THE ACCESS CONTROL EVOLUTION

John Davies, Managing Director, TDSi illustrates why access control needs to evolve to meet an array of challenges ahead

If there is one common thing we have all learnt from the last two years, it's that you can never accurately predict the future.

It has been a reminder that we need to be flexible and open to change and that the old cliché, 'expect the unexpected', is just as relevant as ever. Whilst these ideals are cornerstones of common sense and good security, it doesn't mean that the security industry and our solutions are exempt from moving forward and evolving just like the rest of the world.

Unquestionably, secure access control systems need to evolve to meet the challenges ahead – we need easy-to-use, powerful, fully cybersecure and easily integrated solutions that synchronise with the wider business systems mix, whilst ensuring they aren't compromised in their core duties.

Great expectations

It is fair to say that greater integration of security and business systems has been a pivotal approach for some time now, but clearly this has accelerated even faster during the challenges of the last two years. It's not enough now to have a dedicated secure access control system that can link to other security and business technologies; buyers also want flexible systems which are simple to install and use as part of their overall IT mix.

It is surprising to see that, even in 2022, some secure access control systems still rely upon a dedicated proprietary desktop-based application that is running on a specific server. These systems may integrate with others but they are tied to one client server and need hardware that is configured for the job. In an age where most IT hardware is just an endpoint to specific services, this is an antiquated approach.

Speaking from a security provider's point of view, this isn't helpful either. Solutions are often a one-off sale that leaves less room for upgrades and requires a continuous sales churn to be profitable. The upgrade process is also more complicated and limited. The end user must choose to upgrade the solution and changes must be made to the installed software to gain new or improved features. All too often, upgrades are either forgotten or the end user is unwilling to pay for it.

seeing a shift in demand towards a more flexible approach to delivering physical security. This makes a Software as a Service (SaaS) model for security and access control systems the obvious choice.

By using a browser to access the service, you do away with the need to host it on a powerful server or PC as all the storage and processing is accessed via a powerful but streamlined online portal. It's extremely easy to add the additional client connections and the integration with other systems is all managed from a centralised hub which can be securely hosted on premise or in the cloud, depending on preference.

The speed of installation and use saves time and money whilst locating the solution remotely with full encryption ensures it is harder to hack or compromise. At the same time, it makes integration with other business systems easier but also more secure. It also makes the addition of software upgrades/updates simpler to perform and less invasive on the operations of the security operator and end users.

Securing legacy systems

Another important aspect for many security operators is the ability to ensure software support for all relevant hardware – after all, physical security isn't much use without it. Backwards as well as current/future compatibility provides greater flexibility to end users, allowing them to mix and match existing and new components to find the right combination for the security needs and budgets available.

Developing software without this flexibility is little better than employing proprietary solutions. Equally, by adding up-to-date security protocols in the software you are immediately extending and improving the cybersecurity and physical security of the existing working system, adding even further value but with minimal disruption.

Bringing secure access control up to date

Clearly SaaS is starting to dominate many other areas of technology for both businesses and individuals – just think about all the cloud-based business, banking and entertainment solutions you may use day-to-day. It makes complete sense for access control to offer this powerful flexibility.

> "Moving security to an affordable ongoing cost and doing away with the big capital expenditure investment patterns of the past is inevitable."

Moving security to an affordable ongoing cost and doing away with big capital expenditure investment patterns of the past is inevitable.

Pre-pandemic, the security sector was already experiencing considerable changes in terms of not just technology, but also the way our customers want to procure and run their solutions. Over the last two years this has accelerated

even more rapidly – but there is still a surprisingly substantial number of inflexible solutions on the market.

The GARDiS approach

Customers and integrators have demanded easier integration and interoperability between different security and IT systems for some time, something we pre-empted with our flagship GARDiS range of software and hardware. We envisaged and developed the GARDiS platform well before the word COVID-19 had even entered the public consciousness, having taken a broad and professionally researched view on how access control needed to evolve to meet the demands of this decade and beyond.

The architecture that TDSi decided to pursue ensures that the GARDiS platform is intuitive. Part of this involved analysing how consumers expect their digital services to be delivered now – optimum performance but with minimal fuss for the user. Therefore, the GARDiS software is run through an ordinary online browser, either through a desktop/laptop computer, or increasingly, through a mobile device such as a phone or tablet. There is no need to invest in powerful, dedicated endpoint computer hardware anymore and installation is simple and fast.

> "It is fair to say that greater integration of security and business systems has been a pivotal approach for some time now."

↑ **John Davies,** Managing Director, TDSi

With a single installation (either using an on-premise server or through cloud hosting), GARDiS is quick to commission and use, benefiting security installers as well as end users. By using the popular and highly secure OAuth 2.0 authorisation we have ensured GARDiS is robust against potential threats whilst enabling safe but simple integration with other IT and security systems by using powerful REST API service architecture.

Taking software integration to the next level

By employing the widely used REST API architecture to underpin our GARDiS software, we have laid the foundations for a system which can evolve and meet future needs.

Because we can easily license the API to other developers, GARDiS can be successfully integrated by a greater number of developers of other complementary systems. Not only does this increase the opportunities for systems collaboration, it allows us to plan a more agile programme of software updates and to react quickly to specific integration demands.

We have been able to accelerate the numbers and types of integration and additional feature updates we can deliver to our customers each year and there is less disruption from these as development and testing is continuous and evolutionary, rather than revolutionary.

Another less obvious yet important benefit of this approach to GARDiS is that we can help extend the longevity of the hardware systems which interact with and rely upon the software. Though we have evolved the GARDiS system, we have put extra care into ensuring our customers can migrate their existing TDSi hardware and third party solutions.

As well as developing our own GARDiS hardware, we are always keen to assist our customers in finding ways of evolving their systems, for example, by using RS485 wireless locks, RS485 readers, OSDP readers or SSCP readers to extend and improve current working systems. We want to work in harmony with our customers' IT systems infrastructure and develop our systems with a more cybersecure conscience.

Ensuring secure access control is fit for purpose

As we all adjust to what has been referred to as 'the new normal', the security industry needs to be at the vanguard of technology use and development. As a traditionally risk management focussed sector, the security industry is well placed to ensure the safety of people and property – however, we have to be progressive.

Touchless access control technologies, along with intelligent occupancy management using automated people counting, are powerful options in preventing disease transmission and keeping people safe. The pandemic has brought our industry's role firmly into the eyeline of the mainstream audience, which offers greater opportunities but also means we have more expectations to meet.

With this increased scrutiny on security and how it can help organisations and businesses prepare for the future, it has never been more important for our solutions to lead the way. With the rise of flexible working and evolving work practices, security solutions need to be just as flexible. Even before the world changed there was pervasive demand for fully integrated, flexible and automated secure access control solutions. But, this has now evolved from the ideal solution to an essential one for those looking to survive and thrive post-pandemic.

It will be interesting to see how the world continues to change over the next few years. Whatever the future brings, it is certain that secure but adaptable access control will be playing an important part in keeping people safe and secure, whatever the threats we face.