

The New Face of Physical Security: Converged Detection, Assessment, and Response

To protect people and assets and maintain continuity of operations (COOP), government agencies have invested in multiple physical security systems, including access control, video surveillance monitoring, environmental sensors, paging, and radio communication systems.

These investments could be even more valuable if they operated together rather than in isolation. "Currently, operations personnel use separate systems to monitor each type of sensor, making it difficult to 'connect the dots,'" says Chris Shenefiel, Federal Government Industry Solutions Manager, Cisco. "If you can't bring all your detection sources onto the same network, how can you accurately assess the threat, let alone respond swiftly and appropriately?"

First, Integrate All Sensor Input

Now governments are improving the value of their physical security systems by connecting them to a common platform. The return on investment increases incrementally as government integrates its sensors, building controls, and communications systems.

The first step is connecting sensors to the IP network so that they can be securely monitored from any location. As an example, a citizen who lives near a chemical plant smells an odor in the backyard and calls the public safety answering point (PSAP). Today, lacking any additional information about the nature and extent of the odor, the operator might dispatch several first-responder organizations that arrive only to find a simple natural-gas leak that one person could have fixed. Worse, the operator might dispatch a single officer who arrives to discover a major chemical leak that threatens the entire neighborhood.

What if the operator in the PSAP could also reach out over the IP network to check the chemical sensors deployed throughout in the neighborhood? "With this additional information, operators can make an informed decision to dispatch the fire department plus the hazmat team or just public works," Shenefiel says.

Add Building Access Controls and Communications Systems

Physical security capabilities multiply again when the building access controls and communications systems are added to the common platform. Suppose a disgruntled citizen breaks into a government building, intending to contaminate the offices. Today, the access control system reports a break-in, a motion sensor reports movement in the ventilation area, and a chemical sensor reports high levels. But the events are likely reported on different management systems. "The problem is that a human has to correlate the events, which can delay situational awareness and an appropriate response," says John Speicher, Federal Government Industry Solutions Manager, Cisco.

When different sensor inputs are available on the same management console, security personnel gain a complete operating picture, improving situational awareness. And when building access controls are also connected to the IP network, authorized personnel can take immediate action from any location, such as controlling the ventilation system to safely disperse the chemical, locking down certain areas to contain the intruder, and notifying the appropriate response team. One click can activate one of multiple predefined notification policies, based on time of day and the nature of the event. Examples are starting a radio talk group or sending short message service (SMS) text messages to smartphones.

Implement Policy-Based Response

Finally, a common operating platform for safety and security enables automated, policy-based response to detected events. "If video analytics software detects a person in a restricted area, an unattended package, or some other condition, the system can notify a security guard on a smartphone or laptop and even send streaming video," Speicher says. This capability can reduce or even eliminate the need to assign security personnel to monitor a bank of video surveillance monitors, and also eliminate missed events due to information overload.

Cisco Open Platform for Safety and Security

The Cisco® Open Platform for Safety and Security integrates standards-based solutions from Cisco and its partners, helping organizations minimize risk and protect people, assets, and government continuity. The value of the platform grows as the agency adds more and different sensors and analytics software.

To read more about the Cisco Open Platform for Safety and Security, visit:

www.cisco.com/web/strategy/government/national-open-platform.html

To see a demonstration, contact your Cisco account manager.

To read a case study on Westgate City Center in Glendale, Arizona, visit:

www.cisco.com/web/strategy/docs/gov/AdvancedPhysicalSecurityWestgate093008.pdf




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)