



## **Visual Guard Case Study**

Centralize all aspects of security, for all technologies, in one solution

## The company

Our client is an international insurance company. It employs over 700 people worldwide, most significantly in the United States, Canada, Great Britain, Australia, Switzerland and Singapore.

Over the past 8 years, our client has experienced very strong growth: steady increases in revenue, development of international activities, and an IPO. The company has very quickly become a recognized player in the insurance world. Like any multinational company, it faces challenges of globalization and organizational growth. Security of their information technology is a key challenge. They face a common paradox: how to move information, in a way that is simple and intuitive, fostering business development, while at the same time ensuring an optimal level of security against repeated attacks on confidential data?

This problem is all the more sensitive as the insurance industry requires the handling of highly confidential data. In this context, vulnerability is not an option.

## The need

In the field of access control, the company had introduced several tools to meet various safety needs over the years:

- User authentication mechanisms
- Rights development and management systems
- Password and identity management systems
- Control and audit processes

Each of these needs was covered by a different system, and duplicated for each new application or new technology used within the group.

The proliferation of systems and dispersal of information prevented a clear view of the security policy, and hid any flaws. The company wanted to implement a system of access control to standardize security processes.

“This would be a corporate initiative. Everything would flow through a centralized security hub.” – Head of Security

## Choosing a Solution

Visual Guard was chosen after a thorough analysis of security solutions available on the market. The deciding point was Visual Guard’s ability to clump tasks related to access control: authentication, rights management, user administration, and auditing. A single system was able to cover all their security needs. “We are looking for an all-inclusive toolset.” confirmed the Head of Security.

In addition, Visual Guard provides a multi-technology approach to secure all applications, regardless of technology used. At our client’s request, we began by securing the applications based on .NET, which Visual Guard integrates with perfectly: Winforms, Webforms, Asp.net, Webservices, SCF, WPF...

The next step was to secure our client’s Java applications. In this case, we used the module VGServer, based on web services. This module opens up Visual Guard’s functionalities to any application capable of performing an HTTPS or SOAP request. The company has the ability to secure all of the applications in their portfolio with a single system.

The VGServer can also cover distributed architectures, which was needed to deploy the security in all subsidiaries and branches of the company.

## Process Standardization

Tools for security administration were crucial to meet the needs of our customers.

"The most important benefit of VG for me is that we have a central place to manage the authentication and the authorizations for all the company," said the Head of Security.

The Administration Console is the interface to manage all aspects of security: authentication, user management, creation and daily management of permissions, audit...

"Thanks to the Administration Console (and the different available roles) it is very easy to give the ability to create roles and users to business administrators and divide the tasks between the development team and the administrators."

It is possible to control access to the functionality of Visual Guard, and, for example, assign identity management to heads of departments.

The WebConsole, which will be implemented on site shortly, goes even further: it is intended solely for non-technical administrators, and can be used anywhere there is an Internet connection. A significant advantage for the company, which has subsidiaries in over 6 countries around the world.

Regarding authentication, the company must simultaneously manage internal and external users.

To authenticate users internally, we reused the existing Windows accounts. They are now used by employees to access applications.

For users outside the company, login and password accounts were created using Visual Guard's native membership provider.

Ultimately, their goal was reached: Applications can be used interchangeably with both types of accounts (mixed authentication).

All accounts are managed in a single console. A non-technical administrator can assign roles to each type of account from the console.

The console has been used for both the standardized system of roles and for the permissions throughout the group. The security team has redefined the permissions at the corporate level.

Advanced features such as anonymous roles assigned by default or shared roles used for several applications have improved the match between the system of permissions and actual business of the company.

The next step was to make the list of roles available to administrators for daily management. As the Console can directly map a Visual Guard to a Windows account or group, the new system could be implemented without compromising the original architecture.

The audit feature was also important for our client, who had to comply with various regulations (in particular the Sarbanes-Oxley Act (SOX)).

The standardization of their processes has helped to significantly improve the transparency of the security system. Centralizing all roles in the same place, rather than dispersing them in each application, gives a clear view of safety rules enforced at any time.

Our client has subsequently implemented the log feature, which records events executed in applications. The team has compiled a list of events that should be tracked based on their audit needs. As the log can be augmented, the team was able to add the necessary information to each record to fulfill the requirements of various regulations.

## The results

Visual Guard helped address our customer's needs to standardize their security system.

They now have an overview of all rules applied, and can control their applications at all levels of the organization. "Moreover, the support provided by Novalys has been excellent and very quick" said the Head of Security. The presence of a responsive support team was all the more significant as the company had to cope with staff movements which temporarily weakened the security team. Today, .NET application security has been implemented. The next phase of implementation will secure the complete portfolio of applications.