ENTERPRISE SECURITY: IT'S A NATURAL TREND

PHOTO COURTESY OF PCSC

Enterprise access is increasing in popularity, not because there has been huge growth of companies, but because of the economies of scale with respect to standardized processes and how they manage facilities.

By Karyn Hodgson, Contributing Writer

ABOVE: *Enterprise access allows a user to centrally manage the system, making maintenance and updates much easier than with disparate access control systems.*

What makes an enterprise-level access control system tick? Is it merely the size? The method of communication? Or something more? Access control systems were one of the first genuinely networked security systems before "networked" was even well-understood in physical security. As the methods and players have changed, the definitions have continued to evolve and expand as well.

"For us, enterprise means a large system that is scalable, can be used across industries and is centrally controlled," says Gary Staley, national sales director and founding partner, RS2, Munster, Ind.

Rick Focke, senior product manager, Tyco Security Products, Westford, Mass., stresses the global nature of enterprise access. "It allows the end user to run global reports of a person's whereabouts as well as manage central alarms from one place. They can see at a glance what controllers are on line or off line."

Most enterprise-level access systems have grown slowly over time, rather than being installed as a single, cohesive system. Mergers and acquisitions, expansion and other factors often mean that an end user has at least two and often more access control systems to contend with and make workable.

"The security industry overall has a lot of older equipment that gets used a lot longer, especially compared to IT equipment," adds Beth Thomas, senior product marketing manager, Honeywell, Louisville, Ky. "Security lifespan is upwards of 10 to 15 years and there comes a logical point in time where they want that equipment to do more. Maybe they need extra features. But over time a lot of needs evolve and security becomes more involved."

The challenge for integrators is to take these disparate, sometimes older parts and put them together in a cohesive way to make an enterprise system that benefits the end user.

TRENDS & BENEFITS

Enterprise access control allows end users to centrally manage a system that was once a collection of sites that didn't have much, if any, communication with each other.

"Enterprise access allows the user to centrally manage the system so it doesn't have to be managed at each separate location," says Greg Hetrick, marketing manager, PCSC, Torrance, Calif. "From a maintenance and update standpoint, this makes things a lot easier."

One reason is the ability to take full advantage of the mature and stable networking opportunities that exist today.

"Generally facilities are trying to get away from duplication of efforts and multiple databases," says Bob Mosler, national sales manager, Infinias, Indianapolis. "They are trying to gain consistency. Using data networks makes life simpler and allows security to interface with IT. They also get consistency in building security procedures and processes across the enterprise. They can centralize the decision about what they are going to do and how they are going to do it."

Networks are in large part responsible for the enterprise movement continuing to march forward, adds Walter Helms, vice president and chief technology officer, Matrix Systems, Dayton, Ohio.

"Some of our customers are starting to rethink and consolidate now. When we first started putting these systems in, the networks were pretty fragile. As IT infrastructure gets better and better everything is going IP-based in the security world. The old argument of whether or not to trust the network is a moot point. Now, if you don't, none of these new systems will work at all and you can't be up with modern technology."

Using the company network has mutual benefits for both security and IT. "They end up all on the same version, which is helpful for training," Helms says. "Things tend to change across a corporation. Now you can get uniformity. Also with fewer servers and everything operating from the same place there is a lot to be said on the maintenance side. It is lot easier for the IT guys to maintain databases — a lot less work."

Indeed, IP-based systems are probably the greatest recent trend in both video and access control on

PHOTO COURTESY OF PCSC

Enterprise systems are often organized into either one central server or multiple regional servers.

The Economy's Effect on Enterprise Systems

The past few years have been tough on the pocketbooks of everyone from individual consumers to large corporations. How has the economy impacted integrators' ability to sell and install enterprise access systems?

On the surface, you would think business might have suffered for such large expenditures. And in some cases it has, but in others just the opposite occurred.

"In the last two years the demand has slowed for these systems," says Gary Staley, national sales director and founding partner, RS2. "Typically enterprise applications are the big dollar amounts. People are just not budgeting for large numbers right now. But it doesn't mean our business is down, just that not as much involves enterprise-class installations."

Bob Mosler, national sales manager, Infinias, agrees.

"I think it is probably that the demand and purchase are two different things. The call for it is high, but due to the economy what we have seen are projects being pushed back from year to year trying to get funding. The demand is higher than ever, but financial considerations are pushing it back at the moment."

Matrix Systems, Dayton, Ohio, has recently begun to see a loosening of the purse strings, says Walter Helms, vice president and CTO. "What we were seeing more than a year ago was a lot of capital being put on the shelf. There were a lot of systems in the works. Now they have loosened up that capital to the point where they are doing the upgrades."

That is good news as Rick Focke, senior product manager of Tyco, sees it. "I think we are starting to see the light at the end of the tunnel. The last year has been tough. Even smaller jobs were getting more bidders on them. Enterprise jobs in a lot of cases have been put on hold for funding reasons. It is a grudging purchase. But it seems like there are a lot of projects back on the table now. It's a little tougher for integrators, but we are seeing some good traction now. In general IT spending is up because companies stopped spending in the last few years. Now the wave is building to upgrade."

On the flip side, some organizations are looking into enterprise systems from a cost savings perspective.

"What I have observed is that enterprise projects tend to happen over multiple years," says Beth Thomas, senior product marketing manager at Honeywell. "Projects have been ongoing and may have slowed down a bit but they have not stopped at all. Likewise, other companies that may not have been down that path have put plans in place because of the beneficial costs of consolidation."

PHOTO COURTESY OF PCSC

Replication is the process of taking the information from one server and duplicating on another.

PHOTO COURTESY OF TYCO SECURITY PRODUCTS

Enterprise systems allow users to run global reports and manage alarms all from one location.

the security side, says Stephanie Hensler, director of EAC OEM sales, ASSA ABLOY, New Haven, Conn., a trend that is definitely being felt in the enterprise arena.

Web interfaces are also adding to the benefits enterprise access has to offer.

But in uncertain economic times, enterprise access may have even more to bring to the table.

"Ultimately it saves the client money," Focke says. "They have to have readers no matter what. The physical equipment is there anyway. There might be some extra cost in the servers, etc., but the manpower and efficiency savings more than make up for it."

Thomas adds: "I would say enterprise access is increasing in popularity, not because there has been huge growth of companies, but because of the economies of scale with respect to standardized processes and how they manage facilities. It's everything from operator training, how you wire, how you install, how you manage policies and consistency across organizations. It reduces training costs. You can have operators in a central monitoring station do more or monitor more sites, especially when the user interface is consistent. When you can streamline training, resources, spare parts and processes it is far easier to maintain consistency across an organization."

In some cases end users are driven to consolidate, says Sean Leonard, marketing director of the services and product portfolio, Ingersoll Rand, Carmel, Ind. "There continues to be consolidation in the marketplace as industries mature and they are being increasingly driven by standards. Enterprise access is a cost effective way to meet those requirements as a business by streamlining their compliance efforts."

FUNCTION & FORM

So what does an enterprise access system look like today? What features and functions must be present to make it a workable and beneficial system? How are they set up?

One of the first key decisions is how the system will be partitioned.

"They are usually a multi-facility system," Helms explains. "One class of systems features a central computer at headquarters then literally dozens of remote sites scattered all over the country. The other kind is where you have multiple regional servers reporting back and coordinating through a central server. The purpose is to share information among regional servers. The key to enterprise systems is the flexibility of the architecture. They have to be able to handle variations such as multiple time zones, different holiday schedules, and different policies. All those things need to be considered in the architecture, whether you partition the database by separate servers or one large server.

"Essentially all remote sites are a series of workstations and access controllers out on the network, which is usually a corporate dedicated network. It doesn't physically matter where they are, whether they are down the block or on the other side of the continent."

First and foremost these systems rely on the Internet, Thomas says. "Usually when you talk about enterprise you are talking about WANs or virtual WANs using Ethernet connectivity. It is no different than what you see with IT systems."

That is important, Hensler adds. "The great thing about the Internet is the ability to have it encrypted."

Because, of course, we are talking about security and lots of cyberspace.

"It is critical to have encryption between everything," Focke emphasizes. "You must nail down the security of the system where it goes outside of the building and make sure it is as safe as possible. Also you want to make sure the database is open and rigorous and that the system can operate in virtual environments. A nice Web interface is another must-have now, and it needs to be encrypted, too."

Redundancy and replication are also key factors in a successful enterprise system. "One of the big features of enterprise is that people use redundancy so you can have standby machines in regional servers," Staley says. "Hot standby in the world of servers means that if a server has a malfunction it will fail over to server B. When we say 'hot redundancy' that means it is done automatically by computers without any intervention or touching of a machine."

Replication is the process of taking the information on one server and duplicating it on another. "These machines are all making their own decisions and controlling their own cities and not requiring bandwidth to be talking at all times," Staley explains. "But the regional servers communicate back to the main server at times that will least task the network. So intelligent servers are running on their own, but what we call 'database

Standards & How They Will Impact You

Pulling multiple security systems together across the miles and years can present no small challenge. That is why organizations such as Security Industry Association (SIA) and Physical Security Interoperability Alliance (PSIA) have dedicated groups working on making communication between systems easier.

SIA's open systems integration and performance standards (OSIPS) family is actively working on two new standards that will help information sharing among access control systems. The access control role (ACR) standard defines an interface to an access point that manages both the access point components and the process of seeking access approval. The access control role (ACR) defines the interface of a role-based access calculation that unifies physical and logical access.

"Any kind of access point has to address a myriad of devices physical or logical," says Monica Rigano, director of standards, SIA, Alexandria, Va. "If you think about that at the access point, APC is looking at all that messaging to support that. ACR is really where you are calculating stuff. Is this person really who they say they are? Do we need look up data elsewhere?

"It is more of, what is the information requirement and how do you define those pieces of information so it is commonly understood by all, even non-security systems?"

Rigano stresses that information is non application-specific. "The realization is that the message supported could be anything. It doesn't care if it is someone providing a credential at a door or a log-in at a computer. It is that kind of thinking and concept. At the application level, does it play well with other applications?"

While this standard will affect development at the manufacturing level, ultimately it will help the integrator by standardizing messaging elements across the enterprise.

SIA hopes to have these standards ready for public review later this year, Rigano says.

PSIA is not a standards organization, but a global consortium of more than 70 security manufacturers and integrators focusing on promoting interoperability of IP-enabled devices across every segment of the security industry. One such member is Bret Tobey, intelligent openings business development and product manager for ASSA ABLOY, New Haven, Conn.

"Enterprise customers are the ones that go to network-enabled systems first," Tobey says. "Any time a certain device needs to communicate with a system, even though it is an 'open system' you have to have a driver to make that work." PSIA is dedicated to simplifying and standardizing this process.

"It is difficult to keep access control up-to-date at a data or system level as devices all get smarter. Say company A buys company B and now has two access control systems. As new company C it is critical to all that they share that access information. It is not realistic to just upgrade to one new system. It is very reasonable to communicate over the Internet or Ethernet to frame information so it is understandable. In the past this has been really expensive and system interfaces take a lot of money to develop and maintain. By coming up with a standard way of doing things, groups like SIA have done a fantastic job of creating definitions. PSIA is focused on general agreement within the industry. We want to figure out how to pass basic messages back and forth. Once we have done that the cost of maintaining those interfaces goes down."

PSIA's Area Control working group is focused on coming up with its first basic capabilities by 2011. This "working framework" will leverage other standards to figure out how to most efficiently pass the information.

"We will add new types of value and savvy integrators are going to say, 'Hey, we can leverage that value.' Even folks who don't have IT-savvy roots will benefit. The fact that they are still in business means they have figured out some way to work with IT. As these systems become easier to communicate with, they may find that it is easier to work in this enterprise arena. Maybe in the past they saw the hurdles as too high, but now it will be possible."

PHOTO COURTESY OF INGERSOLL RAND

Access control readers communicate at the door and to the local or master server, allowing for communication of events throughout the enterprise.

replication' is where they are replicating that information back to the main server so they all carry the same information."

Replication is more than just sharing information, Focke adds. "We basically have a collection of servers and one master server. In previous systems orchestration was just personnel records. What we are doing today is orchestrating everything. The entire global database is replicated, creating a master report of all readers, or a global alarm history for that type of alarm. It is a level of magnitude up from previous generations of enterprise systems."

> ***If the integrator can take the vision, gather the requirements and have the right discussion with IT, they can be very successful.***

With higher functionality comes higher responsibility. "There are a lot of what-ifs," Focke describes. "How do you recover if the server is off-line? How do you set up servers and security privileges? Does the system give you the power to slice and dice operators' privileges? What alarms and doors do you get to see?"

Mosler emphasizes, "It is critical today to have a partnership with the IT group and determine how it will fit on their network and be implemented from that standpoint. Who will maintain where the servers will reside? How will you interface with the database engine? Will you have to add to that system?"

Another issue is reader and badge technologies. "These systems tend to grow over time and you often end up with a hodgepodge," Helms admits. "The system architecture has to be able to handle all those. Often that means relying on multi-tech readers or cards (or both) as a temporary or long-term transition strategy. The system has to be able to handle various card types and treat them as one. There are a lot of legacy issues in enterprise systems."

THE IT FACTOR

Not long ago (and in some circles, still) the idea of working with IT was enough to strike fear into integrators and security directors alike. But today's enterprise systems can't function successfully without IT and their networks.

So what can integrators do to make the process go as smoothly as possible? "Get a strong knowledge in the vocabulary of the IT folks," Thomas says. "If you can speak their language you can be a lot more effective in helping physical security be more successful. They will lean on you to approach IT and get things approved. In a lot of cases physical security has a clear vision of what they want to protect but don't understand a lot of the technology. If the integrator can take the vision, gather the requirements and have the right discussion with IT, they can be very successful."

Focke recommends getting both employees and technicians trained in the latest IT technology and terminology and being well-versed in both virtual environments and networking skills. "More and more of the percentage of your employees need to be IT savvy than not."

Mosler says, "If you haven't moved into the IP world yet, you need to. That is where a lot of integrators have struggled over the last five to 10 years, making that transition from the analog hardwired system into the IP world. You need to become fluent so you can have intelligent discussions with the IP professionals. A lot of security people get nervous when they find out an IT person will be in the meeting, but you have to move forward with the technology."

With enterprise access systems it is the only way to ensure you give the end user the best, most up-to-date system that takes advantage of current IP-centric technology. ■