

Advances in Physical Safety and Security in Government: Protect People, Assets, and Information

With leaner budgets, what can government do to better protect employees, visitors, physical assets, and information? “New IP-based physical safety and security solutions are not only more effective, they can actually reduce operational costs by tying in with each other, government communications systems, and network access controls,” says Lindsay Hiebert, emerging technologies manager, Cisco. “When all these systems are connected to the existing IP network, government can automate certain actions to shorten the gaps between detection, notification, and response.”

IP-Based Video Surveillance: Force Multiplier

The new building blocks of physical safety and security in government are IP video surveillance systems, building access controls, unified communications, and network access controls. All connect to the government’s existing IP network, eliminating the costs of separate networks.

IP video surveillance cameras can pay for themselves quickly: Wireless cameras deployed in municipal lay down yards, for example, can help to prevent copper and tools theft.

New high-definition video surveillance cameras have the potential to reduce costs still further. For example, the Cisco Video Surveillance 4000 Series IP Cameras, the world’s first with high definition, capture six times more information than standard cameras while using only a fraction more bandwidth and storage. Governments can purchase and maintain fewer cameras because one camera has the expanded field of view to replace two or three other lower resolution cameras. And higher resolution makes it possible to read license plates and recognize faces.

Other advanced video-based applications from Cisco and its partners that enhance safety or decrease costs include:

- In-car video systems that collect evidence to help prosecute and protect police departments from unfounded lawsuits. “Network-based storage takes less time to manage than VHS tapes, avoids the risk of losing video, and provides peace of mind that evidence can be easily and reliably located,” says Hiebert.
- Gunshot location systems that integrate acoustic sensors and geographic coordinates to automatically direct cameras to the incident scene.
- Automatically registering the geographic location of objects detected on video, which enhances situational awareness. For example, security personnel can continuously track and report an intruder’s exact location in relation to a protected facility, displaying the location in real time on a site map of the facility. Used in vehicles, georegistration can identify the precise location where a gun was thrown out of a moving car or an intruder is hiding.

Building Access Controls: Protecting Property, People, and Information

Protecting physical safety and security at government facilities also requires controlling who enters the buildings and rooms. Cisco Physical Access Control Hardware connects door hardware, such as card readers and locks, to the government’s IP network. Security personnel can centrally control who can enter which areas, and also lock down or unlock areas without the delays of going from door to door.

The Cisco Physical Access Control solution is especially budget friendly because governments can add doors one by one instead of buying an 8- or 16-door access control panel.

Even Better Together

While video surveillance and access control are valuable individually, their business value multiplies when they are integrated with each other and with the government's unified communications and network access control systems. A few examples:

- When someone swipes a badge to enter a building, this can trigger the video surveillance camera to send the person's image to a command center in any location. There, security personnel can compare the image with the badge photo to prevent the use of stolen badges.
- The IT group can restrict network access to employees until they have swiped their badge to enter the building. "This prevents someone from wirelessly hacking into the network from outside the facility, or for an intruder to tail gate an employee to get into the building and then hack into the network," Hiebert says.
- Events detected by the video analytics software or building access controls can automatically invoke notification of appropriate personnel on any communications device.
- The ability to view real-time video when a forced-door alarm is received can reduce the costs of responding to false alarms. The images might show that the alert was sent when someone held open a door for equipment delivery, for example, and does not require dispatching a security guard.

To read about Cisco Physical Security and Safety Solutions, visit:

www.cisco.com/go/physicalsecurity

To read a white paper describing the public safety video solutions from Cisco and its partners described in this article, visit: www.cisco.com/en/US/prod/collateral/vpndevc/ps6918/ps9145/ps9152/white_paper_c89-492776.pdf

To see demonstrations and read more about the Cisco Open Platform for Safety and Security, visit: www.cisco.com/go/iacp2008




Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

 CCDE, CCVP, Cisco Eos, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0801R)