WHITE PAPER

How Enterprises Can Benefit from Physical Identity and Access Management

Market Pulse

A NEW IDG RESEARCH SURVEY REVEALS A GAP BETWEEN ENTERPRISES' DESIRE FOR THE INTELLIGENCE PIAM OFFERS AND ITS IMPLEMENTATION.

For many years, IT has been focusing on eliminating silos between systems to better streamline and audit business processes. Whenever multiple, disparate systems collect similar information, chances increase for inconsistencies or inaccuracies. Silos are insidious: They propagate in places one might never expect.

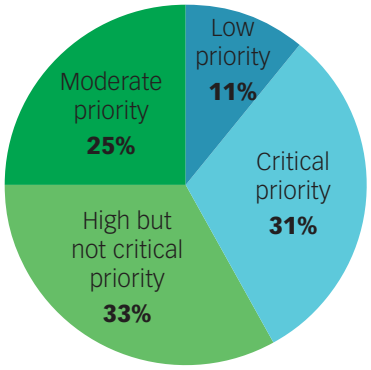
Take the area of identity and access management (IAM). IT rightfully has focused on the digital aspects of authenticating and authorizing employees' identities when they access data. But in addition to digital access to data, enterprises also control physical access to data—whether it's in a data center, a server room or someone's office—through badges, ID cards or keys. The problem is that, too often, the systems tracking physical access and those tracking digital access—even though they both monitor the movements of employees and contractors—are disparate and siloed.

To eliminate these silos, the boundaries of IAM are evolving to incorporate the physical aspects of access. Research firm Gartner defines physical identity and access management (PIAM) technologies as providing "authentication, authorization and provisioning services to control access to doors and other physical environments." Because PIAM is still new to many CIOs and CISOs, there is still some confusion about exactly what it entails and how enterprises can benefit from it. Nonetheless, a new IDG Research survey reveals a high level of interest in the capabilities of PIAM.

That's because PIAM not only brings together physical and digital identity access management systems, but it also integrates those systems with back-end employee and contractor databases, digital access management repositories (such as Active Directory), training systems and compliance applications—in short, any application linking an employee to his role and its security-related activity. For IT executives concerned about security and compliance, PIAM can deliver new levels of insight and integration—while eliminating corporate risk and one more silo.

PIAM is a high business priority and has increased as a priority over the past 12 months.

Importance of Physical Identity Management as a Business Priority



100 RESPONDENTS INVOLVED WITH PHYSICAL AND/OR IT SECURITY PURCHASES AT THEIR ORGANIZATION

CSO Custom Solutions Group

QUANTUMSECURE

» Why PIAM Is Important

In today's security-conscious enterprise, PIAM provides real value by reducing both digital and physical security risks. It manages policies, procedures and access rules for on-boarding and off-boarding all kinds of worker identities—full- or part-time employees, contractors, vendors or temporary workers. By correlating employees' specific roles or identity attributes with data access, whether physical or digital, enterprises can more consistently control access. By centralizing the provisioning process and automating the workflows relating to requisitions and approvals through a PIAM system, enterprises can quickly and efficiently ensure security and auditing of access.

Just as important, they can correlate information about physical events (badge swipes, access attempts) with the identity of those attempting the access. This knowledge helps enterprises provide audit information for both risk management and regulatory compliance requirements.

Because of these capabilities, 64 percent of IT executives consider implementing PIAM a critical or high priority, according to the IDG Research survey. Almost as many executives—60 percent—believe PIAM has increased as a priority over the last year. Respondents also report that PIAM systems could increase operational efficiency and improve business processes, especially in specific areas.

For instance, PIAM can classify physical areas with different thresholds of concern (so that, say, an attempted data center breach triggers a higher response than one at an unused facility). This information can generate reports related to incident handling, allowing IT to track, through KPIs, improvements in response time and security.

PIAM systems can also identify areas where badge access is not required, an indication that workers can have access to areas that are unnecessary to their jobs. In addition, PIAM systems can compare badge use with capacity data. This information can inform cost optimization discussions around how much office space is necessary.

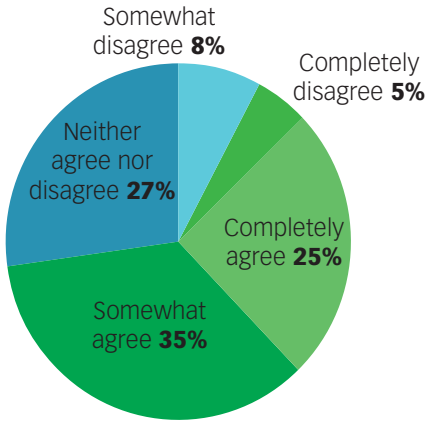
» Why PIAM Is Important

In the IDG survey, just 20 percent of respondents report having what they consider to be complete insight into details of physical access for employees. Physical access control systems (PACS)—from vendors such as Tyco, United Technologies, Honeywell, Johnson Controls, Software House and Lenel—record workers' access details in their logs. However, without PIAM, questions about why someone has access (what rules and policies governed granting that access, when the access must be removed, and how and when access must be recertified) remain unanswered. Currently in most enterprises, granting, revoking and reinstating access are manual processes. PACS are great for access, but not for policy insights.

PIAM systems, on the other hand, accurately manage and track the granular aspects of physical security access, such as:

PIAM is a high business priority and has increased as a priority over the past 12 months.

Agreement that PIAM has increased as a priority over the Past 12 Months



100 RESPONDENTS INVOLVED WITH PHYSICAL AND/OR IT SECURITY PURCHASES AT THEIR ORGANIZATION

- **WHO.** Any given enterprise offers access to a dizzying array of roles: employees, contractors, seasonal employees, temporary employees, visitors, vendors.
- **WHERE.** PIAM systems accurately assess who is where and why. Physical access, when correlated with the risk profile of workers and that of a physical space (secure areas such as data centers exhibit higher risks than other locations, such as cafeterias), creates tight policy control and accountability. Sometimes access relates more to risk management than security. For instance, someone with no training on machinery should not have access to the factory floor, both for his own safety and because of potential liability issues.
- **WHEN.** Enterprises can identify potential unauthorized activities by tracking who attempts access to specific areas after hours or on weekends. Employees may be working, but for sensitive projects, enterprises may want to set up authorization ahead of time.

That's why a majority of survey respondents (77 percent) agree that integration between physical and digital security systems should be improved. Unfortunately, only 28 percent expressed confidence that when employees or contractors leave, their physical access is revoked.

Furthermore, 41 percent of respondents are concerned that they haven't identified all areas of vulnerability. That's because with today's plethora of new technologies, challenges continue to appear. For instance, 63 percent consider it a high or moderate priority to have access to physical identity management processes via smartphones and tablets. Almost all respondents report that they would like to use mobile devices to submit and process requests for badging and physical access.

» How PIAM Eliminates Security Silos

PIAM eliminates silos because it manages the physical perimeter access and integrates that data into back-end systems. This capability gives a PIAM system more functionality than a PACS, which many enterprises have deployed, or custom solutions that IT may have built. Leading-edge PIAM software can integrate policy information from multiple PACS deployed in an organization to create a single management view. PIAM systems also connect with security systems in IT and database systems in human resources systems to manage a person's identities throughout his employment with the enterprise.

That kind of automated insight and reporting is crucial. Research has consistently shown that security problems derive as much from internal employees as they do from external hackers. Sometimes breaches are inadvertent, sometimes not. The point is that it's prudent to track workers in both their physical and their digital representations, and to do so in a way that provides a consolidated view. Someone trying to misappropriate data over the network may be thwarted, but then attempt to download information directly from a server. The policies that bar an employee from digital access should also bar him from physical access.

Having that information in two separate systems would require an IT security expert to manually compare logs to make sure an employee's physical and digital access profiles match. Automated PIAM solutions managing both kinds of access not only provide better controls, but also reduce manual, time-consuming efforts on the part of security administrators.

Eliminating these silos also ensures smoother processing of worker on-boarding and off-boarding. With an integrated system, IT can see that new employees have proper access to any area or digital asset they might need—and can quickly revoke all access when they leave the company. Without PIAM, the security team must manually remove access from each system, which is time-consuming, error-prone and seldom done consistently. Consider this: According to a July 2013 report by NBC's Washington affiliate , a former Reagan National Airport contractor continued to access airport facilities—including airplanes—even after he was terminated. It turned out that he hadn't surrendered his badge, and his access privileges hadn't been revoked.

By implementing an integrated PIAM solution, enterprises can define all policies and procedures relating to the on-boarding and off-boarding process. PIAM software creates an audit trail of access events. This information, in turn, can be used as evidence in compliance audits, showing that specific employees did not have access to unauthorized areas.

» Benefits of PIAM

Enterprises can derive other significant benefits from deploying a PIAM system. In fact, the benefits and the resulting ROI frequently far outweigh concerns about the system's deployment and integration costs.

It's not just that enhanced physical security systems limit the chance of breaches. It's also that integrating HR, PACS and other IT systems improves efficiency by automating workflow, business processes and management of physical access rights across multiple systems.

The enterprise also gains better insights into user activity, allowing it to make decisions beyond security related to real estate and capacity needs. In addition, thanks to an integrated system with automated workflows, enterprises eliminate the time-consuming efforts involved in audits and compliance regarding access.

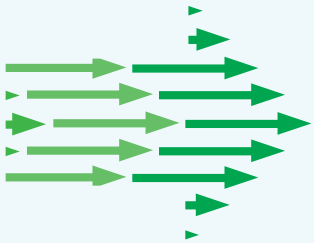
Most enterprises will benefit from deploying PIAM, especially geographically distributed multinationals that have a fluid population of employees, contractors and visitors.

But even single-campus businesses can benefit from PIAM. Consider an airport, which not only has extensive physical grounds to protect, but must also grant access to employees of multiple subcontractors, from airlines to restaurants. However,

The majority of respondents agree that integration between physical and logical security systems could be improved.

BASE 100 RESPONDENTS INVOLVED WITH PHYSICAL AND/OR IT SECURITY PURCHASES AT THEIR ORGANIZATION

HOW QUANTUM SECURE CAN HELP WITH PIAM



Quantum Secure has deployed its PIAM solution in Fortune 500 organizations, U.S. federal agencies and other regulated markets for many years. Its SAFE Suite offers unique solutions for convergence of both physical and digital management of physical identity lifecycle and associated access.

It allows enterprises to streamline access requests and approval processes across multiple types of employees, roles, user-access profiles and physical access systems. This approach allows enterprises to create business policies and workflows using graphical drag-and-drop functionality, without any programming knowledge.

As a result, security managers can deploy proven best practices using graphical whiteboards, enabling diverse physical security systems worldwide to conform to consistent corporate policies. In using prepackaged approval, provisioning and termination workflows, users can automate and streamline physical security tasks. This, in turn, minimizes both costs and risks, helping enterprises comply with industry and government regulations.

because those employees do not work for the airport itself, they would not be tracked by an employee database.

PIAM is just as important in other industries, especially those that have extensive numbers of subcontractors on site or are subject to high levels of regulation. These include energy and telecommunications companies with respect to power plants and other facilities; companies with significant levels of high-value intellectual property, such as pharmaceuticals and technology companies; and companies with responsibility for multiple locations, such as real estate firms.

Increasingly, PIAM is gaining momentum in the public sector and other vertical markets as well. The financial services industry benefits due to increased audit capabilities over access to restricted areas. PIAM helps utility companies with NERC/CIP compliance issues. The aviation industry benefits from automating its TSA credentialing and compliance processes. The U.S. government benefits from PIAM in regard to its physical access requirements for employees and contractors under Homeland Security regulations.

» The Overall Payoff

PIAM solutions offer distinct benefits in the following three categories:

- **CORPORATE RISK REDUCTION:** Enterprises can configure and customize PIAM applications to comply with the policies and procedures of their company and specific industry. Physical access authentication, authorization and ongoing management dramatically reduce corporate security risks.
- **OPERATING COST REDUCTION:** PIAM supports automation of processes and procedures related to enterprise access governance as well as self-service access management, leading to less reliance on error-prone manual processes.
- **COMPLIANCE:** Regulated industries, such as healthcare, financial services and utilities, can define internal controls related to physical access, audit and access recertifications on a periodic basis, including audit background checks against criminal databases.

PIAM ELIMINATES SILOS BECAUSE IT MANAGES THE PHYSICAL PERIMETER ACCESS AND INTEGRATES THAT DATA INTO BACK-END SYSTEMS.

A properly deployed and configured PIAM solution can deliver these benefits, while integrating physical and digital access rights at the same time. With this integration, PIAM solutions provide unprecedented insights into an enterprise's security posture, ultimately providing a high level of reliability and confidence for IT and security officers.

For more information on PIAM, visit www.quantumsecure.com/SAFE