VANDERBILT

News

This article appeared in the September 2016 issue of SDM Magazine*. Read the full posting here.*

Enterprise access control clients are unique — even amongst themselves — in that their problems are often more complex, more difficult to solve and just bigger. Often involving multiple sites over large campuses or even across the globe, today's enterprise customers are cognizant of technology and its potential to help them with their biggest "pain points." What they don't know is how to get there. That is where the security integrator comes in.

"Larger enterprise installations require much more engineering and project management," says Bruce Stewart, business development manager, access control, Axis Communications Inc., Chelmsford, Mass. "Many different aspects need to come together at the enterprise level and, depending on the type of customer, the requirements can vary."

George Martinez, senior product manager for Software House C-Cure 9000 for Tyco Security Products, Westford, Mass., says there are two primary types of enterprise-level

customers. “First are those with multiple systems that are deployed and managed independently across their enterprise; and the second are those who have standardized on a centrally managed, multi-server architecture that is distributed across their enterprise. In either camp the historical trend of systems integration for increasing operational efficiency of these large systems continues. However, reducing security staff demand and lowering the operating and maintenance costs to manage these large systems has been the conversational shift recently with enterprise-class customers.”

Enterprise level installations are becoming more and more complex, says Scott Lindley, president, Farpointe Data, Sunnyvale, Calif. “No longer content to monitor and manage separate access control, fire alarm, video surveillance, intrusion and HVAC control systems, corporate security and technology, managers want to consolidate and integrate various disconnected security and facility management systems. At a dramatically increasing pace, the information technology (IT) department is leading the initiative, particularly given the trend toward convergence of physical and logical security systems.”

The key thing to understand, says Robert Laughlin, president, Galaxy Systems, Walkersville, Md., is that access control systems are no longer separate from other security and non-security systems, but almost always integrated and networked — especially at the enterprise level.

From intelligence to cybersecurity, cost to operational efficiency, convenience to compatibility, enterprise customers are increasingly asking their trusted security integrator advisors for solutions. Here are seven of the most common issues integrators are being asked to address.

1. INTELLIGENCE & EFFICIENCY

As the Internet of Things (IoT), Big Data and other trends proliferate, the enterprise is increasingly demanding ways to do more with their data, including their access control and other security systems.

“The biggest trends in access control are integrations with the rest of the world,” says Stuart Tucker, senior director of enterprise solutions, AMAG Technology, Torrance, Calif. “There is a lot of data captured by an access control system that, when correlated with other information can tell a lot about risk, utilization, and efficiency. As an industry we are just beginning to see the value in combining this type of data for use in security. This includes

areas such as insider threats, geolocation risk analysis and more."

Business intelligence can not only help an enterprise with its security processes, but go much deeper, adding value to the access control system.

"Our customers are increasingly looking for greater intelligence in access control software," says Jimmy Palatsoukas, senior manager, product marketing, Genetec Inc., Montreal. "Rather than responding to events, access control systems will be qualifying multiple events to trigger higher-level incidents so operators respond to what is actually happening as opposed to deciphering a situation based on incoming data."

Situational awareness and big data are two hot trends the enterprise is seeking to understand and utilize, says Brian Casey, general manager, SMB solutions, Honeywell Security & Fire, Melville, N.Y. "Select end users are starting to use their access control system as their overall situational awareness system — they are merging technologies such as fire alarm detection, shooter detection, gas detection, etc. to be able to identify problems on one platform, and then communicate to and manage their building occupants swiftly and accordingly.

"Though not a new concept, big data is about pooling large amounts of data captured by a system, analyzing it, and using the results to make improvements," Casey adds. "In the case of access control, there are many opportunities to aggregate and analyze tremendous amounts of data being generated to 1) Create better future products and 2) Allow end users to gain insight from the data captured. Ultimately this should enhance the security and increase the productivity of an end user's organization."

2. COMPATIBILITY

None of these high-level security or business functions can occur, however, until the systems reach the level of true interoperability. This has been achieved in the past with (often complex) integrations. But increasingly the industry is coming up with standards, protocols and unified offerings to make things easier.

For example, Mitchell Kane, President, Vanderbilt Industries, Parsippany, N.Y., says his company has introduced a custom-configurable data management system that integrates

its security management system with third-party disparate systems, “allowing for an automated business workflow between systems.” This allows enterprise customers to be more streamlined and leverage third-party systems they already have an investment in.

Genetec’s approach is one that is starting to take hold with a few large manufacturers in recent years: unified systems. “Our flagship, open-architecture IP security platform unifies access control, video management and automatic license plate readers into one user interface,” Palatsoukas explains. “[It] also enhances organizational security through unification with other network-connected devices and systems … and provides efficient workflows and greater automation through its unified interface, ensuring that more time can be spent monitoring critical tasks, rather than administrating software…. With correlated data from many systems, customers can make clearer and timelier security decisions based on more information.”

Industry-wide there has been an increasing interest in developing standards and protocols. While the video surveillance industry has done a good job on standardization, the access control industry in particular has been slower to respond. There are several efforts ongoing, from ONVIF Profiles aimed specifically at the access control industry to PSIA’s PLAI (Physical Logical Access Interoperability initiative) and the Security Industry Association’s OSDP (Open Supervised Device Protocol).

“Enterprise-class clients recognize that access control systems that support open standards provide interoperability and reduced supplier independence,” says Frank Gasztonyi, chief technology officer, Mercury Security, Long Beach, Calif. “Peripheral device interface standards, such as OSDP, future-proof reader deployments, and software interface standards such as PSIA, BACnet and IoT expand the security system’s ability to interoperate with non-security related applications.”

Farpointe also recently announced OSDP compatibility with its smart card readers, Lindley says. “OSDP helps ensure that numerous manufacturers’ products will work with each other. Importantly, interoperability can be achieved regardless of system architecture.”

3. COST

Large or small, customers never stray far from the central question, “What will it cost?” For

enterprise level customers costs are naturally higher because of the size of the project. But wireless technology and Power over Ethernet (PoE) are helping both decrease installation costs and increase the number of doors that can be controlled, which ultimately helps the enterprise in their quest for better and more complete control.

“Access control systems that are able to support …a mix of wired and wireless integrated door hardware options to provide cost-effective and appropriate solutions will allow facilities to secure a much larger percentage of access points than in the past,” Gasztonyi says.

ASSA ABLOY offers a wide range of options that can cover openings from the traditional to non-traditional (such as cabinets or IT racks in data centers), says Peter Boriskin, vice president of commercial product management, ASSA ABLOY, New Haven, Conn. “[One of the] most significant trends is better technology at lower costs, which creates the opportunity to bring access control to more openings throughout the enterprise,” he says. (See sidebar, page 90.)

Wireless locking allows the integrator to provide a mix-and-match solution between traditional and hardwired control panels and wireless locks, says Richard Goldsobel, vice president, Continental Access, a division of Napco Security Technologies Inc., Amityville, N.Y. “Wireless locks typically provide a solution with a very low cost of installation.”

4. OPERATIONAL & MAINTENANCE

With enterprise-level access control systems doing more and more things, the issue of ongoing operations and maintenance is becoming critical. Customers are beginning to look at cloud computing environments and access as a service to help with these challenges.

“A recent trend in security is leveraging the popularity of cloud computing, or the idea of a specialized third-party server hosting and managing IT-based solutions,” Casey says. “Access control is no exception. This is helpful to many companies that aren’t able to provide the significant IT time and expertise required to install and maintain dedicated AC servers.”

While it is true that many enterprise level customers do have their own dedicated security operations centers, the idea of the cloud is one that is working its way up the chain — and

one that is increasingly popular as IT departments have more and more say in the physical security world.

“One trend we are seeing is the increased demand for application virtualization support, which involves moving dedicated server infrastructure to virtualized environments where customers already have heavily invested in IT strategies for virtualization of critical business systems with high availability and disaster recover protection,” Martinez reports. “I believe we will continue to see increased virtualization of enterprise access control server infrastructure with more of a transition to private cloud environments.”

Leveraging the cloud to host access control solutions while deploying devices at the site eliminates the need to deploy and maintain on-premises software, Palatsoukas says. “End users want to reap the benefits of cloud technologies and convert their capital expenditures into lower recurring operations expenditures … [as well as] protect their people, assets and environment without worrying about the maintenance of their security system. The future of security services is bright as it enables end users to benefit from seamless security updates while reducing IT operational costs.”

5. CONVENIENCE

We live in a convenience-driven world, from our cellphones to our smart watches. It is no surprise that these same types of features and functions are finding their way to the enterprise boardrooms, offices and parking garages. Many access control providers are starting to offer mobile credentialing, which is attractive to the enterprise for many reasons.

“The convenience factor of mobile device support … has become more ingrained in our population than carrying an access control credential,” Goldsobel says. “Many people are even buying more expensive shatterproof and waterproof phones, but would not consider spending an additional two dollars for a more durable access control credential.”

The BYOD (bring your own device) trend allows employees to use their smartphones as access credentials, providing increased security at a lower cost, Tucker says. But, he admits, they are not without their challenges.

This forward-thinking trend is not going away, and more and more providers are figuring out

ways to make it work. AMAG recently introduced a mobile credential system, Tucker adds. And many other manufacturers and integrators are doing the same.

“More and more organizations are looking at ways they can incorporate mobile devices into their security posture, utilizing smartphones and tablets as methods for credentialing and granting access,” Kane says. “Manufacturers across the industry are answering this call and exploring new ways of implementing these tools into their access control solutions while balancing the security concerns associated with BYOD policies.”

Mobile devices aren’t just the credential, Martinez says. “Later this year we will be releasing a new mobile application that can convert a tablet or mobile phone into a virtual access control door for mobile checkpoint applications,” he says. “Enterprise class customers can now quickly mobilize access control checkpoints with roaming security personnel and they will be able to enforce access controlled personnel presence at a temporary location such as a corporate event or a manned gate entrance with no physical access control infrastructure in place.”

Cypress Integration Solutions, Lapeer, Mich., recently introduced a similar concept, says Tony Diodato, CTO. “Our new generation of handheld, wireless, mobile card readers allows greater flexibility and interoperability for perimeter, mustering and data collection applications,” he says.

Casey predicts the mobile trend will continue — and perhaps even merge into the biometric world. “Over time, as the technology becomes more accepted, we expect card volume to drop, but not go away completely. Ultimately the adoption will depend on costs, user experience, and willingness from organizations to take this intermediate step of a virtual credential — or whether they decide to go straight to using biometrics as their primary means of identification.”

Indeed, biometrics has experienced a resurgence in the past few years.

“Biometrics are more widely accepted as a legitimate next-generation form of credential,” Casey adds. “When Apple introduced the fingerprint scanner in the iPhone 5S, it brought biometrics awareness to the consumer market. As a result, development for biometrics is in its prime, leading to more reliable technology and decreasing prices.

6. CYBERSECURITY

The more things get integrated, inter-operational and connected, the more a growing threat is affecting the enterprise. Cybersecurity is a huge problem at all levels, but as several large enterprises have learned in recent years (from Target and Home Depot to the Social Security Administration), a breach can have devastating effects on business. At the access control level, manufacturers and integrators have been saying for years that the traditional proximity credential is not secure. Increasingly, users are listening, Lindley says.

“There is a cascading movement of end users wanting to more fully protect the front ends of their enterprise access control solutions and their contactless card systems — both proximity and smart card — with an additional layer of security to prevent hacking and fraudulent use.”

One way to do this is through encryption. “An aspect of securing the card’s information is to make the internal numbers unusable,” Lindley explains. “To read them, the system needs access to a secret key or password that provides decryption. The newest of the MIFARE standards, DESFire EV1, includes a cryptographic module on the card itself to add an additional layer of encryption to the card/reader transaction.”

The “security-of-security” issue is one of the most discussed trends in the industry, Palatsoukas says. “Organizations are seeing more cutting-edge measures to secure their privacy and data. We have already seen tremendous demand for secure and encrypted communications between devices and client applications within the video surveillance market. The same applies for access control. There have been efforts made from card to reader, and now that security push is going to cover communication from reader to controller, and from controller to client application with more encryptions, authentications and authorizations.”

But complete cybersecurity goes beyond just encryption, and some manufacturers have begun stepping up by making sure their new products and systems are cyber-hardened.

“Cybersecurity has and continues to be top of mind for C-level and IT/security leaders, and we are fully engaged with our enterprise class customers on that front,” Martinez says. “It has driven us to launch our Cyber Protection Program that takes a holistic approach to combatting cyber threats.” (For more on this and cybersecurity see this month’s cover story

on page 56.)

“With so many systems on the network, organizations are more mindful than ever about their cyber risk,” Stewart adds. “End customers, installers and manufacturers need to ask the right questions and ensure that the right steps are being taken to protect against cyber threats.”

7. FUTURE-PROOFING

One of the biggest challenges to the enterprise customer and integrator alike is how to upgrade in an affordable and timely way. The concept of future-proofing is one that is often implemented in the enterprise, allowing large organizations to evolve their investments rather than rip and replace.

This is the part that rests almost entirely on the integrator.

“As access control solutions are updated and software and new functionality added, integrators have to be up-to-date on these enhancements to share the value of these features with their customers,” Kane says.

The best thing about future-proofing is that it benefits the integrator equally with the enterprise client, allowing them to become invaluable guides as technology inevitably changes.

“By helping them realize how they can improve processes, mitigate risk and meet compliance, as well as secure their buildings, employees and assets … they will have a customer for the duration,” Tucker says.

Beyond Access Control: Helping Companies Improve Processes a--nd Operationalize Business

Access control systems focus on who goes where and when. But how are companies implementing their security programs? For example, how does an employee gain access to a restricted area? What other factors are involved to obtain such access? How do companies audit this process and ensure they maintain their compliance requirements, such as SOX, PCI, HIPAA and NERC/CIP? Many companies have an endless manual process, which requires paper-based or electronic forms, emails and spreadsheets. The end result is increased risk, by having individuals with unnecessary access.

Using affordable, policy-based security technology to automate processes does three things:

1. It saves money. Organizations normally add people when processes become inefficient. Rather than add people, implement a policy-based security solution, which integrates multiple data sources to simplify and enhance the user experience while reducing errors and streamlining operations.

2. It mitigates risk. Automating manual processes reduces the risk of errors and policy breaches. A policy-based solution enforces each step in the process is complete.

3. It meets compliance. A policy-based solution ensures that only those people with proper approvals and requirements have access to secure areas for the time frame needed.

Small staffs and tight budgets are today's challenge. Technology replaces inefficient processes and protects employees and assets. A policy-based solution saves money, reduces risk and helps companies meet audit and compliance requirements — the three most compelling business drivers needed for companies to make investments into security programs. *—Contributed by Kurt Takahashi, senior vice president of sales, AMAG Technology.*

Securing Non-Traditional Openings

Non-traditional openings such as server cabinets, employee lockers and other supply and storage cabinets represent a significant emerging opportunity for access control and security integrators to add new value to their current systems and services they offer

customers. This new generation of electronic cabinet lock systems provides a path for security professionals to grow their business and provide a powerful new service for their customers.

As wireless technologies and network convergence continue to evolve, there continues to be an overall reduction in the costs associated with securing an opening while improving performance. As a result, the industry has seen a sharp surge in the deployment of non-traditional electronic locks in high-density applications. From corporate campuses, medical facilities and law enforcement, to retail storefronts and data centers, businesses today recognize the value of enhanced security, inventory control, and detailed audit trails that electronic cabinet locking solutions offer.

A large corporate client we are working with is deploying an enterprise-level electronic locker solution using cabinet locks on their corporate campus to track and manage employee assets. In the past each of the campuses may have included several hundred doors of access control. With the addition of the lockers, the client is now looking to deploy as many as 3,000 openings at each site.

Data centers offer yet another area of opportunity. A service provider that we are working with is looking to deploy thousands of server cabinet locks across all of their sites. With both front and rear doors on every server cabinet, there are as many as 10 times more openings that could be secured in comparison to traditional access control systems.

The growing popularity of these high-density cabinet lock installations is attributed to a combination of new codes and regulatory requirements. These new requirements are driving a wide variety of new ways to secure openings for tighter management of information and physical assets. Compared with mechanical solutions, electronic cabinet locks provide better monitoring and control while improving overall functionality as an extension of traditional access control systems. — *Contributed by Benjamin Williams, CSI, senior product manager, ASSA ABLOY EMS & OEM Group.*

Networks Propel Access Control Systems to the Enterprise

We live in a connected world where more and more devices of all types are being added to

networks. As a result, networked systems offer great potential for integration that can deliver heightened situational awareness and greater overall security.

While access control systems have long been a key component of security, the network has transformed them from standalone solutions into a vital part of a more robust, highly integrated enterprise level system that allows users to utilize a single control platform to monitor the state of a location or facility — and more. The interconnectivity of these advanced systems can also improve system accuracy, responsiveness and automation, all of which add up to stronger, more effective access control and overall security, including evaluation and performance of policies and procedures.

The advanced technologies behind today's access control solutions enable users to collect and share data across multiple systems, data which is fed into a central command center and used to automate functions that were once extremely time-consuming and labor-intensive. Compared with managing multiple systems and solutions, automation streamlines processes like badging, monitoring and more. This makes operations and personnel more efficient and offers organizations the potential to realize significant savings on staff costs.

With integration, end users also benefit from the combined strengths of security modalities including video surveillance, access control and other systems, which improve safety and security using the emerging model of predictive analytics. With all the data that is readily available, incidents can be detected more quickly, and information can be correlated and prioritized to allow incident response personnel to take faster and more effective action.

Ultimately, the power of networked access control solutions to serve on a security hub expands the capabilities of access control, delivering greater performance, efficiency, security and value. As these advanced solutions and technologies continue to evolve, they will be capable of offering even greater functionality and flexibility to address a broad range of security and budgetary requirements across a wide-ranging field of applications. The continually expanding functionality and applications are elevating networked access control, delivering tremendous value at the enterprise level. — *Contributed by Robert Laughlin, president, Galaxy Control Systems*