For Infrastructure & Operations Professionals

May 24, 2011

Case Study: Gaining Visibility Into The Experiences And Issues Of Securitas France Users

By Jean-Pierre Garbani

With Doug Washburn, Evelyn Hubbert, and Lindsey Kempton

Executive Summary

Security services is a growth industry fueled by global development and the need, in many countries,for custom services such as specialized guarding and surveillance. This demand for security services is amplified by the generalized use of technology. In 1998, Securitas Security Services, a Swedish company, acquired Proteg, a French security services company. This acquisition and the security market expansion transformed the French IT department: From a relatively limited and older set of applications, Securitas France had to move to more modern and reliable IT services. In an obviously security-conscious business, assessing the vulnerability of workstations was of prime importance. But gaining better visibility into application flows to and from end users soon became another requirement. How to select a solution that is simple, pragmatic, scalable, and evolving in functionalities without taxing a very cost-conscious IT organization was a challenge that Securitas France overcame successfully by selecting Nexthink's solution.

Situation: Rethinking the it role to better Support Securitas France end users

Created in 1934 with only three employees, Securitas is now a world leader in security services and surveillance. Headquartered in Sweden, it's represented in 45 countries and has more than 280,000 employees. Securitas offers, among others, services in guarding, risk management, monitoring, consulting, and investigations. Securitas services apply to a variety of industry segments and company sizes; for example, several hundred Securitas cars patrol the streets of Stockholm every night.

Securitas' business expansion in France was a catalyst to seek better and updated IT services. Originally, relatively old and limited IT solutions were used, and a complete rethinking of IT services was inorder. One of the key elements of this IT renewal, in a highly security-conscious organization, was the vulnerability assessment and the overall management of user workstations, which rapidly became a key objective of the transformation project.

The initial goal was to gain visibility into users' workstations: activities, governance, adherence to the company's rules, and visibility into potential security risks. In the meantime, however, Securitas France had deployed an enterprise resource planning (ERP) system — PeopleSoft — with five key applications.

This deployment led to a keen interest in understanding better the customer experience around the availability of applications services, the true service level seen by the end user, visibility into service usage, and generally a better understanding of transaction flows and workloads.

Best practice: Securitas understands its business and end user requirements

To successfully gain visibility into its users' workstations, Securitas France was challenged to find a single tool that could provide complete visibility into workstation activities while preserving the privacy of users. Although several products on the market offered access to partially relevant information, the Securitas approach was mindful to not fall into a "technology trap"

of using multiple agents that would each provide only partial answers. Likewise, the nature of Securitas France's business calls for narrow margins, and total cost of ownership (TCO) is a very important parameter when it comes to IT. As a result, the selection of an end user management tool had to be:

· **Simple and pragmatic.** Most of the Securitas France personnel are composed of security agents. With only 45 employees in the IT department, there are precious little resources available to deploy and maintain complex and resource-hungry solutions.

· **Scalable and evolving.** While Securitas France is initially deploying the tool to only internal staff, in the future, it may reach into its customers' workstations and expand the tool's use to collect even more information about end users in terms of compliance and licensing rules' conformity.

The results: Securitas met scalability and cost requirement

The security organization's goal was to select a single tool that would achieve the expected results, but with the potential to evolve and do more, instead of deploying several agents, each with separate functions and reporting tools. Ultimately, Securitas France selected Nexthink. This proved to bethe right choice for the security organization because the Nexthink application fits within theTCO constraints and is both scalable and versatile in functionalities. It's a simple tool to use and deploy, yet it provides complete visibility into end user activities as well as the workstation and its software and hardware inventory. As part of the selection process, Securitas France ran a proof of concept (POC) to assess how the solution would conform to its requirements. Because of the project preparation, the solution was deployed in a big bang fashion within the next six months and yielded immediate results: According to Securitas France, it used less than 20% of a full-time equivalent (FTE) to support the Nexthink solution. This was the type of return on investment (ROI) Securitas France was looking for.

Next steps: Securitas plans for better services

The results it achieved internally has broadened the scope for how Securitas France will use the Nexthink application. Because of its ease of use and its adoption by IT, Securitas France now uses Nexthink to reach clients' workstations where it ensures that they conform to their organizations' policies. But the real expansion will come to the adoption by other Securitas organizations: The efficiency of the solution has attracted the attention of other countries. Over time, the word about France's result will spread and lead to more deployments and deliver similar benefits.

May 24, 2011 © 2011, Forrester Research, Inc. Reproduction Prohibited

Case Study: Gaining Visibility Into The Experiences And Issues Of Securitas France Users 3 For Infrastructure & Operations Professionals

RECOMMENDATIONS:

How to apply Securitas France's best practices to your organization

Securitas France achieved its functionality goals and stayed within the cost and TCO parameters that it initially set. The selection of an end user management solution was the key element inthe overall success of this operation. By keeping a cool head and thinking ahead to deployment and support, Securitas France selected not only the solution that fit its functional requirements but also avoided the technology trap pitfall of deploying complex solutions to resolve simple problems. To achieve similar success in your own environment, infrastructure and operations (I&O) professionals should:

· **Define your requirements in steps.** Again, with a look toward efficiency, define a first set of features to be deployed, and then gradually expand the scope of the project.

· **Look beyond the hype and license costs.** TCO was a driving parameter for Securitas whenit was evaluating and selecting its end user management tool — but this calculation requires more than just license costs. I&O professionals should ensure that their requirements also include functional, support, and maintenance costs parameters. Insist on a product evolution road map to ensure that the product will scale in both dimensions for your future needs.

· **Run a poc as part of the selection process.** This is a key step Securitas France undertookto ensure that the newly selected end user management solution met its functional, support, and security requirements. I&O professionals can do the same by making sure that all functionalities are proven and effectively fit their requirements.