

ACCESS CONTROL TRENDS & TECHNOLOGY

Opening the Door on Enterprise Security



The path to security systems unification can start at “the edge”

By Tom Heiser
and Eli Gorovici

Long before we were first exposed to the wonders of the Internet, computer viruses, pharming and phishing attacks, enterprise security was an important business priority. In most organizations, however, physical security is managed by one department, while data security is looked after by another. As a consequence, security administrators are left with multiple user databases, redundant and/or disconnected security policies and totally independent systems

and technologies. The net effect of the gaps created by this model is that the enterprise remains vulnerable to both physical and data security breaches.

Today's security challenges demand we adopt a more "holistic" view of enterprise security. New security threats, compliance requirements, and a myriad of available security solutions must be balanced against other business priorities, limited budgets and staff. Enterprise security has developed into a "team" sport that requires a more integrated and layered approach. No longer is the security department locked away in the basement beyond the reach and attentions of the rest of the company.

Physical and IT Security Convergence

Managing digital identities and user access is more important than ever. Security should be the joint responsibility of both building security and IT. Traditional integration solutions have historically been intrusive, difficult to deploy and costly. New open platforms and software-based systems fit nicely into the IT structure for both IP-based access control and video surveillance.

For the past 20 years, IT and physical security have been operating as separate entities, so it is natural to question why it is so critical that their paths intersect now. The reason is simple: Now more than ever, the IT department and the security department occupy common ground. Asset management is clearly tied to possible breaches in IT security. As physical security increasingly uses IT equipment, the sharing of the network becomes an issue.

There is no question that we are experiencing another form of convergence and it is critical that each group work with the other to leverage their individual expertise.

An Industry IP Snapshot

There is general agreement that 15-20 percent of video surveillance installations are true IP-based solutions. An even larger num-



ber of installations are using hybrid technologies that will eventually move to true IP.

Until recently, there was no true IP access control solution. Very similar to the hybrid video solution, access control did not go directly to the edge — it stopped at the control server and the rest of the journey to the door was based on traditional wiring. Today, access control

is beginning to follow the evolution path of video surveillance, and we are beginning to see software and hardware that is designed on IP standards directly on the door.

We are seeing concerted movement toward open standards so that multiple systems can reside on the same platform, creating an end-solution that can be customized to meet the needs and requirements of each individual installation.

Why IP Access Control?

IP-enabled access control processor platforms and host interface solutions that go directly to the door are now available. They are designed to provide a complete and full-featured access control hardware/software infrastructure and contactless smart card read/write capability at "the edge" of the network for software-based host systems. A perfect solution for new building installations, these products require less wiring (standardized), are cost-effective and are ideally suited for today's IT-centric security environment. Impressive end-user benefits for these solutions include:

- **Installation.** New projects can be more rapidly deployed with significantly



less wiring to the door. Today, 16 wires are required per door. With IP, only a single CAT 5/6 is needed, and that is often already in place. The IP solution uses off-the-shelf equipment, including standardized power supplies and enclosures, which make a much smaller footprint than traditional access control. When combining IP access control with other IP solutions such as video surveillance, hardware can be shared for multiple applications including storage, networking, wiring and battery back-up. Users can also integrate their current access control solution and migrate to IP as doors are added. It is easily scalable from one access point to thousands.

- **Technology.** IP-to-the-door is a Power over Ethernet (PoE)-enabled technology, so only one cable is required for both network and power. As a software-based solution, upgrade costs are effectively minimized. End-users maximize investment by using the latest hardware technology and leveraging the existing IP infrastructure.

- **Infrastructure.** Each installation where access control is being deployed already has an IP/IT infrastructure, so the IP-to-the-door solution takes full advantage of wiring, hardware and systems already in place. And wireless is becoming a prevalent solution when hard wiring is not available — again cutting down on installation issues.

- **Maintenance.** With an IP-based solution, existing IT management tools help isolate any issues that might occur within the access control solution. You also have the added benefit of survivability. Today, if an eight-reader panel fails, all eight doors go down. With IP-to-the-door, only one door is lost on failure, which means less downtime, less maintenance and no catastrophic failures. A major benefit of IP-based systems is a constant “health check,” which will immediately notify the user if a reader is down. A traditional system will not report

failure until a user is unable to open a door or access point.

- **Services.** An IP-based solution means one maintenance contract for your physical security command-and-control center, including access control and video. Time is reduced with implementation to provide a more predictable model

door very expensive. Then with the next door, the cost per door spikes down, because you have spare ports. With IP-to-the-door, you can leverage the cost savings of the IT environment to secure more doors. With a fixed cost-per-door, physical security pays less per door; thus enabling organizations to deploy more security for the same amount of the

“IP-based solutions are 30 percent less expensive to purchase, 30 percent less expensive to install and take 30 percent less time to learn.”

that is more easily bundled and priced to protect margins. This also creates one platform for cameras, doors, IT security, reporting mechanisms and other integrated software solutions for configuration, maintenance and management.

- **Network Wiring Out of the Closet.** IT closets are valuable real estate, and people are fighting for wall space. Under the old paradigm, physical security needed to coordinate with IT to get room on the wall. With IP-to-the-door, that wall space is unnecessary — all you need is one CAT-5 going out. If you have PoE and UPS power on your network equipment, it does not even require another power supply. Edge technology enables physical security to extend the network wiring out of the closet. No more controller or power supplies clogging up the closet anymore — it is right at the door.

- **Pay Less Per Door.** Before IP-to-the-door, if you wanted to add one door, the first thing you needed to know was, “Is there room on one of the panels to add one?” If not, you had to buy another panel to add this door, making the first

money. IP-to-the-door offers a fixed cost-per-door, including the product and the locking hardware. It is easier to budget, and the cable and installation cost less. There is also the added benefit of greater installation flexibility — if a controller is not close, the network is always nearby.

- **Increased Physical Security Focus.** The physical security department still manages the access control. They still own the door and what controls the door. As physical security becomes leaner and more efficient, they can focus more on management instead of installation because the majority of power, capability and capacity issues will be managed by IT. Physical security will still need the security integrator and the knowledge he or she brings to manage the access to the door. The ownership of how you get from the closet to the door, however, is now controlled by IT.

Once IP-to-the-door is fully understood and widely deployed, it opens new possibilities with respect to already-deployed IP video surveillance solutions. This illustrates how access control and video make the leap from “integration” to “unification.”

After Integration: Unification

Integration means only that two products work together. Unification means that a single, multi-functional application can provide unified security, administration and event response.

Integrated systems require a user or integrator to log into separate systems to program coordinated responses to system events. Failure to program either system properly can cause inconsistent or failed responses — and because integrated systems remain separate, neither can detect the programming inconsistency and warn the user. Technical support teams may not be able to resolve the problems efficiently because they are not aware of the inconsistencies, thus increasing total cost of ownership and system downtime.

Unification brings about a higher level of availability to physical security due to access/video server consolidation and more efficient use of standard hardware, IT tools and a shared knowledge base. Unification goes well beyond integration, and unified systems are already exerting major impact in terms of system cost, efficiency, overall capabilities and level of security.

Cost Effectiveness with Increased Efficiency

A unified system means one user interface, simplifying installation, training and operation. No more duplication of system administration and other tasks. What's more, a single user login provides simple and secure access to all security func-

tions. Unified IP systems also provide higher availability and reduced maintenance costs due to access/video server consolidation — and networking issues are handled by the IT department using standard tools and practices. Unified system manufacturers will also offer unified hardware — for example, access panels that can store video and control pan/tilt/zoom cameras. The unified system is no longer reliant on the host computers for control or DVRs for video recording, which adds a level of survivability and greater efficiency, since edge devices can control both aspects of the system. Because of this architecture, IP-based distributed processing allows for modular, unlimited expansion of both access control and video based on needs and budget.

New unified systems already offer much more than the yesterday's "advanced" integrations of bolted-together components. Thomas L. Norman, CPP/PSP/CSC, author of the book "Integrated Security Systems Design," best summed up the tremendous potential IP-based solutions offer: "I go by the 30/30/30 rule," he says. "IP-based solutions are 30 percent less expensive to purchase, 30 percent less expensive to install, and take 30 percent less time to learn."

Unified IP-based systems provide enormous advantages in terms of system openness and

flexibility; enhanced efficiency at lower costs, higher levels of functionality and improved overall security. Unified systems, based on open architecture, are just beginning to demonstrate their unique power and functionality. ●

Tom Heiser is vice president of Networked Access Solutions for HID Global, with responsibility for setting the business objectives, strategy development and tactical action plans for VertX and IP devices on a worldwide basis. Prior to joining HID Global, Heiser was with Tyco Safety Products, where he was director of product management for Access Control and Video Systems (ACVS).

Eli Gorovici is president and CEO of DVTel Inc. He has more than 15 years of senior management experience in the digital data communications industry. Previously, Gorovici was vice president, global sales and marketing, for NICE Systems' Visual Interaction Management Division.



Tom Heiser



Eli Gorovici



HID Global
9292 Jeronimo Road
Irvine, CA 92618

For more information, please visit our
web site at www.hidcorp.com/edge

Contact: Thomas Heiser
949-598-1668

email: theiser@hidcorp.com