



March 2005

How to Buy Access Control Software

Choose wisely and work with a few good companies that provide quality rather than a group of mediocre ones.

By D. Douglas Graham, Contributing Writer

Security dealers or integrators should exercise as much care and caution when purchasing access control software as they do when buying a new car. The selection of the right vendor can be just as important as one's choice of automotive make and model, and so it goes with control access software.

Choose wisely, security industry experts recommend. Although the marketplace is replete with software providers, not all will be up to the task of servicing the products they sell.

"There's a lot more involved in the purchase of access control software than simply buying the program," points out Jeff Koziol, product manager, access control, Ingersoll-Rand Security and Safety, Bristol, Conn., a mechanical and electronic control and life safety company.

"Security product dealers often pick two or three strategic providers to partner with and leave it there," Koziol asserts. "Partner with too many suppliers, and you run into a control problem. All software comes with a learning curve, so you'd better make sure your supplier has good service techs onboard.

"The suppliers you pick should therefore be vested in security products and ready to service them after the sale," he advises. "You don't want to deal with 10 jack-of-all-trade software houses when a couple will do just fine. It makes far better business sense to work with a few good companies than a bunch of mediocre ones. Quality, not quantity, is what you should be looking for in software providers, bottom line."

Picking the Package

Because more software packages are available in the marketplace than suppliers selling them, the next trick will be to determine which product will work best for you and your client. Decision-making in this area should be based on the answers to a series of questions focusing first on the

environment in which the system will be deployed and the uses to which it will be put.

Important considerations should include the number of doors requiring control, the number of people receiving access and how frequently the system will need to be adjusted at each location to accommodate personnel changes.

The answers to such questions will indicate the type of software required. For example, a system controlling an access point with 1,000 users will need to be highly robust and scalable. Do not hesitate to ask the supplier whether the system can be upgraded and what the cost would be.

Integration can influence the purchase decision. If a client wants to add a video component or a graphics package that allows for remote viewing of a facility's access ports via a computer monitor, will one or both enhancements require the use of a totally different software platform? If the answer is yes, then such a software system may entail additional expense.

Another key concern is the issue of remote locking. In the majority of access control applications, all the data required for entry is input at the point of access – a card is swiped, a key is pushed, a biometric reading is taken and the door unlocks and opens.

However, occasionally clients may wish to open the door and keep it open from some other location. Others may opt for CCTV or some similar method of visual monitoring. Will the software package in question address this possibility or will augmentation be required?

Visual monitoring also may mean new hardware that the company providing the system will want to sell separately, which also can increase expense.

"Make certain the system you select is scalable and expandable," recommends June Colagreco, director of marketing communications, Honeywell Access Systems, Oak Creek, Wis., a provider of access control products. "You will need to know sooner, not later, what and how many third-party pieces can be added to the package. You don't want to be locked into two and wind up needing six.

"Say your client is a mini-mall that buys the equipment for surveillance monitoring," Colagreco suggests. "If the owner buys the building next door, he will need to expand his system, so the system he has already had better be expandable. Take nothing for granted. Make sure the package you invest in covers all possible contingencies."

Customer interest in software applications being accessible offline is increasing, adds Jay Vaitkus, product and market manager, Stanley Security Solutions Inc., Indianapolis, a provider of access and security solutions for institutional, commercial and industrial businesses and organizations.

For example, Vaitkus suggests, in a college dormitory in which conduit cannot be run to a remote door, an online system in which the door lock is hard-wired to the controller could not be used. An offline, self-contained system may be the only option in such a case.

Sometimes both types of systems will be operating at the same facility. In such situations, one must know whether a separate system is required for each or whether one system that works online and offline is acceptable.

What about the Operating System?

"You will probably want a platform that is based on a network-based operating system (NOS)," advises Peter Boriskin, director of technology for Tyco's Access Control and Video Systems, Software House, a wholly-owned subsidiary of Tyco Fire and Security, Lexington, Mass. "Your technicians ought to be able to work with whatever platform you chose. It should be something secure and reliable but easily supportable."

If the package under consideration is open-architecture and Windows-based, ask if it is up to par with current operating systems and PCs. A software platform not supported by the latest Windows operating systems may not allow certain older-generation systems to run. It is vital that providers keep up with the most recent generation of Microsoft products.

Although a system running on open architecture offers many advantages (not the least of which is that it is much easier to add peripheral equipment to an open-architecture system than a closed one), it has at least one significant drawback. Because open architecture is "open," it can be compromised.

A closed system is unbreakable because everything is managed by the provider of the software. However, a closed system also can be problematic, because when the provider goes out of business, its tech support department goes with it.

Sidebar: Can Your Software Do This?

Access control software ought to be multitalented. It should have the ability to cover multiple credentials and support keypad, code, mag-stripe, proximity and biometrics.

It also should be programmed to allow users to create and manage their own badging modules. Features such as these create value. The right package will provide all of that, and the right provider that and more.

"A security dealer in need of control access software should first determine which manufacturer is likely to bring the most value to the table," recommends Robert Bayer, director of sales for PSCS Corp., Torrance, Calif., a building security and management solutions provider. "A dealer will want to work with someone who can provide products that will help him expand his business.

"The provider should fully understand the security requirements of customers and have a line of product available designed to meet the full range of their need, be that a standalone system or a package sophisticated enough to provide access control for an entire country," Bayer advises. "It's really all about value bottom-line – first the value offered by your provider, and secondly the value you as a dealer pass along to your customers."