



## PREXIS

### 2005 COMPUTERWORLD HONORS CASE STUDY

#### BUSINESS & RELATED SERVICES

TEAMS PROVIDE A METHOD BY WHICH A SECURITY VENDOR CAN ANALYZE AND ELIMINATE VULNERABILITIES IN THEIR SOFTWARE BEFORE RELEASING IT TO MARKET. [20055303]

*A Search for New Horizons*



Robert Carrigan,  
Chairman of the Chairmen's Committee

Ron Milton,  
Vice-Chairman of the Chairmen's Committee

Dan Morrow,  
Chief Historian

#### SUMMARY

Ounce Labs provided a method by which security vendor Entegriety Solutions can analyze and eliminate vulnerabilities in their software before releasing it to market. Entegriety now establishes and certifies quantifiable security requirements, drastically reducing potential costs associated with future security patches, security breaches, legal implications, and loss of customer loyalty.

#### APPLICATION

Entegriety Solutions provides software for customers to manage the foundation of e-business security. With diverse product lines that include access management, secure file content delivery, and the most widely accepted solutions for developing and deploying secure, distributed applications, Entegriety lists Citibank, Daimler Chrysler, Hewlett-Packard, Lawrence Livermore National Labs, and United Airlines among its customers.

Entegriety's product diversity demands a complex development organization with simultaneous projects being written in multiple programming languages. The company's secure, distributed middleware products range up to 3-4 million lines of code, some of which was developed by Entegriety up to 15 years ago. Before products are released, they must pass rigorous testing against strict internal security requirements.

To enable thorough security testing of its products without using costly manual review teams, Entegriety chose Ounce Labs' product Prexis based on its ability to assess large enterprise applications and provide management-level analysis. Built on proprietary security complier technology, Prexis can analyze millions of lines of code in minutes, so assessments can be run frequently throughout development, and results can be tracked against security baselines.

Able to analyze C, C++, Java, and JSP, Prexis can assess Entegriety's entire range of products. Its detailed analysis of the source code is also ideal for testing Entegriety's access management and middleware products because it can assess individual pieces of code without requiring a complete, front-end application. Most importantly, Prexis' management-level information gives an overall picture of security levels for each project. Ounce Labs' unique V-density (vulnerability density) metric is used to guide remediation efforts toward critical vulnerabilities and evaluate applications against security release criteria.

Confidently delivering secure software is an important goal of Entegriety's. Prexis allows the company to set very strict security requirements at the beginning stages of product design and development, and test the applications against those requirements throughout development. The quality assurance team also uses Prexis to pinpoint critical vulnerabilities at their exact line of code, sending those files back to developers to make sure these flaws are fixed before the product is sent to customers.

#### BENEFITS

Security problems caused by vulnerable software is not a new or isolated problem. Consumers are increasingly burdened by threats of Internet worms, identity theft, and other attacks that target mistakes made when the software they rely on was written. This is an even more serious problem for businesses and government agencies, which depend on software to house critical data, carry out financial transactions, maintain control of transportation and utilities, and other functions that we often take for granted as citizens. The firewalls, intrusion detection systems, and other security devices and

services used to protect vulnerable software from being attacks have grown to an industry of over \$11 billion, according to analyst firm the Yankee Group.

This implementation specifically gave Entegriy the ability to efficiently measure and improve the security of software it delivers to its customers. Entegriy now can assure its products adhere to quantifiable security standards, which saves for itself and its customers the costs associated with frequent software patches, product updates, or potential security breaches.

For the software industry as a whole, this project is a model of how to improve security in the software development process: starting with strict, quantifiable requirements, giving developers tools to track and fix vulnerabilities, and inspecting all products thoroughly to make sure potential problems are addressed before they put customer resources at risk.

## **IMPORTANCE**

This project could not have succeeded without the technology. Prexis allows a user to analyze millions of lines of code in under an hour, a task which a large team of experts could achieve only a fraction of in a period of several months. Even if companies could afford such an enormous expense for a small number of their applications, the accuracy and consistency of analysis could never match the automated technology in Prexis.

The reasoning and skill that manual review teams bring to code assessment projects is greatly enhanced by Prexis, because it focuses their attention of the critical elements of the software that may expose systems to malicious code and other attacks. Other customers are carrying out similar projects with Prexis, in some cases analyzing applications with hundreds of millions of lines of code – a process that would be inconceivable without such a robust, scalable technology.

## **ORIGINALITY**

The technology used in this project is brand new. Some technologies have been created in the past to address the problem of software risk, including binary analysis tools, penetration testing software, and open source assessment applications. While these products have offered different levels of value, they have been implemented because there has been no method available to accurately identify the fundamental mistakes that make software vulnerable.

The solution to this problem, automated source code analysis as a technology has been publicly available for less than a year. It is a completely unique approach to what many consider the largest problem in information security and auditing – not only the existence of software vulnerabilities, but the inability to measure and analyze software risk.

## **SUCCESS**

Entegriy accomplished all of its software risk assessment goals using Prexis. It created a way to establish and test for strict security requirements of its software. It dramatically increased the analysis capabilities of its review team, which can now assess several applications consisting of millions of lines of code without throwing the product's development process off schedule. Prexis' high-level reports show quantifiably that Entegriy developers and QA staff are delivering more secure software.

The most indicative evidence of the success of this project is Prexis' time-to-value for Entegriy's business process. Within one week, Prexis was fully integrated into the company's review process, immediately increasing the review team's contribution to software quality and security.

## **DIFFICULTY**

Assessing the problem actually took place before Ounce Labs was founded. Having each worked in nearly every aspect of information security for over 15 years, the founders of Ounce Labs heard from business executives at top financial, government, and other organizations that assessing software risk was one of their biggest unsolved operational problems. It was not difficult to determine that the most effective and efficient way to address this problem is to analyze risk at the source code level, where the problems originate.

Designing and building software to accomplish this task was a much more difficult task. The few previous attempts to solve this problem were open source applications that offered very little usable

information and no practical value to business organizations. Ounce Labs' founders recruited veterans of software development with a variety of backgrounds required to create a product that could read and compile source code and analyze its functions against tens of thousands of potential security problems. Ounce Labs has several patents pending for the technology behind Prexis, which represents nearly three years of research and development that took place to build this solution.