

# Bridging the Great Divide: The convergence of physical and logical security

By David Ting

---

**Many organizations are now looking to bridge physical and logical access systems for unified enterprise security management, and as these companies are realizing the benefits of a converged solution, the industry is beginning to redefine the role of security.**

The role of security is changing dramatically. Many organizations are now looking to bridge physical and logical access systems for unified enterprise security management, and as these companies are realizing the benefits of a converged solution, the industry is beginning to redefine the role of security.

All organizations need to protect their corporate assets – whether it's preventing the theft of office equipment, providing a safe environment for employees and their belongings, or keeping hackers and industrial saboteurs from wreaking havoc with networks, applications and databases. Yet, because physical and logical security have traditionally been handled by separate organizations and technologies, few companies can envision the benefits from their convergence.

Physical and IT security departments have been operating as distinct entities for years. Now security concerns around networks and databases have led some organizations to ask why physical and logical security systems cannot work together to share real-time data and strengthen each other.

## Converged security

As a practical definition, “converged security” refers to the integration of physical access systems and related technologies (such as magnetic cards and readers) with identity management and user authentication technologies (such as enterprise single sign-on, tokens and proximity cards). This integration enables an organization to establish and manage a single, consolidated repository of all user authentication credentials, and to employ a centralized means to establish access policies for all physical and logical resources.

The concept of converging physical and logical access security is not new. It has been around for some time, but historically, implementation has been a problem. Because physical and logical security systems traditionally operated in totally independent worlds with no reason to interconnect, convergence has always been costly and

complex. Various vendors have tried to solve this problem using approaches such as multifunction cards, pure identity management solutions and consolidating reporting systems. For a variety of reasons, these efforts have not been successful and have proved costly and extremely time-consuming to implement – often taking several years coupled with major investments. However, an opportunity now exists for the worlds of physical and logical access security to come together at last.

Physical and logical convergence makes it possible for organizations to have:

- One identity-based system for managing all physical and logical access
- A unified network policy for both network and remote access that leverages card status and user location information from physical access systems
- Tight correlation between building, LAN and remote VPN access for a tighter security posture
- Enforcement of company anti-passback/tailgating building access policies
- Exchange of events and alarms from the physical access system to the logical access system
- An identity-based reporting system for use in forensic investigations
- A streamlined workflow for creating, deleting and modifying user identities from both systems simultaneously

With the convergence of physical and logical security technologies, organizations now have new opportunities to better coordinate security resources in critical and emergency situations and achieve compliance with regulations, such as US Homeland Security Presiden-

tial Directive 12 (HSPD-12) or the Federal Information Processing Standard (FIPS). HSPD-12, which mandates a common identification standard for US federal employees and contractors, was issued by the US Executive Office of the White House in 2004. The convergence of these two technologies provides the two-factor authentication that ensures compliance with these regulations.

## Benefits of convergence

When physical and logical access security components work together, organizations can use them to complement and reinforce one another. For example, a network access policy could be established that would grant a user logical access to applications only if that user had first swiped his or her employee badge that day when

---

**Tailgating is a common security problem in which a person without an ID badge gains access to a facility by following closely behind another person who has just swiped his or her badge.**

---

entering a facility or restricted area. Furthermore, companies can grant or refuse network access based on a user's physical location, user role and/or employee status. This means that all users must physically badge in to use the organization's facilities and network – and cannot access their company's virtual private network (VPN) while already logged in to the building. This prevents fraudulent user logins, further raising the protection of each user's identity and the organization as a whole.

Tailgating is a common security problem in which a person without an ID badge gains access to a facility by following closely behind another person who has just swiped his or her badge. With convergence, logical access security can be set up to alert corporate security whenever employees who have not swiped their badges attempt to log on to PCs, thereby providing a means to better enforce badge-swipe compliance and facilitate the enforcement of company anti-passback/tailgating building access policies.

Convergence provides companies with affordable two-factor authentication (complex passwords and a second form of identification), which is recommended by experts as the best protection against unauthorized application access. Convergence at the system level enables reuse of the existing card-based infrastructure, and would allow even badges with magnetic stripes to be used as the second factor, sparing organizations the cost of additional smartcards, tokens, or biometric scanning systems, while at the same time strengthening IT security.

With the convergence of physical and logical security systems, organizations have the ability to coordinate responses to problems and/or emergency situations. For example, when employees resign or are terminated, there is often a lag time of days or even weeks between when their physical access rights and logical access rights are terminated. This situation often results in disgruntled former employees logging in remotely and stealing confidential data. Convergence prevents this problem by allowing organizations to terminate physical and logical access privileges simultaneously.

## Conclusion

What organizations are ultimately looking for is greater control over all aspects of their security. Convergence allows organizations to maximize the security potential of both systems to protect corporate assets, while not forcing dramatic workflow changes on the employees. Organizations of all sizes and types are taking the first, positive steps toward physical and logical access security convergence and a more secure future. All of these benefits, plus the better protection, cost savings, risk reduction, and increased compliance associated with them, make converged physical and logical security a worthwhile goal for any security-minded organization.

## About the Author

*Recently named as one of InfoWorld's Top 25 CTOs of 2006, David Ting has more than 20 years of experience in developing advanced imaging software and systems for high security, high-availability systems. Prior to founding Imprivata, he developed biometric applications for government programs and Web-based applications for secure document exchange. David was formerly the technical manager of Kodak's Boston Technology Center, a systems development group for Eastman Kodak. Prior to that position, he managed Atex System's Imaging Department, where he was responsible for the first full-color output system used in the newspaper industry.*