

SUCCESS WITH SENTRYACCESS

NENIX *and* SECUGEN CORPORATION: Secure Access for Biometric Developers



COMPANY OVERVIEW

As the global leader in biometric devices, SecuGen has literally made security its business. SecuGen provides biometric solutions for physical and network security, employing the most advanced fingerprint recognition technology currently available.

A critical factor in SecuGen's success has been the ease with which its optical recognition devices integrate into a variety of computing environments. Because its sensors are available in both stand-alone and PC-connectible configurations, SecuGen biometric devices can be integrated into virtually any type of operating platform or application.

BUSINESS CHALLENGE:

STRENGTHEN AUTHENTICATION *and* PROVIDE ACCESS CONTROL TO SGDN

SecuGen maintains two external networks: one for its Partner Network (SPN) and another for its developer network, the SecuGen Developer Network (SGDN). Through SGDN, SecuGen provides developer resources that enable clients to create custom software applications that use SecuGen peripherals for user authentication.

When SecuGen first launched its SGDN network, there wasn't the same need for tight control over resources, as SecuGen was a young organization and those accessing the site were known to it. As SecuGen grew into the leading market position it currently holds, however, the need for additional user authentication and a method for protecting and controlling access to these resources became apparent. A constantly increasing number of users were visiting SGDN, and the amount of resources being made available through it grew in parallel.

Responding to these issues of authentication and authorization, SecuGen developed its own solution that used its biometric devices to protect entrance to both the Partner and Developer Networks. In order for a user to enter either SecuGen system, fingerprints needed to be provided and verified against the relevant database.

Combining award-winning fingerprint recognition technology with the emerging leader in secure authorization and access control enabled SecuGen to protect developer extranet resources.



A router would then direct a user to the appropriate network server, which in turn queried the appropriate network database for fingerprint verification. If verification was successful, the user was allowed to enter the SecuGen network. A critical concern, however, was that **as soon as a user was granted access to the system, he was able to view any and all resources and applications residing there.**

Said Won Lee, CEO of SecuGen, "we had multiple user groups obtaining information through SGDN. But we didn't differentiate between these groups, or track user behavior. Basically, once a user identity had been verified, that user had access to all the resources within our extranet."

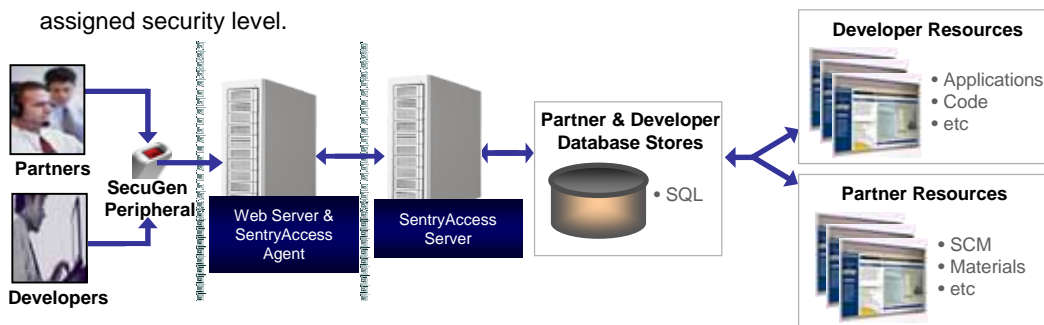
SUCCESS WITH SENTRYACCESS

SOLUTION

"Integrating SentryAccess software into SGDN web and authentication servers provided SecuGen with the robust authentication and authorization needed to keep pace with their growing user population," said Steve Hong, Nenix's CTO and SentryAccess architect. "It also has provided SecuGen with a method for tracking and monitoring site visitor behavior, which can be very valuable for a security-minded organization."

Registered SGDN users are now authenticated through a combination of SentryAccess and SecuGen technology. Using a web browser, members navigate to the SGDN login page at <http://sgdn.secugen.com>. A SentryAccess component residing on the SecuGen web server, the SentryAccess Agent, intercepts the login request and prompts the user for login information, including user name and password / fingerprint. The SentryAccess Agent forwards the login request to another SentryAccess component, the SentryAccess Server.

The SentryAccess Server resides in the network's backend, behind a hard firewall. Once it receives a request from the SentryAccess Agent, it queries user and policy databases for authentication verification and resource permission information (authorization). If authentication is successful, a personalized menu of available resources is presented to the user. These menus display only the items for which the user – based on his profile – has permissions. This is an important security consideration as users may longer browse through all the resources contained in SGDN; users may only view items appropriate to their assigned security level.



Lee pointed to Nenix's all-inclusive solution as a key factor in choosing SentryAccess. "Several other vendors required us to purchase additional modules in order to get the same functionality Nenix delivers as standard, such as auditing and logging features," Lee said. "With Nenix, there was just the one software purchase, and we got everything we needed: authentication, access control, with easy-to-use auditing, logging, and reporting tools included."

RESULTS

For Lee and his SGDN developer community, SentryAccess lives up to its promise of delivering secure access control and authorization. "Protecting resources and assigning user groups is easier than we expected. We can even delegate administrative responsibility to as many different people as we choose," said Lee. "Further, by combining SecuGen's fingerprint recognition technology with SentryAccess we are able to protect our developer resources behind an additional authentication layer. And now, access to these resources is reserved for only those having the proper entitlements. As a bonus, we are able to monitor and track user behavior, which is reassuring."

COMPANY INFO

Company Name:
SecuGen Corporation®

Industry:
Biometric Solutions

Locations:
Santa Clara, CA
Tokyo, Japan

SecuGen® on the Web:

www.secugen.com
www.secugen.co.jp

DEPLOYMENT INFO

Operating System:
Microsoft Windows

SentryAccess Agent:
Windows 2000 Server

Web Server:
Microsoft IIS 5.0

Database:
Microsoft SQL 2000

Contact Nenix:
2310 Walsh Avenue
Santa Clara, CA 95051
1.408.970.9242
www.nenix.com
support@nenix.com

