software Assurance. The solutions to protect you are here. What are you waiting for?

## References

---

- 1 Computer Emergency Response Team, *Vulnerabilities Reported*. <http://www.cert.org>
- 2 Web Application Security Consortium, *Web Application Security Statistics Project*. <http://www.webappsec.org/projects/statistics/>
- 3 Joseph Feiman, *Application Developers Should Assume Responsibility for Application Security*, November 16, 2006, *Gartner*
- 4 Theresa Lanowitz, *Now Is the Time for Security at the Application Level*, December 1, 2005, *Gartner*
- 5 Mark Curphey, *Software Security Testing: Let's Get Back to Basics*, October 2004, *SoftwareMAG.com*
- 6 Bruce Jenkins, Major, USAF (Ret.)
- 7 Computer Emergency Response Team, *Incidents Reported*. <http://www.cert.org/>
- 8 Sharon Gaudin, *Number of Hackers Attacking Banks Jumps 81%*, August 2, 2007, *InformationWeek*
- 9 Thomas Claburn, *Record Number of Data Breaches Reported in 2007*, December 31, 2007, *InformationWeek*
- 10 Ibid.
- 11 *Identify Theft Resource Center*, August 22, 2008  
<http://idtheftmostwanted.org/ITRC%20Breach%20Stats%20Report%202008.pdf>
- 12 Khalid Kark, *Calculating the Cost of a Security Breach*, April 10, 2007, *Forrester Research*
- 13 Joe Feiman, *Gartner Market Share: Application Development Software, Worldwide 2007*, June 2007, *Gartner Group*

