



January 11, 2005

## Trends 2005: Security Convergence Gets Real

A Market Niche Matures

by **Steve Hunt**

with Jonathan Penn, Andy Bartels, and Stephan Wenninger

### EXECUTIVE SUMMARY

Growing numbers of organizations are recognizing the natural economies of scale and operational efficiencies available when physical security teams work with similar, complementary IT security groups. In 2005, companies in Europe and North America will increase spending nearly threefold on projects that combine traditional physical security controls with IT security. That is, locks, cameras, entry systems, and even guard desks will be upgraded to work with the same computing systems that control computer and network sign-on, identity management, and security incident management. Consequently, IT security vendors will rush to merge or find partnerships with their physical security brethren to respond to the new opportunities.

### WHY "CONVERGE" SECURITY?

Historically, physical security vendors sold their products only to physical security departments, sometimes known as the corporate security, campus security, or simply facilities departments. Meanwhile, IT security vendors targeted IT security departments, the CIO, and the occasional business unit manager. The two markets have always been almost entirely segregated. But now the lines of demarcation are blurring, and customers are inviting vendors from both sides to work together.

### THE CONVERGENCE OF PHYSICAL AND LOGICAL SECURITY IS NOT A FAD

Security is no longer performed quietly in the basement of the building, away from the cares of business managers. Now, security plays an instrumental role in compliance with regulations, protection of personal information, and enabling many business processes. Therefore, business managers are looking for ways to have better security while also cutting costs and finding economies of scale. One way that this can be achieved is by converging IT security with overlapping corporate or physical security functions.

- **Consolidate credentials for IT and physical access onto a single card.** A smart card can serve as an ID badge for building access and can also store IT credentials like passwords and digital certificates. Standardizing on a single card may save costs and improve security.
- **Connect the processes for granting and revoking building and IT access.** Linking the processes for managing employees' IT access rights with those for managing their building access will get people productive quicker and will improve security by ensuring that all necessary revocations take place when appropriate.



#### Headquarters

Forrester Research, Inc., 400 Technology Square, Cambridge, MA 02139 USA  
Tel: +1 617/613-6000 • Fax: +1 617/613-5000 • [www.forrester.com](http://www.forrester.com)

- **Correlate security events across the physical and IT realms.** Security event management systems, presently used to monitor and respond to IT-related events, should incorporate events from physical security systems. An alert should trigger if, for example, the VPN signals an employee logging in remotely while the badging system indicates that he is inside the corporate office.
- **Unify the auditing of physical and IT rights and events.** By assessing authentication and authorization processes and controls across IT and physical facilities, organizations will find many opportunities for improved efficiencies and security. For example, Forrester recently performed an audit that showed ways in which one company could streamline processes of employee and visitor badging by integrating existing identity management systems. It also indicated that the company could save money on cameras by aligning intruder detection processes with the IT incident response procedures.

### Watch For Sudden Growth During The Next 12 Months

The market, currently described as the convergence of physical and logical security, is beginning to take off. Forrester expects private-sector spending to top \$300 million in 2005 (see Figure 1). Europe will lead in per-capita adoption with projected spending of more than €137 million. Total spending on convergence projects in the public and private sectors in North America and Europe will exceed \$1.1 billion in 2005.

### These Numbers May Be Conservative

Some public sources project much higher spending by government agencies and port authorities. Although 2005 budgets have been announced or allocated for massive government convergence projects, Forrester does not expect actual spending to exceed this forecast because of political factors and the complexity of the proposed projects.

Disaster planning is another area of natural convergence. But because disaster recovery best practices have long called for IT systems and physical system backup, Forrester did not calculate disaster-recovery-related spending in this forecast.

Furthermore, the specter of regulations affecting IT security certainly could cross over and converge with physical security. After all, it will only take a few large audit firms to start including physical security checks in their Sarbanes-Oxley audits to transform the nature of security management. If that happens, spending could as much as triple over these forecasted numbers.

**Figure 1** Forecast: Europe And NA Security Convergence Spending, 2004 To 2008**1-1 Forecast: Europe and North America security convergence spending (US\$ millions)**

	2004	2005	2006	2007	2008
Large-scale convergence projects in NA and Europe	19	68	175	382	856
Physical/logical access control projects in NA and Europe	50	150	413	903	1,656
Other projects performed jointly by IT and physical security departments in NA and Europe	13	45	118	246	406
Public sector: border control convergence systems, law enforcement projects in NA and Europe	410	820	1,899	4,202	8,003
Small projects (data center security, communications security, etc.) in NA and Europe	14	40	108	229	369
<b>Total</b>	<b>506</b>	<b>1,123</b>	<b>2,713</b>	<b>5,962</b>	<b>11,289</b>

**1-2 Forecast: North America security convergence spending (US\$ millions)**

	2004	2005	2006	2007	2008
Large-scale convergence projects in NA	10	36	93	202	453
Physical/logical access control projects in NA	30	90	248	542	994
Other projects performed jointly by IT and physical security departments in NA	10	35	92	191	315
Public sector: border control convergence systems, law enforcement projects in NA	250	500	1,200	2,600	5,001
Small projects (data center security, communications security, etc.) in NA	10	30	81	172	277
<b>Total</b>	<b>311</b>	<b>691</b>	<b>1,713</b>	<b>3,707</b>	<b>7,039</b>

**1-3 Forecast: Europe security convergence spending (€ millions)\***

	2004	2005	2006	2007	2008
Large-scale convergence projects in Europe	11	39	101	219	491
Physical/logical access control projects in Europe	24	73	201	441	808
Other projects performed jointly by IT and physical security departments in Europe	4	12	32	68	112
Public sector: border control convergence systems, law enforcement projects in Europe	195	390	853	1,953	3,663
Small projects (data center security, communications security, etc.) in Europe	4	12	33	70	112
<b>Total</b>	<b>238</b>	<b>527</b>	<b>1,220</b>	<b>2,751</b>	<b>5,186</b>

\*US\$ to Euro exchange rate: €1.22

(numbers are rounded)

Source: Forrester Research, Inc.

### Convergence Projects Improve Efficiency And Security

The reasons for the sudden rise over the estimated \$500 million total sales of 2004 include the large European Union-funded border, law enforcement, and homeland security projects, especially in Eastern Europe, as well as the availability of US Homeland Security funding. Additionally, early adoption of multifunction smart cards as a single card for physical and logical access and the emergence of new convergence technologies from companies like CoreStreet and NetBotz have added to the sales rise. Companies like Honeywell, Siemens, and others have contributed to the increase with technologies involving large-scale system integration consisting of authentication, authorization administration, and audit processes.

Additional factors contributing to the rise in 2004 sales includes:

- **Standardization.** The convergence think tank Open Security Exchange is growing in prominence as a standards discussion group.<sup>1</sup>
- **Entry-point technology.** Fingerprint, hand geometry, and facial recognition biometric readers at large campus entry points, airports, borders, and other ports are becoming increasingly common.
- **Surveillance.** IP-based network cameras from Axis Communications, Panasonic, and Sony Electronics and enhanced video systems from vendors like Extreme CCTV, NICE Systems, and ObjectVideo, continue to grow.
- **Integration.** There are new possibilities of integration between camera and access control systems, such as consoles that display video of physical or logical access events along with event log details of that event: Archival searches of access events along with video images are also becoming available.
- **Security event management.** Vendors ArcSight, eSecurity, and others are following Computer Associates' lead in converting their event monitoring consoles, which were originally designed for IT security events but can now correlate physical access events.

### VENDORS AND SYSTEM INTEGRATORS WILL ADAPT SLOWLY AT FIRST

According to a recent ranking by Wachovia Capital Markets, large physical security system integrators like Computer Sciences Corporation (CSC), Lockheed Martin, and Northrop Grumman collectively account for 39% of the market share for US federal government system integration projects.<sup>2</sup> But none of these firms have turned their relationships with IT security vendors into significant convergence strategies.

Conversely, other top system integrators like Accenture, BearingPoint, SAIC, and Unisys have active relationships with IT vendors and are talking about the convergence of IT and physical security as a focus of their respective security practices.<sup>3</sup> While none of these firms articulates a clear vision on their Web sites regarding convergence, they nonetheless are sensitive to the challenges and opportunities of merging corporate and IT security projects in the private sector, in some cases partnering with convergence experts ActivCard and Daon.

Honeywell and Siemens are the most mature large integrators in terms of convergence strategy — they've combined IP cameras, access control, security event monitoring, and identity management in their comprehensive systems architectures. Tyco Fire and Security combines several product and service brands, such as ADT, American Dynamics, and Software House, to pull together some basic convergence projects without any formal convergence strategy or significant IT partnerships. Software House stands out, however, because it is a founding member of Open Security Exchange. Lenel Systems International is focused on products rather than integration. Forrester's conversations with Lenel reveal almost no awareness on its part of the opportunities of convergence with IT security.

#### WHAT IT MEANS

##### CONVERGENCE PROJECTS MEAN MONEY

End user organizations can save money by streamlining historically disparate security projects, while vendors can capitalize on new spending.

- Firms with interest in improving operational efficiency may now comfortably explore convergence projects.<sup>4</sup>
- Smart cards function as a platform for multiple uses: corporate ID badges, building access, computer and network access, and more.
- New technologies (most notably from NetBotz and CoreStreet) open up new opportunities for efficient identity and privilege management, security monitoring, and trouble detection.
- A team comprised of members from the two security groups should coordinate their efforts in complying with common standards and regulations.
- Convergence extends beyond products. Organizations can develop joint awareness and training workshops addressing common security concerns: social engineering, proper document and data disposal, workplace harassment policies (including e-mail and Web use), and more.
- The convergence market will grow rapidly during the next five years as enterprise risk management points more companies to greater security efficiencies and effectiveness.
- Vendors of physical or logical security controls ought to investigate trends and seek out convergence applications for their respective technologies.

## SUPPLEMENTAL MATERIAL

### Online Resource

The underlying spreadsheet detailing the forecast in figure 1 is available online.

### Methodology

Forrester gathered data from interviews with 60 end user organizations in the US, Canada, and Europe. We also spoke with several vendors with products or services related to the convergence of IT and physical security, and industry experts Jill Allison of FireWorks Security Ventures; Sandra Jones, principal consultant of Sandra Jones and Company; directors of the Open Security Exchange; and members of the National Biometric Security Project.

### Vendors Interviewed For This Document

Axis	IBM
BearingPoint	Lenel Systems International
Computer Associates	NetBotz
CoreStreet	NICE Systems
Dao	ObjectVideo
Gemplus	Software House
HID	

## ENDNOTES

- <sup>1</sup> The Open Security Exchange is a group of IT and physical security companies working to establish standards and to promote convergence projects. For more information, see <http://www.opensecurityexchange.org/>.
- <sup>2</sup> Edward Caso, managing director for Wachovia Capital Markets, covers government system integrators and highlighted Anteon as an important IT integrator in his November 30, 2004 report. He also ranked CSC, Northrop Grumman, and SAIC as the top three system integrators by annual sales.
- <sup>3</sup> All four are among the 20 Top system integrators by annual sales, listed here in order of market share: SAIC, 9.9%; Accenture, 3.4%; BearingPoint, 2.7%; and Unisys, 1.4%.
- <sup>4</sup> The most successful convergence projects allow the respective physical and IT security departments to retain their autonomy. In other words, convergence happens best as discrete projects, not as a converged security organization encompassing corporate and IT departments. See the December 10, 2003, Planning Assumption “Trends 2004: Limited Convergence Of IT Security And Corporate Security.”