

## **Choose Products Designed Specifically for Homeland Security Missions**

**SAP and other vendors have repackaged applications to address homeland security needs. However, most enterprises will do better by selecting products developed directly for this area or by looking at data integration strategies.**

---

**Event:** On 27 February 2003, SAP briefed Gartner on SAP Security Resource Management, its homeland security offering.

**First Take:** Like many vendors, SAP seeks to cash in on homeland defense spending by U.S. federal agencies and other governments worldwide. Accordingly, SAP has put new packaging around previously released e-government and supply chain offerings. SAP will first target customers involved in homeland defense, border control, customs and emergency management. SAP did not develop the repackaged offering specifically for these missions. However, customers that have homeland defense-related information already managed in an SAP application should consider Security Resource Management, provided SAP can extend the functions efficiently to homeland defense missions.

Other vendors have taken a similar approach to the homeland security market. In Gartner's opinion, vendors that repackage products without developing functions customized for homeland security missions will not have much success. They must work to understand the roles and missions of government and critical infrastructure owners, and their needs for integrating data and communications, interoperability, and collaboration. It will take patient effort to spot the real opportunities and strong development to solve the real problems of homeland security. Homeland security encompasses such a broad set of processes that a single solution will not be forthcoming in the near future. In certain cases, individual modules may be appropriate — for example, software developed for those responding to hazardous materials may work well in biological attacks. But enterprises should understand what they are getting.

Until SAP and other business application vendors develop specialized applications for homeland defense, most enterprises should look to niche providers with mission-specific solutions. Vendors whose products directly address a homeland security issue or that design new products for specific homeland security problems offer the best chance of success.

Data integration products and skills should take a higher priority than repackaged enterprise applications that focus on internally managed data. Enterprise systems may work when the scope of control encompasses all available or required data. But the main obstacle to the use of business systems in the homeland security role is that they are designed for viewing and analyzing internally owned data, not the external data necessary to coordinate emergency response teams, or to monitor customs and shipping. Therefore, the key task is integration with disparate systems, not a single monolithic system.

### **Gartner**

**Analytical Sources:** French Caldwell, Daniel Miklovic, Kristian Steenstrup and Rich Mogull, Gartner Research

### **Recommended Reading and Related Research**

- “Know How Much Homeland Cybersecurity Will Cost You” — To manage homeland cybersecurity costs more effectively, enterprises should use a total cost of ownership model, by which they can assess their current and planned homeland cybersecurity costs across a broad range of categories. **By Roberta Witty**
- “GIS: Public Access for and Against Homeland Security” — We recommend that government organizations first scrutinize and then classify as sensitive certain kinds of geospatial information that are freely and anonymously available via the Internet. **By Gregg Kreizman**

(You may need to sign in or be a Gartner client to access all of this content.)