



**NETCLARITY presents...**

AGIA's Case Study on ***Auditor 128™***



## **Protecting Web Assets at AGIA with *Auditor 128™***

### **AN ON DEMAND SECURITY & VULNERABILITY MANAGEMENT SYSTEM CASE STUDY**



by Bill Tyson, CMO and SVP, AGIA

#### **AGIA History and Background**

The history of AGIA reflects a pioneering spirit well founded in the knowledge of insurance. In 1951, James B. Wigle, CLU, the founder of AGIA, initiated a program of marketing group insurance through the mail to affinity groups.

In 1956, Continental Casualty developed a new type of disability insurance and designated Association Group Insurance Administrators as their exclusive marketing agent for California. Over the next 10 years, Jim Wigle acquired over 400 hospital endorsements of his insurance programs and this segment of

his business grew steadily. In the years that followed, AGIA developed relationships with several additional clients whose benefit programs have provided profitable, sustained growth for AGIA and meaningful benefits for the organizations and their insureds.

When John Wigle joined AGIA in 1974, he expanded on the foundation laid down by his father. John continued to focus on the specific needs and unique characteristics of each client's membership to expand their programs. AGIA's success can be greatly attributed to his commitment to mutual goals, and delivering on the promises AGIA makes.

Through ongoing reinvestment in technology and personnel, AGIA has grown steadily from an insurance agency managing startup programs in the late 1950s to what we are today: a technologically advanced, multi-faceted, full-service administrator, managing programs with over 30,000,000 bank members, over 12,000,000 association members, and over 2,500,000 insureds.

### **AGIA Identity Theft Prevention Program**

Bill Tyson is the Chief Marketing Officer and Senior Vice President for AGIA. Bill and his eSolutions team manage a whole host of digital properties for the marketing and sale of voluntary benefit programs. Recently, the team developed and launched a new, rich media presentation with micro web sites to communicate the risks of identity theft to consumers within membership organizations and offer Identity Guard CreditProtect® as an identity theft solution. He wanted a network security solution that provided quick and easy CVE remediation, adding an additional level of protection to the digital properties AGIA manages.

Bill has chosen **Auditor 128™** for AGIA. His Web Developer Jim Mannix, said he set up **Auditor 128™** and tested it by pointing it at three machines, and in 45 minutes it had found a few vulnerabilities that were quickly patched. In the next section, Jim Mannix reports on how **Auditor 128™** is protecting web assets at AGIA.

### **Protecting Web Assets at AGIA**

At AGIA we host and manage over 50 different database-driven, ecommerce-enabled websites across numerous servers and are building new sites and web applications on a daily basis. We build and maintain these specialized and feature-rich sites for our valued customers in the Insurance Industry and take our responsibility to protect these assets very seriously. The nature of the technology we employ, specific government regulations like HIPAA, and our own high standards demand that we take a proactive approach to Web Security.

Prior to implementing **Auditor 128™**, we had no efficient way of knowing our level of exposure to network-born vulnerabilities. It was not feasible to manually research the current state of vulnerabilities that our Web infrastructure might potentially expose us to. In the extensive time that would have been required to implement a manual security audit, our infrastructure would have changed and new vulnerabilities might have been introduced by any number of normal development or maintenance activities.

Given that time was a critical resource, it seemed the most efficient way to leverage that resource was to immediately implement already proven solutions for network security. We realized that not only should every company that is serious about network security perform comprehensive security audits, but they should do so at regular

intervals. It became obvious that we needed an automated solution.

NetClarity's **Auditor 128™** appliance fills this need perfectly. NetClarity makes a network security and vulnerability management system housed in an appliance that plugs-and-plays on any network, regardless of the operating systems of individual pieces of equipment on the network. The system audits all equipment on the network and delivers reports about their vulnerabilities that provide point-and-click remediation.

The security management system is easy to configure and is up and running in about 15 minutes. All you have to do to configure it (after a short installation procedure) is to click a button in its browser-based interface. It automatically goes out and finds the IP addresses on the network. You can then select the particular machines to audit.

NetClarity **Auditor 128™** performs extremely thorough vulnerability auditing and probing against the network, servers, workstations, routers, and more. The comprehensive nature of the audits is remarkable. We recorded over 2500 individual probing connections against a single machine in one case. Every kind of vulnerability you can imagine is covered. New vulnerabilities are updated for inclusion in auditing scans automatically, as soon as they are discovered.

This appliance is a security management system that allows you to audit equipment by scheduling custom configurations for daily, weekly, or monthly audits or on demand audits. It

also updates vulnerabilities either on a schedule or on demand.

In spite of the complexity of the internal workings of the audits, it is very simple to configure, schedule, and control the auditing. You can initiate a wall-to-wall, in-depth audit at full speed and launch it as part of a concentrated audit, or you can schedule regular, metered "background" audit scans of specific assets and schedule them to occur during off-hours to avoid impacting your normal business activities. NetClarity **Auditor 128™** manages a highly complex activity through an easy-to-use browser-based interface.

The reports **Auditor 128™** generates are outstanding. The easy-to-read PDF-format reports are as comprehensive as the audits they document.

For any given server, for example, you will see a list of all possible vulnerabilities and a rating of the severity of each item. Next to that is a very detailed description of the vulnerability and a reference to that entry in the CVE Database with references and links to sources that will provide or assist in resolution of that vulnerability.

The (CVE) Common Vulnerabilities and Exposures database is **the** authority for up-to-date information on the specific vulnerabilities known for any kind of computer or networked device. The detail with which the NetClarity **Auditor 128™** reports describe each vulnerability is great, but the information on how to remedy each item and the links to important sources of patches and more is invaluable.

Once you get over the initial surprise of how many vulnerabilities might be lurking within your infrastructure that you did not know about, these detailed reports guide you quickly along the path to remedy each issue. They are easy to read and have varying levels of detail in versions designed for three different user levels—Executives, Managers, and Administrators.

Distinct logins and passwords are available for Executives and Managers who do not need the technical details found in Administrator reports. They can log in to get the appropriate reports at their convenience and are not forced to muddle through information that is specifically for the system administrator.

Once we worked through the reports from the initial audits and took a first pass at remedying vulnerabilities in order of priority, we performed another audit, reviewed the reports showing any remaining or new vulnerabilities, and then repeated the process until we had

protected all equipment and eliminated all avenues of attack.

It is a very satisfying experience to see the before and after results and to be able to explicitly show the benefits of this proactive approach in clear, illustrated, and comprehensive reports.

NetClarity **Auditor 128**<sup>TM</sup> has allowed us to quickly shore up our infrastructure and provide solid, ongoing protection against attack. Performing regular auditing scans on a daily, weekly, or monthly basis gives us real peace of mind, awareness, and validation of the true security of our IT assets.

At AGIA we have put **Auditor 128**<sup>TM</sup> to the demanding task of protecting our diverse and mission-critical infrastructure. This outstanding product continues to excel at that task. With NetClarity **Auditor 128**<sup>TM</sup> on our network, we get regular validation that we are protected against attack and enjoy a significant increase in security.

Copyright © 2004, PredatorWatch, Inc., d/b/a NetClarity. All rights reserved worldwide. **Auditor** and NetClarity are Trademarks of PredatorWatch, Inc. CVE<sup>®</sup> is a registered trademark of MITRE Corporation. CreditProtect<sup>®</sup> is a registered trademark of AGIA. Other servicemarks, trademarks, and copyrights mentioned in this document are property of their respective owners. NetClarity is an IBM Business Partner.