apriorit

Case Study: **Multiagent Corporate Security Monitoring System (USA)**

Areas: Corporate Security, User Activity Monitoring, Distributed System Management, Large System QA

Client: US-based company (NDA protected name)

Project started: 2006

The Situation:

The Client worked with Apriorit on development of the product for remote computer investigation as for corporate security norm compliance (email databases and chat logs parsing, tracking files with sensitive information, monitoring for illegal content, etc.) for 2 years.

The developed product had a significant market success and so the client decided to extend this product line with a product of the same basic functionality but with the **client-server architecture** performing monitoring of the corporate network in real time.

The Problem:

It was obvious that the project was to be very large: there were a lot of features that had to be integrated into the new architecture; moreover, there were a number of new features planned to improve product competitiveness.

The new architecture itself had to face high requirements as the solution had to monitor various and numerous user activities on workstations supporting up to **100 000 simultaneously working agents**. Moreover, the system had to work stably in case of any component problems.

Auxiliary modules to maintain such big distributed system – such as update, compatibility, general search, management modules – also were not the trivial tasks.

One more question was the system testing. The product included more than 200 different features and at the same time had to guarantee support of tens thousands PCs.

Apriorit team had all the necessary expertise to implement security features for the system as it was them who had developed the local product version. The challenging part was the new architecture creation and development of the supporting modules for the big distributed system.

The Solution:

Apriorit formed a separate team for this project consisting of 6 developers and 3 testers. Developers of this team actively discussed the tasks and ask for consultations of the local product version team. A smooth integration process was created to incorporate the newest stable versions of the corresponding basic functionality modules to the current corporate system releases.

The first important task was to create a **flexible smart architecture** that could support and guarantee acceptable performance of the multiagent system. A number of smart architecture solutions were produced. To satisfy the requirement of the system stability against internal module errors, and also facilitate the process of debug and bugfix, the architecture with the minimal module connectivity was proposed. Besides making developers' life easier, such architecture allowed the Client and the team to build easily and quickly the limited versions of the system with some selective range of features and promote them on the market gaining customer response.

Module development had two directions: existing functionality adaptation and new unique feature creation. Among other original solutions, Apriorit team created such features as:

- file classification by their content (signatures) and not extension (to resolve file renaming problem);
- downloading of the big, locked files from the agent machine to the server for analysis (databases, email databases, chat logs, big files that could be deleted – created feature resolves the problem of file integrity even if a user tries to delete this file during downloading);
- all file operation monitoring together with filter and template system;
- and also some other features.

Agent infrastructure maintenance also needed some special solutions, in particular:

- perform automatic update of agent versions installed in the network;
- protect agents from deletion or blocking;
- manage the situation when the server connection is lost.

It was also a challenging project for testers. The solution discovered to be especially antivirus compatibility sensible, and so QA team had to prepare detailed and extended test plans, and developers introduced a number of improvements that finally allowed the product to go peacefully together with a wide range of popular and locally widespread antivirus solutions.

A huge number of features also complicated regress testing. It was the project where Apriorit QA Department introduced Impact Analysis technique and now heavily uses it.

The initial team consisted of 6 developers and 3 testers. In 1 calendar year they prepared the first market-ready version of the product.

After the key customers' response and general public evaluation, the plan and roadmap for the second version was created. The team of 10 developers and 5 testers took the next stage.

The Impact:

Knowledge and expertise of Apriorit team made it possible to bring the product version to the market and gain certain success there. Building various limited versions allowed the Client to faster and better research customer response. Based on their needs, the plans for the further development were created.

While the solution is still developing, its current version is supported by only 3-person team. Such work efficiency for a feature-rich solution is achieved due to the flexible architecture and well shared product knowledge of the team.

What's next?

Get the **free estimation** of time and effort for your project! After initial research, we'll provide you with the basic task dropdown and estimates indicating approaches and tools we can use to save your budget.

All we need is a brief project description sent to the info@apriorit.com with "RFP" mentioned in the subject.

Apriorit Inc.

Headquarters
Plehanova str. 34B,
Dnipropetrovsk, Ukraine
49000

Phone
+380 (50) 340 1747

Web
info@apriorit.com
www.apriorit.com