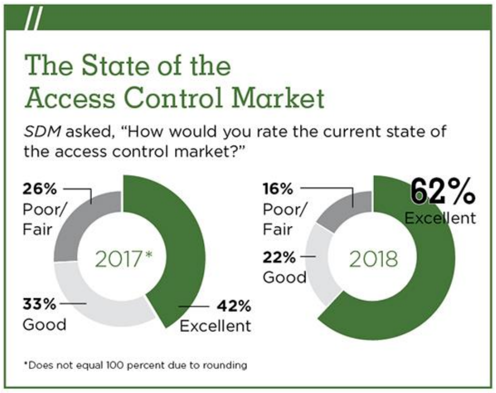
The State of the Access Control Market in 2019

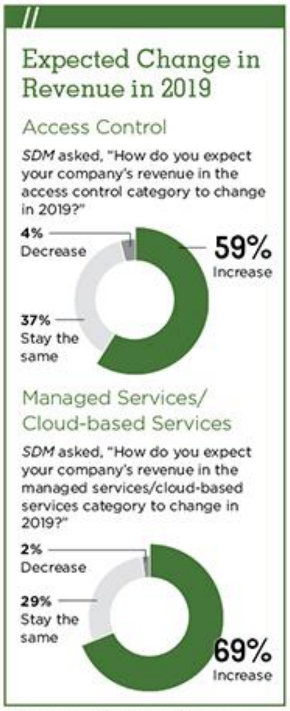
Security integrators and manufacturers see renewed interest from end users in the features, benefits and use cases access control can provide, and are starting to see an uptick in retrofits and upgrades.

Matthew Netardus of Security 101-Hampton Roads says his company saw a definite uptick in access control retrofits in 2018, one of which was the Wells Fargo building in Norfolk, Va., pictured above.

As end users upgrade or integrate their access control systems they are overwhelmingly seeking open architecture-based platforms.



A large majority of respondents described the current state of the access control market (in late 2018 when the survey was fielded) as "good" to "excellent," with more than six in 10 describing it as excellent. // SOURCE: *SDM* 2018 AND 2019 INDUSTRY FORECAST STUDIES



Expected Change in Revenue in 2019

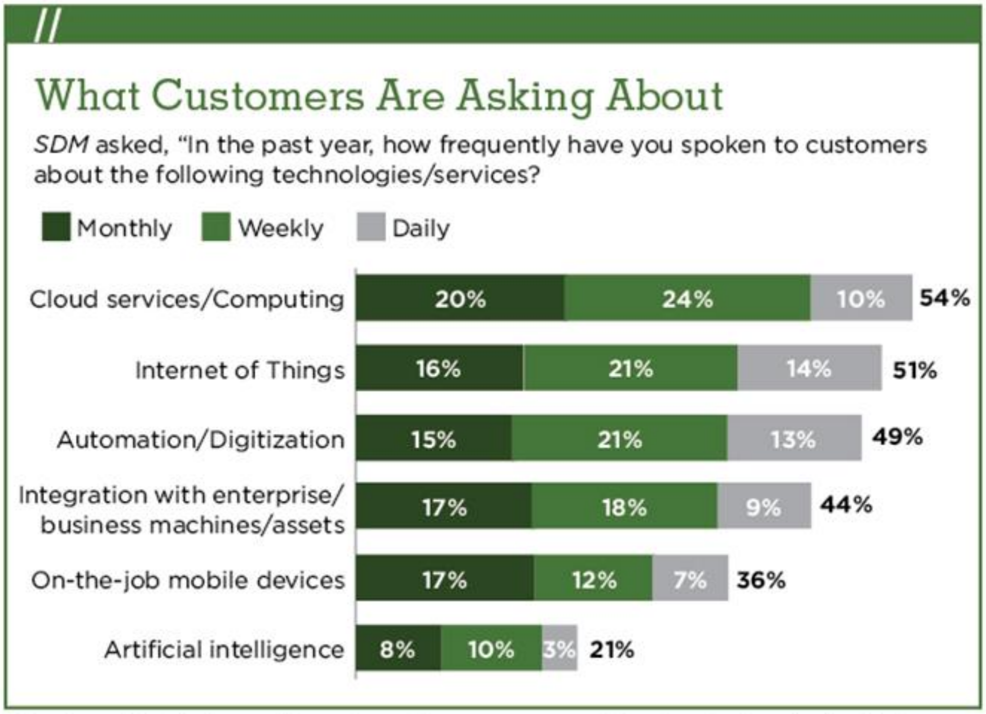
Access Control

SDM asked, "How do you expect your company's revenue in the access control category to change in 2019?"

Managed Services/ Cloud-based Services

SDM asked, "How do you expect your company's revenue in the managed services/cloud-based services category to change in 2019?"

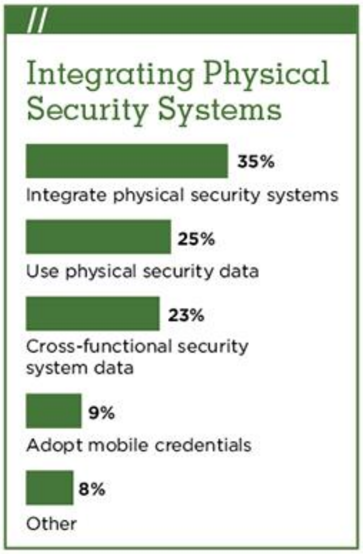
Nearly 60 percent of respondents anticipate revenue from access control systems will increase in 2019; and for managed services/cloud-based (including integration of connected machines and assets in the wider enterprise) that number is nearly 70 percent. // SOURCE: *SDM* 2019 INDUSTRY FORECAST STUDY



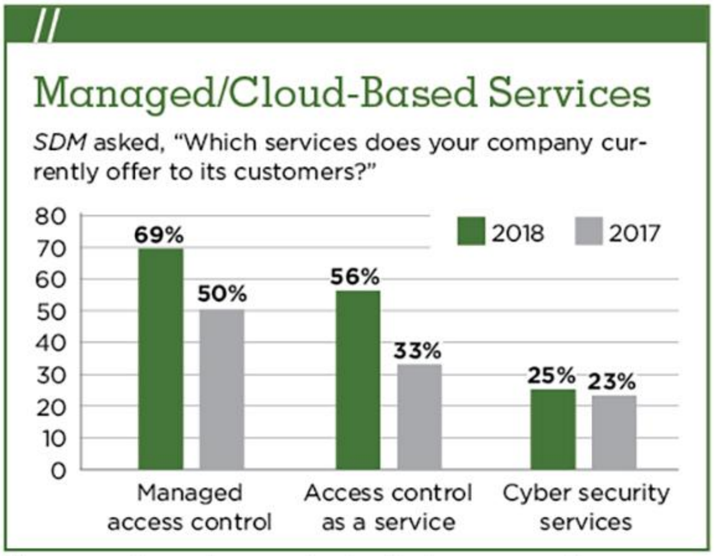
What Customers Are Asking About

SDM asked, "In the past year, how frequently have you spoken to customers about the following technologies/services?

Cloud and IoT, followed by automation, are some of the top technologies being discussed at least monthly with half or more of customers. // SOURCE: *SDM* 2019 INDUSTRY FORECAST STUDY



Integrating physical security systems — access control, video and alarm — and expanding cross-functional areas were the top physical security initiatives in a recent survey of 700 security professionals about advanced technology adoption to improve physical security practices. // SOURCE: BENCHMARKS, TRENDS AND BEST PRACTICES SURVEY CONDUCTED ON BEHALF OF BRIVO, DECEMBER 2018



The percentage of respondents offering managed access control rose 19 percentage points over last year, while access control as a service increased by 23 points. // SOURCE: *SDM* 2018 AND 2019 INDUSTRY FORECAST STUDIES

For decades the dominant story in access control has been that it was a victim of its own success: that is, customers were reluctant to change out what was still working — even 15 or 20 years on — and didn't see the benefit in spending the money to upgrade, even for significantly new or different features. While still early days, according to many integrators and manufacturers, this attitude is definitely starting to shift. In fact, for the first time in a long while, more integrators are talking about the growth of upgrades and retrofits for access control. What is driving this trend?

It is likely a combination of factors — from changing buyers and interests to cyber security concerns, a desire for more business intelligence based on the data access control can provide and recent security technology developments that not only improve the user experience, but the return on investment (ROI).

"We definitely saw a significant change in upgrades," says Keith Kranz, sales manager, LVC Companies Inc., Minneapolis (SDM's 2018 Systems Integrator of the Year). "We had a few the year before but nothing like this year. They are not going from legacy to latest but from older tech to browser-based. They are trying to get rid of the client/server model."

Dennis Thiele, ISG development and technical support for LVC, points to a couple of driving factors in the past year, including the sunset of Windows 7 and the final end-of-life deadline for the old Casi Rusco systems in 2020. "People who [dragged] their feet will have to make a decision in the next six months, so we anticipate a lot of customers we reached out to and they did nothing will be making the decision to upgrade."

Steve Wagner, president, Open Options, Addison, Texas, agrees, adding, "System age, particularly in access control, has played a part in recent growth, as has certain business consolidations that led to end-of-life announcements, forcing end users' hands in making system changes. Many systems installed during the Y2K push have come to their rightful end."

But the trend goes beyond those companies that have to upgrade.

"Obviously the economy was really strong in 2018 and it felt like there was more corporate spend for things like [upgrading]. They could finally take advantage of this," says Jack Johnson, managing partner and vice president of sales and marketing, Star Asset Security, Orlando, Fla.

Access Control Goes Mobile

Over the past decade, mobile access technology has been well proven and increasingly adopted in the retail, hospitality and real estate industries. With mobile phones continuing to revolutionize how people communicate, bank, shop and perform many other daily tasks, mobile access technology is becoming a quickly growing sector due to its increased convenience, security and cost savings.

Moving to a more digital approach adds speed and flexibility beyond traditional systems.

To bring real value, new access control technology must at least maintain or improve upon existing security. Smartphone credentials are more secure than plastic cards as they require possession of the device, a security code to activate it, a link to the mobile app and the downloaded credential. Security can be further enhanced by end users requiring the use of biometric identification standard in modern handsets as a second factor of authentication upon launch of the app. The phone's built-in GPS technology enables security to quickly locate the device (and its owner). For high security areas, facility managers can add biometric readers using iris scans, facial recognition or fingerprints. Personal identification numbers (PINs) can also be entered through the phone's keypad.

Unlike plastic cards, smartphone credentials can be reused, transferred and remotely deactivated. Mobile credentials can help organizations eliminate the direct costs of plastic badges and printers. Imagine costs for a large university where administrators must regularly encode, print and sometimes ship tens of thousands of badges to incoming students. These expenses are largely alleviated by using smartphone credentials.

Realistically, smartphone credentials won't entirely replace plastic badges within the next few years. But, dealers and integrators can prepare customers to make the switch now with a hybrid solution. Readers capable of supporting a wide range of traditional cards as well as mobile credentials exist today to facilitate this solution. These readers allow for a phased approach to newer card technologies and eventually mobile credentials when the time is right.

Mobile access control technology is poised to build upon the success already seen in several segments to become more widely adapted and to leverage the vast adoption of smartphones, apps and digital technology to improve convenience, security and cost. — *Contributed by Greg Berry, vice president, mobile credentials for LenelS2, part of Carrier*

"It was a great year for us," Johnson adds. "We did a lot of business in access control in 2018, more than in 2017."

Justin Wilmas, senior director of global sales, AMAG Technology, Torrance, Calif., echoed both reasons. "The economy is much stronger this year than last year and years past. With that you see more construction, more funding available, and overall from a general outlook the U.S. access control market grew significantly because of that.

"We have seen really good growth in the access control market, and that has been around the retrofit market . . . We saw double digit growth in our retrofit market."

Integrator Matthew Netardus, systems design and engineering, Security 101, Hampton Roads, Va., says the majority of his company's growth last year came from access control. This was a conscious switch for the company, he says. "We were founded in 2013 and originally focused heavily on video surveillance . . . From 2017 on we have been intentionally migrating to access control as our primary offering."

Netardus says as video has become more commoditized, access control has been the technology of choice for the integrator to differentiate itself from the competition. He has also seen a big uptick in retrofits. "That has definitely been our niche in the market. We have completed a half dozen major retrofits in 2018 and in 2019 we have a few major ones on the level of several hundred doors. We are doing complete switch outs to new systems."

While the official numbers didn't move the needle much — IHS Markit shows the access control market growing at a steady pace of about 5 percent to 6 percent, the same as in recent years — anecdotally there was a definite shift in 2018.

"We did very well in the access control space," says Despina Stamatelos, product marketing manager for Synergis, Genetec, Montreal. "We grew 30 percent year over year."

SDM’s own 2019 Industry Forecast showed a 9 percentage point increase in perception of the strength of the access control market from 2017 to 2018, with 84 percent of respondents reporting the state of the access control market to be good to excellent. However, of those reporting a very good/excellent perception, the number jumped a whopping 20 percentage points from 42 percent in last year’s poll to 62 percent this year.

What’s more, almost 60 percent expect their revenue in access control to increase in 2019. This compares with only 35 percent who were similarly optimistic the previous year.

Beyond retrofits, nearly everyone pointed to three primary technology trends driving forward access control: the cloud/managed or hosted systems; mobile credentials; and wireless locks.

“2018 was strong and 2019 looks like it might be our best year ever,” says Hank Monaco, vice president, marketing, Johnson Controls Building Solutions North America, Milwaukee. “We are continuing to see good upwards momentum in that category. Some of it has to do with some of the abilities we now have to provide management in the cloud. Our customers certainly like that.”

Stephen Carney, vice president of product marketing - physical access control solutions at HID Global, Austin, Texas, adds, “The growing demand for connected mobile experiences and the benefits of cloud architectures continued to drive the access control market during 2018. By 2020 it’s estimated that 20 percent of physical access control solutions will be shaped by mobile technology and cloud architectures.”

Richard Goldsobel, vice president, Continental Access, a division of Napco Security Technologies, Amityville, N.Y., points to all of these technologies as the reason for their success in the past year. “Business is good. There are definitely some particular growth sectors we have hit in 2019. The two biggest by far are locking/hybrid systems — [the combination of] traditional hardwired access units and wireless locking systems is huge, the largest growth area in access control — [and] hosted and managed services, which is growing dramatically.”

With technology advancements customers want, the financial impetus to implement them and other strong incentives, the access control market looked strong in 2018 and is on track to stay solid, if not improve, in 2019.

Changing Buyer Habits

One thing industry experts point to when it comes to the shifting access control buyer is the rise in importance of the IT department. An evolving trend, the IT manager has gone from “in the room” to “at the table” to — more frequently — “decision maker.”

“More IT departments have become entrenched in access control to the point where it is more readily accepted and quite a bit better managed by the IT side than in the past,” Goldsobel says.

One of the reasons IT has a greater say than ever is the meteoric rise of the cyber threat in recent years. Not only do they want to know what is going on in their network, but how it is secured, and — importantly — how it will stay secure.

M&A Activity in Access Control: Who's Buying Whom?

From 2000 to 2018, there was a general upward trend in consolidation in the physical security industry, which has grown by a CAGR of 7.5 percent in that time period. Access control alone has seen 742 deals in the last decade, according to Memoori. HID Global has completed multiple acquisitions over the last 10 years; and in the last couple of years, Vanderbilt and its holding company, ACRE, have added to their portfolios through strategic growth. More recently, at the end of 2018, ACRE added Open Options to its roster of brands and in April 2019, bought RS2 Technologies in an effort to strengthen its access control holdings across North America.

"Large companies are looking for ways to build their portfolios through the addition of innovative technology, as well as by acquiring companies that add value to the overall brand," says ACRE CEO Joe Grillo. "The access control sector of the security industry is highly fragmented, making it one area where M&A activity is poised to make a dent in the overall landscape and drive consolidation forward."

Despite its positive impact, security integrators have expressed concern about the trend, with worries that the smaller companies being bought will be dissolved into large-scale company offerings. Grillo, however, says ACRE's goal is to allow its companies to remain independent and profitable. "With its R&D resources and sales channels, RS2 Technologies is very strong in customer service and tech support among their resellers and we will let them continue to operate independently as we do with many other parts of our portfolio," Grillo says, adding that RS2 has been growing faster than the surrounding market, which was a big draw for the company.

As for future M&A activity, all signs point to a continuation of the trend. "However, I know that as we see the economy start to cool off a bit, many companies will become more cautious about the opportunities they pursue, waiting for the ideal price, timeframe and business fit that will truly augment their overall portfolio," Grillo adds.

"As more users are buying with cyber security in mind, solutions developed with cyber security at their core are becoming increasingly attractive," says Andreas Pettersson, CEO, Arcules, Irvine, Calif. "Cloud-based systems are at a significant advantage in this regard because vulnerabilities can be addressed almost instantaneously by remotely pushing automatic updates to the system."

Johnson says cyber concerns definitely drove some of their larger enterprise customers to upgrade older legacy panels last year. What's more, many of the IT departments are looking to manage the access control system with the same expectations as some of their other technologies and upgrade much more regularly.

"The decision makers are beginning to change," Johnson says. "We are seeing a trend towards IT having control of all of these because we are putting in IoT devices that hang on their network.

Because of cyber concerns they can't afford to manage legacy technology . . . In their world ever-greening is a big deal; every three to five years they switch things out to keep up with all the changes."

This may have the effect of significantly shortening the upgrade schedule for access control systems in the future, he adds. "IT people are saying, 'We need to budget to go with more current access control all the way from the file structure and database to the hardware.' We are moving from facilities decision makers that want to put something in and make it work for 10 to 20 years to seeing those amortization schedules shortened because of cyber security and rapid changes in technology."

Derek Arcuri, team lead of industry and application market for Montreal-based Genetec, agrees. "We have seen the shelf life of access control come down significantly. The average organization has 42 systems attached to their IT network. The systems integrator has to go through and validate that their devices, along with the software, are geared toward that type of requirement. Devices that are not protected according to IT standards are likely to be swapped out."

Despite these reports from the ground, at a high level, research firm IHS isn't seeing a large uptick in upgrades for access control, says Bryan Montany, research analyst and lead analyst for access control intelligence service, IHS Markit Technology, Englewood, Colo. He explains the seeming discrepancy this way: "Yes, there is a small uptick in retrofit projects. Consolidation of IT and security, concerns about cyber, trends toward IP in general are leading some end users to do a little bit more retrofit projects. But it is still relatively small in terms of overall impact . . . Retrofits are growing and that is exciting from an integrator's perspective. Even a minor uptick from 5 percent to 6 percent makes a huge difference [to them]."

Another thing end customers are becoming increasingly aware of is the experience access control can help facilitate at their businesses. There is a growing focus on creating new user experiences, Carney says. "Enterprise customers increasingly want to create trusted environments within which they can deliver valuable new user experiences. Users want the 'digital cohesion' of being able to use smartphone apps to open doors, authenticate to enterprise data resources or access a building's applications and services. Demand will continue to grow for smarter and more data-driven workplaces, as well as a risk-based approach to threat protection, improved productivity and seamless, more convenient access to the enterprise and its physical and digital assets and services."

A few years ago the talk was all about convergence. That is here and now.

"It's safe to say that all trends revolving around the network, such as the IoT and cyber, are greatly impacting the security industry and continue to shape the way that organizations leverage technology solutions for both security and business operations," says Eric Widlitz, vice president, North American Sales, Vanderbilt, Parsippany, N.J. "This convergence has played a significant role in the growth of the security industry and has also created the ability to extend these solutions beyond the safety element to include the improvement of business efficiencies, such as building or event management."

When it comes to business intelligence, access control is a natural fit.

"Access control is rich in data; it is just a question of how they can tap into that data to make more informed decisions, and more end users are recognizing that this [access control] system is already collecting the data they need," Arcuri says. "Our end users are maturing to the point where they are no longer looking for access systems to lock and unlock doors. They are looking for ways for security to be more credible in the enterprise so the CEO can see the value to the organization . . . They are requesting more automation and workflows to help improve operations, and access control is often the answer."

Howard Himmelman, marketing and business development, Access Hardware Supply, San Leandro, Calif., says the access control system may even start to eclipse video in terms of importance to the end user. "I believe the access control space will grow immensely. I think it will become the pivot point for all security, even overtaking video. The reason, in my opinion, is video is often just forensic, an after-the-fact analysis of an event. Access control is actually providing control in the present . . . It is a natural fit to become one of the core elements or disciplines of any operating business."

When it comes to building intelligence and integration with access control, Montany points to a solid trend, based on research he conducted on building management system platforms where he asked security integrators, installers, vendors and end users which security systems are the highest priority to integrate into a broader smart building. "The overwhelming answer I heard was that access control was the biggest demand. In 2018 access control was the most common security domain to be integrated through BMS and a little less than 30 percent of all access control equipment installed was integrated in some capacity. That percentage is growing pretty tremendously. By 2023 IHS anticipates the number will be closer to 45 percent."

Montany points to two reasons for this. "First it is a comparatively low-cost alternative . . . If you don't have the money to spend on hundreds of occupancy sensors, the easiest way to get a feel for that is looking at access control data . . . More importantly, entry through access control systems can act as a trigger. One common example is how an employee badge scan can trigger all kinds of automated responses such as lighting and HVAC systems responding in a nuanced way or the summoning of an elevator to the correct floor."

Finally, whether it is integration with a building system, an upgrade or a new enterprise system, one requirement is now non-negotiable: no more proprietary systems.

As end users look to upgrade or integrate their access control system into a larger BMS platform, what they are seeking is overwhelmingly open architecture, Netardus says. "A lot of ours are changing to open architecture platforms. Not only does that give them the ability to change locks and controllers but it also gives them the flexibility to change integrators if they feel they need to."

Bruce Stewart, business development manager for access control, Axis Communications Inc., Chelmsford, Mass., saw this trend in action recently. "Everything is going to IT solutions and it makes sense that they are managing it. We had several end customers talk to us at ISC West regarding updating their systems or saying their company is mandating they update to a more open platform."

Technologies & Solutions

As end users increasingly look to migrate to open platforms, cloud and systems that provide them with more business intelligence, access control manufacturers have also stepped up with technology that allows them to do that in a way that is not only exciting, but economical.

One of the technologies seeing widespread adoption in recent years is wireless locks.

"We are seeing more and more wireless applications," Himmelman says. "Locks on doors used to be simple. Today they are intelligent and will do nothing but grow. I consider this year to be a new launch point for the industry."

Netardus is particularly excited about wireless locks this year. "We will do close to 750 wireless installations this year," he says. "That comprises probably 50 percent of our access control business, especially in the education market, but also spreading into commercial, not only because it lowers the cost per door, but also the disruption. If I can have a wireless system, put an aesthetic lock on the door and not have to have techs pull wire, that is a win."

Goldsobel points to the cost of acquisition and installation coming down as one reason wireless locks are gaining in popularity. "That helps drive the ability to install security at doors that weren't targeted a decade ago as being feasible to get security at the door. That is driving a lot of that growth and why we are seeing so much with our wireless locking . . . because the ability to get security at these doors is going up."

Wireless locks are an "enabler for access control growth," adds Rajeev Dubey, director of product management, distribution, access control building technologies and solutions, Johnson Controls, Milwaukee. "Although wireless locks are considered the solution of choice right now, the underlying need is a solution that lowers the installed cost of a door compared to a traditional access control system. Such solutions will be a game changer for the market as a whole, purely because they cut installation time and costs and in turn are more affordable."

Peter Boriskin, chief technology officer, ASSA ABLOY Americas, New Haven, Conn., also sees wireless technology having the greatest influence on access control in the immediate future. "We continue to see growth and demand for wireless, even in sectors that have historically been slower to adopt it, like government. One reason for the rising demand is the growing need for access control for more doors and more applications. Wireless access control makes this possible and provides new operational opportunities. For example, it allows for greater connectivity among devices within an access control ecosystem, which results in better data about the functionality and efficiency of a facility."

Another recent development helping grow the access control space is the replacement of Wiegand with OSDP.

“One of the key drivers will be the adoption of OSDP, says Jim Lantrip, vice president, enterprise solutions, ADT Commercial, Irvine, Texas. “OSDP is an access control communications standard developed by the Security Industry Association to improve interoperability and add encryption between access control head-ends and security devices like readers.”

Manufacturers have begun to push OSDP more in recent years, as well. “I think OSDP [has had] more of an impact recently,” Arcuri says. “Mercury and HID are really driving that. Years ago they were looking at a cooperation where HID would enable OSDP from the reader up and Mercury from the controller down. But with the new Mercury Red Boards and modules that support OSDP on all devices, that is helping improve awareness of potential vulnerabilities.”

OSDP not only provides more cyber security, but also offers other benefits end users want, Carney says. “The Open Supervised Device Protocol standard dramatically enhances overall security while delivering other advantages, including increased flexibility and operational efficiency for the long term, and the ability to support both current and future technology requirements . . . OSDP offers the benefits of bidirectional communication for configuration, status monitoring, tampering and malfunction detection, and other valuable functions. It enables customers to flexibly enhance system functionality as needs change and new threats emerge, and it reduces installation costs as compared with earlier protocols.”

OSDP is playing an important role in product selection today, says Steve Van Till, president and CEO, Brivo, Bethesda, Md. “We are finding that more and more end users and integrators are specifying it. All of Brivo’s control panel products support OSDP.”

Another significant trend is unified access control and video systems, which have been emerging for a few years as a growing preference for end users. The change recently, Montany says, is the cost has come down, driving more end users to consider this option.

“The cost of unified access and video systems dropped by 30 percent to 50 percent from 2015 to 2017. As those prices drop, end users will gobble those solutions up,” he says. But this is only the beginning. The next step in smart buildings and integration is AI.

“This will lead to more and more deep learning analytics in these security solutions,” Montany adds. “We will increasingly see software from more of a broader security perspective, so no longer will it be just access control software, but increasingly security software solutions that are managing everything security-related in a building . . . That is really where the growth is going to be occurring in the next five years . . . and if you are an integrator you need to be aware of that.”

Are Your Customers’ Access Cards at Risk?

Today, duplicating some access control cards is as easy as purchasing a card cloner and being near a card to copy. It’s so easy that you can do it in less than 5 seconds without the cardholder’s knowledge or permission. Despite this security risk, these unsecure credentials are still in wide circulation.

So, it’s no surprise that more than half of the 3 million access credentials sold every year are vulnerable technologies such as these, presenting a huge security risk for facilities using these technologies.

The most secure access cards currently on the market are next-generation 13.56 MHz smartcards with AES encryption. Fortunately, they’re around the same price as older, less secure legacy cards, so they should be an easy sell. We strongly recommend every new system an integrator installs should include secure smartcard credentials and readers. If you have customers who currently use legacy cards and readers, we encourage you to educate them on the risks and make a plan to upgrade their access control systems.

By next year, about 20 percent of all access control credentials will be mobile technology, so end users would be wise to incorporate mobile credentials and readers as a future-forward investment. Mobile credentials can be issued or revoked from anywhere, they cannot be cloned, and they benefit from the extra protection of the mobile device’s PIN/biometric security. In most cases, they eliminate the need for physical cards or fobs.

Biometric credentials use a person’s unique physiological traits as their access control credential. They are highly secure, can never be misplaced and are cost-free. They are the only technology that provides positive authentication of the user before granting access. When combined with a credential or PIN code they create double or even triple authentication. *— Contributed by David Busco, director of marketing – Global Solutions Marketing, Anixter*

People want to work with one technology partner, says Peter Lau, president, security, Honeywell Commercial Security, Atlanta. “What we are seeing more and more from end customers is they want to standardize on a platform where they know the hardware will integrate and work seamlessly with those platforms.”

Lau adds that AI could really speed up the pace of change in the future. “When you think of things like analytics or AI or machine learning and how that changes the security landscape, this technology allows end users to get more insights from their security platforms. Companies are going to be looking for technology partners able to integrate those technologies or be able to have those on their platforms. Instead of waiting, customers are looking for a little more innovation in the space.”

Monaco agrees, adding that the access control space is only getting more exciting as a result of these and other developments. “We talk a lot about video advancements, but I would say as a category some of the advancements being made in access control are equally exciting and prompting folks to take a fresh look. Things like machine learning and building management can be a motivator, as well. We think about not only safety and security but also sustainability and the ability to manage costs. Access control plays a role in all that and we do see our customers spending more time being considerate about how they would like to apply this technology in their environment.”

Last but not least, cloud and mobile are two of the hottest technology advancements to come to the access control space in recent years, and many experts see them as the next primary drivers going forward.

“Increasing cloud adoption is the number one external driver of our business growth today,” Van Till says. “We are also seeing mobile credential sales tripling or quadrupling year-over-year.”

Montany calls mobile credentials “the most significant change in North America” in the past year or two. “In earlier years like 2015 we ran into a constant problem where when we wrote mobile credential reports vendors and integrators were generally optimistic about sales and expectations to see 150 percent to 200 percent growth; but when we actually got the data back it wasn’t matching the stories and conclusions we came to. There was a lot of hype but actual adoption rates were not quite as fast. Now all of a sudden in 2017 and 2018, that story is finally catching up to where integrators and vendors wanted it to be.

“Globally in 2018 mobile credential sales or unit shipments were under 10 million,” Montany says. “Compare that with 500 million new physical credentials and there is still a massive gap. But we are seeing 150 percent to 200 percent annual growth for mobile credentials, so we might have over 60 million in 2022. That is what the trajectory looks like. It is still a small portion of the market, but it is growing rapidly. “

According to Scott Lindley, general manager, Farpointe Data, San Jose, Calif., “Mobile access control will have the biggest impact on our part of the market. Gartner suggests that by next year (based on a 2017 survey) 20 percent of organizations will use mobile credentials for physical access in place of traditional ID cards. Let’s rephrase that last sentence. In less than six months, one-fifth of all organizations will use the smartphone as the focal point of their electronic access control systems. Not proximity. Not smart cards. Phones!”

Steve Spatig, general manager, electronic access solutions, Southco Inc., Concordville, Pa., sees an interconnection between wireless, mobile and cloud for end users. “[They] are all part of the IoT framework and will have the biggest impact on all elements of security systems from user credentials to software infrastructure . . . to off-premise software. These solutions . . . provide less of a barrier to entrance for providers seeking to implement access control. With solutions that can communicate wirelessly and accommodate mobile credentials, entry-level end users will be able to more easily adopt access control solutions. The cloud-based element means they won’t need to buy and install software, and equipment manufacturers will find it much easier to add access control into their products.”

Cloud and mobile-based solutions are driving both innovation and industry growth, agrees Jeff Stanek, president, LenelS2, Pittsford, N.Y. “This is an exciting time for access control, with many advancements on the horizon. The areas of mobility, unification and cloud utilization are some of the key themes driving innovation . . . Mobile technologies will revolutionize the security industry in coming years as end users look to adapt to an increasingly mobile workforce. It won’t happen overnight, but we’ll see an elimination of requirements to install software or have the workforce carry plastic cards, benefitting both administrators and users.” (For more on the mobile trend, see “Access Goes Mobile” on page 40.)

With all of the newer advancements and technologies happening in the general access control space, Netardus says this is causing the access control industry to become less commoditized, particularly compared with video. “There are more parts and pieces to it and the combination of those and how you install and service them means it is still possible to make a significant difference between integrator A and B, where on video it is easy to copy someone else.”

Service-Centric Culture Shift

With an increasing emphasis on cloud services, the security integrator has more opportunities than ever to continue that differentiation with services related to access control, video or even cyber security — as evidenced by PSA Security’s surprisingly popular rollout this year of its Managed Security Services Provider (MSSP) program, in which the organization partnered with industry-leading solutions providers to bring cloud-based cyber security services, video management, remote video monitoring and access control solutions to integrators as part of a program that will support implementation of the new business model into their existing operations.

At its annual conference, PSA TEC, held in March 2019, PSA president and CEO Bill Bozeman was pleasantly surprised by the level of interest security integrators were showing. “When we were projecting the MSSP rollout I assumed there wouldn’t be as much interest as there has been,” he told attendees. “Why you filled up that room is a mystery to me, but I am very pleased.”

It is no mystery to Stanek. “As our industry and technologies evolve, we expect integrators will earn more revenue from services and less from the resale of physical goods as the industry moves to the cloud. Forward thinking integrators are already making changes to ensure their business process and employees are up to the challenge.”

Star Asset Security is one such integrator. “We are taking more of an IT-centric approach to business,” Johnson says, adding that whether it is fully managed access control, cyber-related services or more extensive service plans and agreements, the service aspect of security is expected to grow exponentially.

“We are in this pivot. We try to sell some form of service-level agreement on everything we do for access control. If we look at it as managed service and hosting fees we are still lean on that. But it is growing, and we plan to do a lot more on that. We are being asked to manage access control. It is only running between 10 percent and 5 percent at most on hosting and service agreements right now, but our goal is to move to a minimum of 30 percent.”

Cloud provider Arcules notes a definite uptick in interest in these types of services. “The difference between when we started our business in 2017 versus 2019 is night and day with regards to the receptiveness to the investment in cloud-based service,” Pettersson says. “There is still a significant amount of work to do in terms of educating the market, but we have found there are many out there who simply ‘get it’ and are more forward thinking when it comes to the benefits the cloud presents.”

3xLOGIC attributes this trend to its steady growth that “substantially exceeded expectations,” says Matt Kushner, president and CEO of the Fishers, Ind. company. “We see no reason that our growth will slow this year; we expect another banner year. The dealer market is getting more comfortable selling cloud-based solutions and end users continue to increase their demand for cloud.”

Montany makes a distinction in access control services and access control as a service, but both are growing.

“The market for services related to installation and maintenance of access control systems . . . the growth rate is less than double, more like 9 percent. But that has been slightly accelerating. So while the equipment level is stable, we have seen growth rates in services go from 7 percent a couple years ago to 9 percent. If you jump ahead to 2021/2022, I imagine you will see double digit growth.”

When it comes to access control as a service, however, the growth rate is even more exciting. “That market is less than 10 percent of the total market size of access control equipment,” Montany says. “But the CAGR for that market for the next five years is over 18 percent. It is a tremendously growing opportunity for those vendors and integrators playing in this space.”

In fact, Netardus says he considers managed access control the biggest opportunity for his company in the coming year. “To get in and be able to offer the expertise behind a high-level access control system and make it be everything it can be is important.”