

FEATURE SETS THAT SELL

End users need to get more out of their access control features than ever before — their budgets demand a balance between feature sets and usability.

By **Karyn Hodgson**, Contributing Writer

For the third consecutive year, *SDM*'s exclusive report, "Access Control: Feature Sets that Sell," seeks to identify what features and functions make access control systems appeal to end users. This year, it is apparent that many of the same features as in previous years top the list, but there is more. End users are increasingly faced with tougher choices about where to spend their limited funds. Making more of their existing investment, software upgrades and a renewed look at how the access control integrates with other areas of the busi-

ness are bigger concerns, according to many manufacturers and integrators.

"They want more for less," says Matthew Ladd, president and COO, The Protection Bureau, Exton, Pa. "Budgets are getting tighter and tighter, but security is still expected to perform with less capital money."

Joseph Dahlquist, product manager, Chamberlain Access Solutions, Elmhurst, Ill., agrees that customers want to see profit come out of their expenditures. "In today's economy end users are only interested in retrofitting, upgrading or expanding their sites with solutions that will help them to become more profitable."

This places an extra burden on the customer to choose wisely, adds Jennifer Toscano, marketing manager, Ingersoll Rand Security Technologies, Carmel, Ind. "The average end user gets to make a choice every 10 to 15 years. When you only get to make a choice that seldom, the significance is pretty impactful. The customer wants to feel comfortable making that choice and moving forward with a system that will fit their needs today and in the future."



PROTECTING THE INVESTMENT

Whether they are investing in a whole new access control system or just trying to maximize the one they have, end users are very interested in making sure their investment is protected, both from a physical sense and an economic one. And manufacturers are responding with solutions that fit the bill.

“We have a lot of product that has been sold over the last 15 or 20 years,” says Richard Sedivy, director of marketing, DoorKing Inc., Inglewood, Calif. “People are not replacing those systems right now. They are maintaining what they have rather than going through the expense of installing new. Seeing that, we wanted to come up with a way to further service those users better in this day of the Internet.”

DoorKing in essence manages the old modem updates for them while giving them a modern Internet interface to work with. “Essentially we’ve provided for old systems that people are reluctant to replace right now because of the economy and given them an Internet-programmable system at very little cost.”

Chamberlain, too, had to rethink its customer approach. “The slowed economy has caused business owners to investigate solutions that can help them run their businesses more efficiently and profitably,” Dahlquist says. “Our AccessMaster Overlock system addresses these needs by automating processes and deterring tailgating, while increasing the visible security at each unit door.” It can also operate wirelessly, he says.

“In some ways the economy has changed the way people think about the investment they are making,” Toscano believes. “We have a new series of AD electronic locks that enable a dealer or end user to purchase a lock and put it on an opening with one credential reader and, as needs change in the future, switch out the module for a smart card, while still keeping the mechanical lock on the door. They like the idea of making a choice that protects their investment for the future.”

Rob Blasofsel, access/video integration manager, Honeywell, Melville, N.Y., agrees.

“Both consultants and end users are looking for resourceful ways to capitalize on existing investments verses having to go in and replace them. Our approach to the end-user tech transition is based on business improvement consulting services. It allows for a mutually beneficial relationship between the manufacturer, dealer and end user and we end up helping our customers plan for tomorrow.”

PCSC, Torrance, Calif., is focusing on helping customers protect their investment by offering true

redundancy. “As we get more and more into the IP world there is more of a push for redundancy or fault tolerance, meaning that it can’t fail as long as one controller is up and running,” says Brian Lyle, director of sales. “In the security market people are starting to see what IT people have been living for many years.”

Some end users are using existing access control features in a new way, such as mapping and floor plans, says David Barnard, director of dealer development, RS2, Munster, Ind. “They are dealing with more limited resources. Instead of an officer in each building who knows that building, now they may be dealing with a centralized guard station that is managing multiple buildings and may not even have seen the building. Graphic maps help them administer that much more effectively.”

Gloria Lubben, CPP, executive vice president at SecureAlarm Systems, Grand Rapids, Mich., adds: “I would say that what people have been doing is looking for ways to have their access system do more — not to create a separate system for new issues they are facing, but looking to see if their system has a new way to save them time, money and make them more efficient.

Wish List

End users want access control systems to do more than ever before, but don’t necessarily have the funds to invest in a lot of new hardware. Today’s top list of desired features could include many of the following:

IP or Web-based — Using the power of the Ethernet and existing infrastructure to maximize benefit.

Ease of use — Interactive, efficient and able to make formerly challenging things easier.

Integration — With logical access control, CCTV systems, human resources, HVAC and time-and-attendance.

Software-based — Including partitioning and the ability to upgrade easily and quickly to multiple users.

Managed access — Some end users would like integrators to do the hard part, allowing them to focus on *using* rather than maintaining the system.

Wireless — Allowing them to put access control into areas that otherwise would be cost-prohibitive or not easy to install.

Scalable — The ability to upgrade without having to change hardware.

Open architecture — Allowing them to use multiple different systems and make them all work together.

Reliable — Consistent performance year after year.

FEATURE SETS THAT SELL

SOFTWARE SOLUTIONS

“Where manufacturers have stepped into the limelight is by making it more about the software than the physical access solution,” Lubben says. “We are seeing a lot of clients looking at their access control platform as a database. What are its capabilities to be able to share data with other business management throughout the organization? Does it share information nicely? Is it an open platform? When an office can put someone new into their database and have it automatically download into security’s database it is a real advantage to people.”

Lyle feels this trend is being extended by SDKs. “There is an expectation now that software kits become more available and can take and interface different field applications more readily and easily than ever before. You can build your own entire system with different interfaces because of the way the technology is now with the software development kits.”

Paul Ahern, vice president/general manager, Cypress Computer Systems, Lapeer, Mich., thinks this is a major trend, as well. “The biggest thing I am hearing is people looking for more of a Web-type interface versus traditional PC-based interfaces. They are looking for an IP-type solution that is a little more robust than the traditional.”

RS2 introduced a Web-based client a little over a year ago, Barnard says. “We have seen quite a bit of movement to that, especially with larger end users where they have multiple locations across the United States. They might have 25 to 30 workstations. Every time the software was due for upgrade they would have to upgrade all 30 and the internal head-

aches were growing as the system grew. By going to the Web-based client the user can update that software in one location and all the other users just log in remotely via the Web and are taken care of.”

Blasofsel refers to this as virtualization. “People are taking what would normally be the Windows OS and packaging into a virtual file on a virtual computer. Instead of running one computer they can put 15 physical servers onto one server and it saves IT and security a lot of money. That has really been on the rise this past year.”

Web or IP-based system offer advantages in programming and streamlining operations, Ladd says. “Web clients are very much a preference. Everyone wants to access the system whenever they can through the browser or smart phone. It used to be that security directors and staff would provide all reporting. Now as systems develop, the security director can say ‘run the report yourself.’ Their log-in will give them access to their people and the security director can distribute that responsibility of reporting.”

JOINING FORCES

Software and Internet-based platforms allow for much more integration with other systems and customers are taking advantage of that.

“End users are looking for stronger and growing software integration for their management operating systems and HR style programs,” Ladd says. “They also continue to push and request for integration with building management systems.”

For some it’s about compliance issues, says Tom Donovan, president, Tri-Electronics Inc., Hammond,

Video Takes the Lead as Integration Platform

The same economic situations that have end users hanging onto their access systems longer and changing the way they think about how they are used has seemed to serve as an impetus to invest in video surveillance.

“Video is where we have seen major change in electronic security in recent years,” says Matthew Ladd of The Protection Bureau. “In the past we have seen access integrated with video but access was the lead program. Now I am seeing that video is the lead program and access is an addition to it.”

David W. Barnard of RS2, agrees. “One of the hottest sellers we have

now is the DVR and NVR integrations. Access control has been doing okay, but video is going great guns. DVR/NVR integration allows the end user to maximize their money by having integration with access control.”

Customers see value in integrating video, adds Gloria Lubben, CPP, of SecureAlarm Systems. “A lot of clients are pretty big on video. They think ‘if I can’t have people, at least give me tools that make me more effective.’ There are a lot of dollars being spent on video. But we strongly recommend they synchronize it in a single database with access control.”



Integrating video surveillance with access is undergoing renewed interest because of advancements on the video side and enhanced capabilities of its integration with access control.

PHOTO COURTESY OF RS2

Ind. “Today people are trying more and more to authenticate time and attendance compliance issues, controlling who goes to what door at what time.”

Other facilities are using security systems to help them “go green,” Lubben says. “They are taking that information and applying it to some of their green initiatives such as energy efficiency, lighting and HVAC control. The green initiative has created opportunities to be creative with technology.”

Dahlquist has seen this trend manifested in using access control for automating certain functions.

‘You can have a product with all the bells and whistles, but if it is hard to use, it will be hard for the customer to embrace it. There should be a balance between feature sets and usability.’

“Lighting automation is a feature of our access control system that we are beginning to see more in installations. With the revitalized focus on energy efficiency and automation tools, more facilities are realizing savings as a result of leveraging the lighting zone automation of the system.”

Another developing solution is the integration of physical and logical access control, allowing end users to do things such as making sure that the person logging onto the computer is actually physically in the building and using the same credential or smart card for both actions.

MAKING IT EASIER

There is still one overreaching “feature” that virtually all customers place a high priority on: ease of use.

“Customers are looking for systems that are simple to use, very interactive and simple to drive with the overall system capability,” Lyle says.

In addition to being easy to understand and operate, it could also mean efficiency, too. “Just getting all the information to where it is usable and having a more robust database instead of having to enter information over and over again makes things simpler,” Ahern says. “Having something that maintains everything and they don’t have to do a lot of maintenance if an employee’s information changes is key.”

Toscano agrees. “You can have a product with all the bells and whistles, but if it is hard to use, it will be hard for the customer to embrace it. There

should be a balance between feature sets and usability. If they can’t understand that an alarm has been generated, what good does it do?”

Just because technology is king, that doesn’t mean it should be overpowering. “At a time when technology is king, and features and capabilities are of such interest to decision makers, it’s dangerous to allow products or the interfaces used to control them to become difficult to understand or operate,” Dahlquist believes.

Ideally, a good access control solution should make the end user’s job easier, says Jim Ballatin, senior account representative, Blue Ridge Security Systems Inc., Anderson, S.C. “These days there may be a lot of different people that manage a system. It is no longer automatically a security manager or IT manager; it could be the office manager changing settings. Ease of use becomes very important. Access control needs to be instantly changed should an event happen. We had a situation with one customer where the customer laid off their access control manager and we had to retrain an employee because that was the only person who knew how to do things.”

One way The Protection Bureau is making things easier for clients is by offering managed services. “A lot of clients are switching to managed services,” Ladd says. “We are working on one project now where we are replacing their guard station and doing everything remotely through cameras.”

There is clear value to such a solution, according to Barnard. “Instead of buying an access control head end, some end users are looking...cloud-based solutions where they have the access control equipment but it is more like a central station scenario. Some of these smaller to mid-size companies especially may not have an internal IT department so they rely on someone outside to manage their infrastructure for them.”

What does all this mean for dealer and integrators?

Lubben thinks end users are getting savvier about shopping for solutions. “Customers are being more deliberate about decision-making processes. They want to make sure if they spend money they are not going to have to re-spend it in a couple of years.”

Ladd suggests that the best way to stay on top as a dealer or integrator is to make it more about solutions. “I think the industry in general got into a habit when times were good of selling product and not solutions. Now that clients’ budgets are tighter and competition is higher, clients want integrators that can help give them a solution to their needs and not just hardware for it.” ■