MAKING THE CHOICE

Fixed costs, customized solutions and user convenience - determining factors in buying physical identity and access management

By Ajay Jain

The migration of physical security technology to a network platform has made it easier and more convenient for organizations to integrate the various modalities of physical security into a unified configuration to better safeguard their employees, visitors, premises and material/intellectual property. Open architecture further enables central control of the various security systems on a single platform, providing higher levels of operational efficiency across the enterprise as well as improved standardization of policies and procedures.

Similar operational benefits have been achieved from advanced physical identity and access management (PIAM) software solutions that allow security identities to be managed and streamlined across disparate physical security systems within an organization by creating a single identity for each individual across all physical security systems. Integrating physical with logical systems, the software can ensure synchronized and policy-based on- and off-boarding of identities and their physical access levels across multiple security systems.

With increasing frequency, enterprise-wide physical identity and access management software systems are playing key roles in organizational strategy. Physical identity and access management software is a ready-made solution for organizations looking to upgrade and enhance their physical security strategies, remain compliant with requirements mandated by various regulations or integrate and maintain alignment with security policies during and after a corporate consolidation.

TO BUILD OR BUY

Without question, PIAM software is an effective tool that can readily address multiple challenges where improving efficiencies through identity management is needed. The uncertainty arises when making the decision as to whether a PIAM software package that addresses compliance, operational and quality needs should be developed internally or purchased as a commercial, off-the-shelf (COTS) solution.

The appeal of building an in-house, custom application is often founded on the belief that company processes, business challenges and unique needs are better understood within an organization, rather than by an outside vendor. The solution can be developed more accurately and less expensively.

Conversely, many identity management issues and requirements are similar in nature, and it will save time, and potentially costs, to purchase a COTS package developed by a more specialized software developer.

Understanding the differences between these two approaches can yield significant benefits, but it's not an easy choice to make. There are, however, three key areas that should be considered when making the choice between an in-house developed solution and a COTS package:

Cost. If considering an in-house developed solution, costs must include the time-intensive process of developing the outline/application, assigning personnel and determining charge-back costs for development, testing and support. Because of the nature and complexity of the PIAM application, the development must take into consideration workflow that integrates a variety of business system processes as well as the integration between existing hardware and/or software systems. For example, when one set of privileges changes, whether physical or logical, that alteration must trigger automatic, complementary revisions in other sets.

With regard to the development team, assignment of personnel is dependent upon the technology resource pool and their experience with this platform. The team may have to be expanded to include personnel with expertise in specific business processes.

Based on these drawbacks, recent trends indicate that organizations are no longer looking within to create and maintain the custom applications that address large scale identity management needs, but rather are turning to external, professional resources that offer application-targeted solutions built on best practices and with a proven track record.

Unlike an in-house developed software program, costs for COTS solutions can be negotiated and determined up front. Any additions or custom developments can be quantified prior to the start of the project, and a schedule for incremental upgrades or changes can be identified for budgeting purposes. In addition, COTS solutions usually provide a better ROI over the long term based on more robust features, greater reliability and the ability to scale at a lower cost than an in-house solution.

Customization. In many organizations and vertical industries, regulatory compliance is the impetus for instituting an identity management program. For example, corporations subject to the Sarbanes-Oxley Act require stringent management of user identities and access to information while ensuring system integrity. The CFATS rule governs the petrochemical industry, while the Gramm-Leach-Bliley Privacy Act protects information in the finance arena. In other areas, NERC/FERC security regulations govern the energy sector, and HIPAA privacy rules are enforced in healthcare. Banks need to comply with the Basel Committee on Banking Supervision, and pharmaceutical companies are regulated by the Drug Enforcement Agency. Government agencies perhaps face the greatest need for compliance, including FIPS 201/HSPD-12 credentialing requirements and TSA regulations for airports.

Custom solutions that are in compliance with mandated access control requirements are more readily available from vendors who understand the requirements from both the business/regulation side and the technical side. The work is done, built into the application, and in most instances, the software program will meet the customer's requirements out of the box.

Convenience. Operation and use of PIAM software must easily and readily include the capability to manage all types of identities including permanent and temporary employees, contractors, service providers and vendors. It should be an easy and straightforward process to manage details of a physical identity, such as biographic and biometric information, as well as results of security checks and historical usage. In addition to aggregating access level information from various systems, PIAM software should encompass details such as risk level, area owner, multiple approvers and prerequisites for access, while providing audit trails of all transactions. These features, and other proven system amenities, make implementation and use of COTS software more convenient than a homegrown solution.

The ideal COTS solution will take cost, customization and convenience into account, as Quantum Secure did when we created our policy-driven SAFE software suite. We believe a COTS solution should be designed to connect disparate physical security, IT and operational systems, automate manual security processes around contractors and reduce both costs and risks.

The host of applications provided to automate physical security system functions must include physical identity management, role-based access, self-service administration, identity/event correlation and reporting. Control should be provided through a single, Web-based interface that is easy to manage and use.

A properly designed and engineered COTS solution, for physical access and identity management, will be the more cost effective solution every time.

Ajay Jain is the president and CEO of Quantum Secure.