



**Alexandru Zamfir**

Executive Director

**Cisco Expo 2010**

17 – mar - 2010

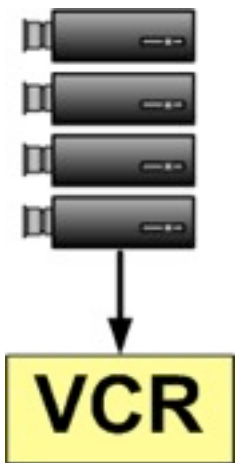
<http://www.probitas.ro/wolf>



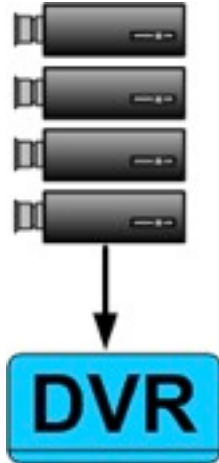
IP VIDEO SURVEILLANCE

# Video Surveillance Evolution

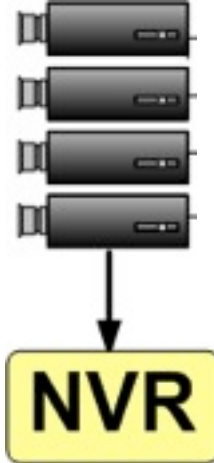
Analog Cameras



Analog Cameras



Analog Cameras



## VCR & Analog

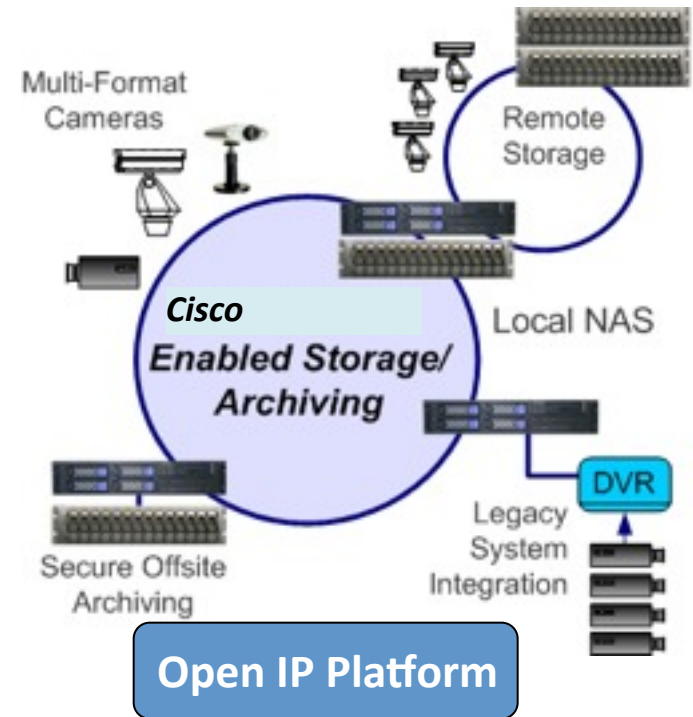
- Standalone box
- Poor image
- Hard to search
- No remote access

## DVR

- Easier to search
- Consistent Quality

## NVR

- DVR benefits
- More storage options
- Limited network connection



## Cisco Video Surveillance Platform

- Secure viewing from anywhere
- Fail-safe redundant storage
- Easy integration with other systems
- Enterprise class storage and support

# Multi-Services Platforms

## MSP-1RU



- 1RU Rack Mount Chassis – 17.2" x 19.8"
- Intel Xeon Processor
- On-board Hardware Diagnostics
- 300W Power Supply
- 4 Hot-swap 3.5" SATA Drive Bays
- 750 or 1TB SATA Drives (No RAID)
- 1 Full-size PCI-x/e Card Support
  - (1) 16-port Exacq Card (short term); OR
  - (1) 16/8 Port Wanaka Card (future)*

## MSP-2RU



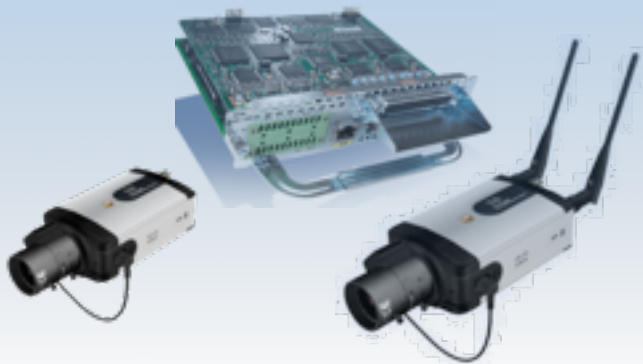
- 2RU Rack Mount Chassis – 17.2" x 25.6"
- Intel/AMD Based Quad-Core Processor Support
- Motherboard can support two Dual Xeon Processors (2nd processor may be a future option)
- On-board Hardware Diagnostics
- Supports up to two 900W Modular Optional Redundant Power Supplies
- 12 Hot-swap 3.5" SATA Drive Bays
- 750 or 1TB SATA Drives (RAID 0/1/5)
- (3) Hot-swappable Fans
- 100% Cooling Redundancy
- FiberChannel Option Supporting Connectivity to External Storage Arrays
- PCI Card Support
  - (1) RAID Card – Included in all configurations
  - No support for Exacq encoder cards
  - Up to (2) 16/8 Port Wanaka Cards (future)*

## MSP-4RU



- 4RU Rack Mount Chassis – 17.2" x 25.6"
- Intel/AMD Based Quad-Core Processor Support
- Motherboard can support two Dual Xeon Processors (2nd processor may be a future option)
- On-board Hardware Diagnostics
- Supports up to three 900W Modular Optional Redundant Power Supplies
- 24 Hot-swap 3.5" SATA Drive Bays
- 750 or 1TB SATA Drives (RAID 0/1/5)
- (5) Hot-swappable Fans
- 100% Cooling Redundancy
- FiberChannel Option Supporting Connectivity to External Storage Arrays
- Up to (4) 4-port Flagstaff Video Cards (USB)
- Full-sized PCI Card Support
  - (1) RAID Card – Included in all configurations
  - Up to (2) 16-port Exacq encoder cards
  - Up to (3) 16/8 Port Wanaka Video Cards (future)*

# “Router – Integrated” IP Video Surveillance and Video Recording



Integrated Analog Video Gateway  
Hybrid Analog and IP Cameras  
Integrated Video Management and Storage System



## Cisco Integrated Services Routers

- **Analog Video Gateway: IPVS-16A**
  - Analog video interface for IP Video Surveillance
  - 16 Analog Video Ports: MJPEG, MPEG-4
  - 8 Contact Closure Ports
  - 2 RS-485 ports for device Pan/Tilt/Zoom control
- **Integrated Video Management and Storage System: VMSS**
  - Targeted at <32 stream (camera) deployments
  - Utilizes pre-packaged VS Operation Manager and VS Media Server
  - Manage, view and archive surveillance data for up to 32 devices simultaneously
  - Unified interface into IP Cameras and Analog devices (through the AVG)



# Software Components:

## Video Surveillance Media Server (VSMS)

- Video Surveillance Media Server is the core component in the Media Platform, enabling distribution, archiving and management of video feeds.
  - Make video an information resource
    - Proxy and stream live feeds
    - Store and stream recorded media
  - Infinitely customizable
    - Add custom UIs
    - Use best-of-breed codec: Motion JPEG, MPEG-2, MPEG-4
    - Highly Scalable – Cameras, Clients, Storage
    - Share IT Infrastructure intelligently – Storage Systems and Bandwidth
  - Open and distributed
    - Integrate with other systems
    - Expand system as needed
    - Harden System as needed (fail-over and redundancy)

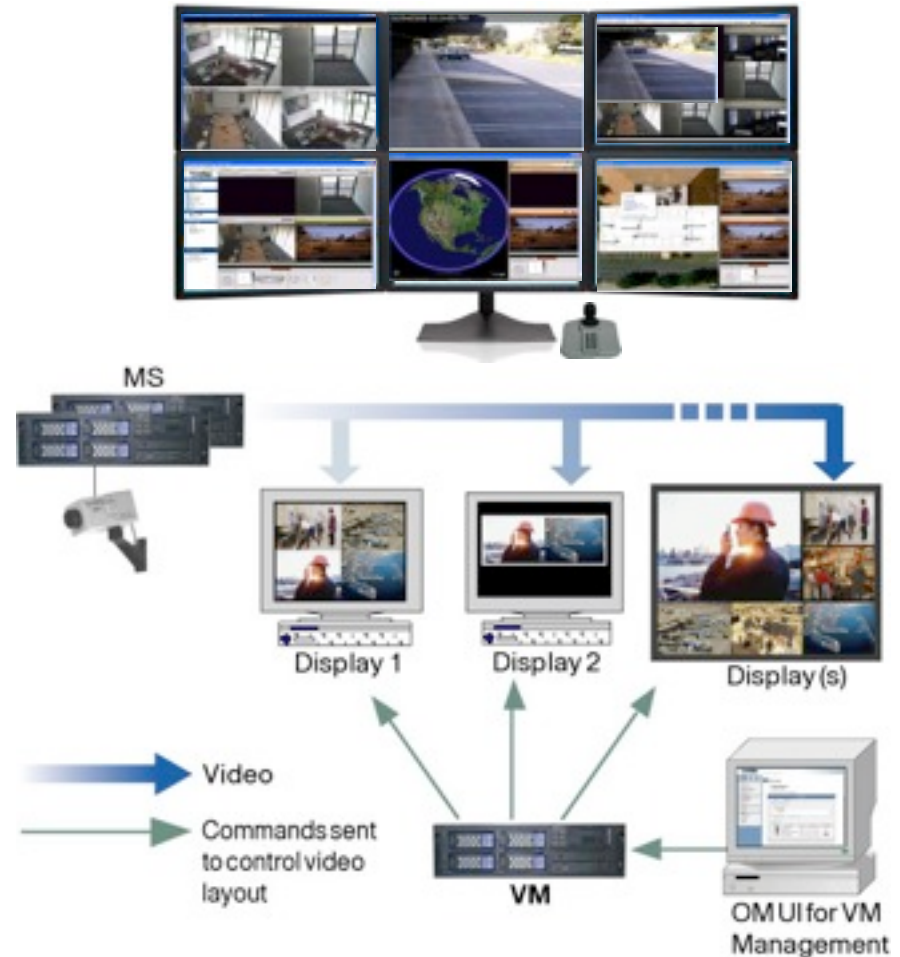
# Video Surveillance Operations Manager (VSOM)

- Enterprise solution
- Highly configurable to effectively manage complex video applications
- 100% browser-based UI
- Multiple web-based consoles to configure, manage, display, and control video throughout a customer's IP network.
- Unlimited cameras, storage, viewers



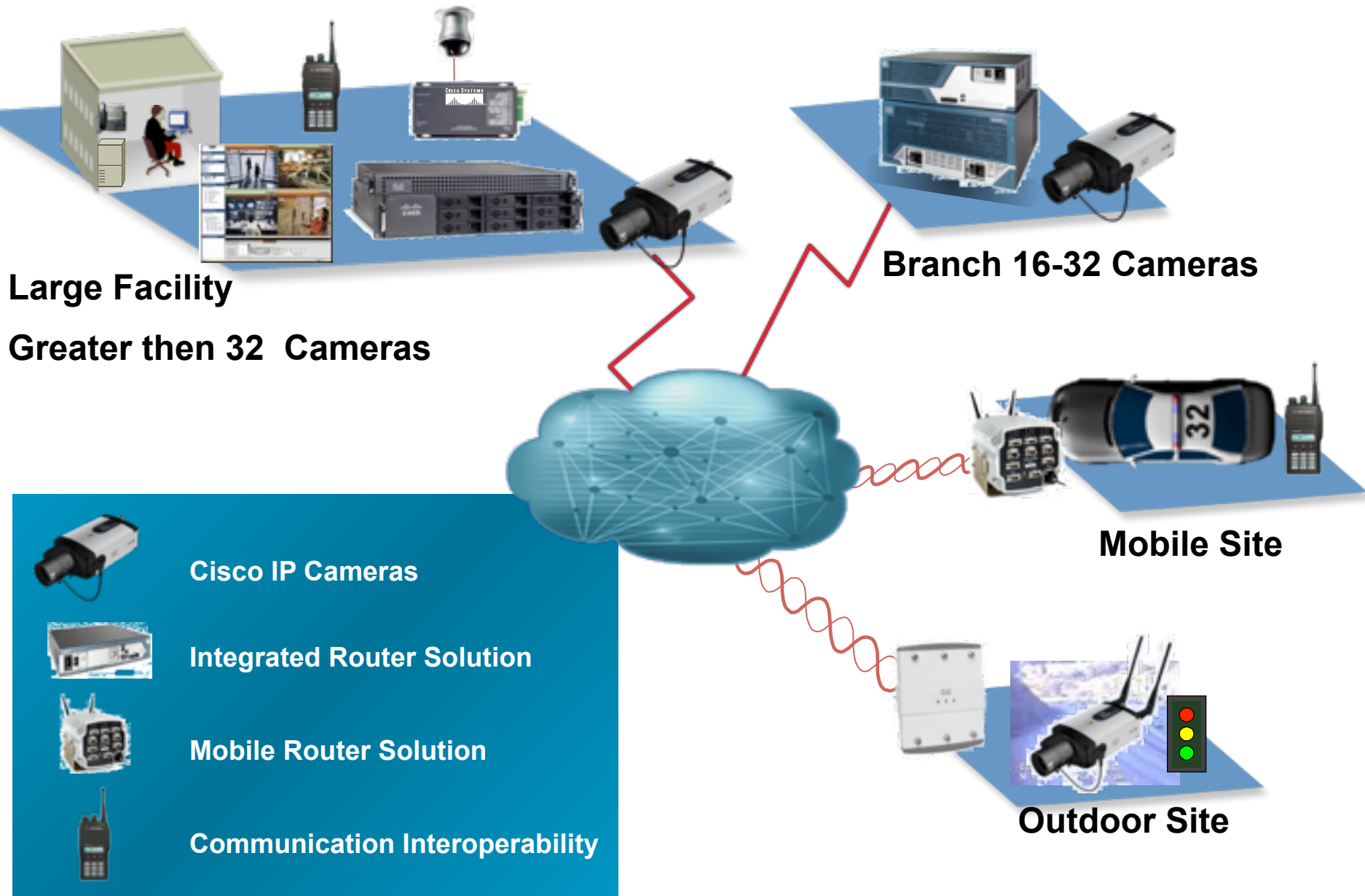
# Video Surveillance Virtual Matrix (VM)

- Controls an infinite number of video displays on network
- Easily integrates with other systems
- Flexible delivery of live & archived video
- Distributes to Video Wall
- Controls multiple video displays from a single station
- Event/Action
  - Push video to remote screens





# Cisco Networked Video Surveillance Solutions



# Cisco IP Video Surveillance Cameras 2500 Series

## Fixed Cameras

- CIVS-IPC-2500
- Fixed Wired Camera



- CIVS-IPC-2500W
- Fixed Wireless Camera



- CIVS-IPC-VF38
  - ✓ Fujinon 3 - 8 mm
- ✓ CIVS-IPC-VT38
  - ✓ Tamron 3 – 8 mm
- CIVS-IPC-VF31 @
  - ✓ Fujinon 3 - 11 mm
- CIVS-IPC-VT31
  - ✓ Tamron 3 – 11 mm
- CIVS-IPC-VF55
  - ✓ Fujinon 5 – 50 mm
- CIVS-IPC-VT55
  - ✓ Tamron 5 – 50 mm

# Cisco Video Surveillance IP Camera Fixed Domes

- Same core Cisco IP Camera as the Standard Definition (SD) wired version
- Fixed Dome Form Factor
- Power Over Ethernet (Indoor)
- Multiple Flavors
  - Indoor Flush Mount, Surface Mount
  - Indoor Vandal Resistant
  - Outdoor Vandal Resistant
- API for interfacing with third party vendors
- Integration with VSM and Stream Manager
- Available Q2 CY09



# Introducing Cisco IP Video Surveillance Cameras

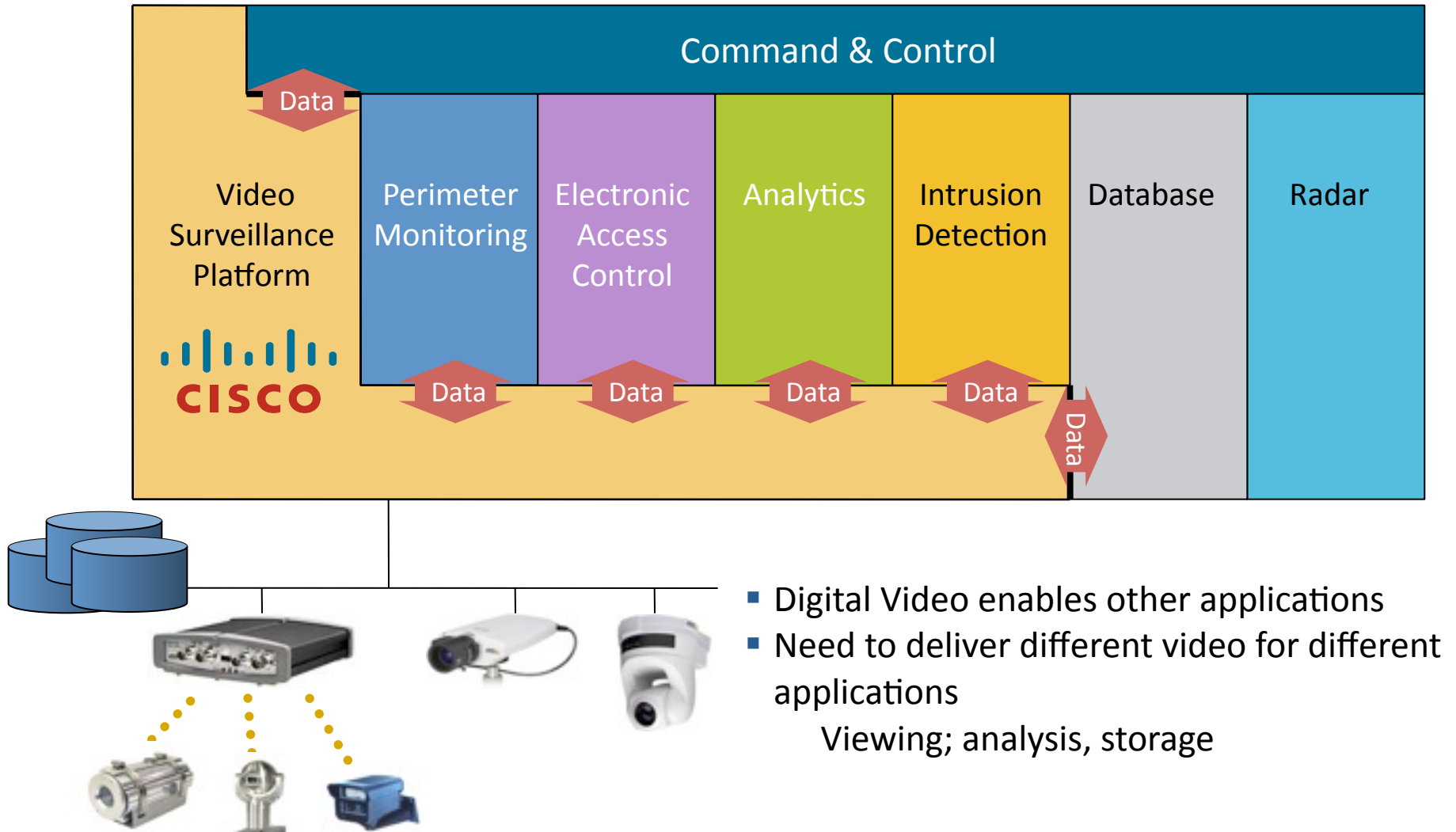
## 4500 High Definition Cameras

- True HD Video Surveillance Camera
- Outstanding Image Quality
- No other HD VS camera on the market
- 1080p (1920 x 1080) 30 FPS
- 720p (1280 x 720) 60 FPS
- H.264, MJPEG Compression
- Dedicated Digital Signal Processor (DSP) for Video Analytics
- USB Memory Card
- Application Programming Interface (API)
- IPv6



Wired and Wireless (available Q2 CY09)

# Open Architecture “Enables” Integration with Other Applications

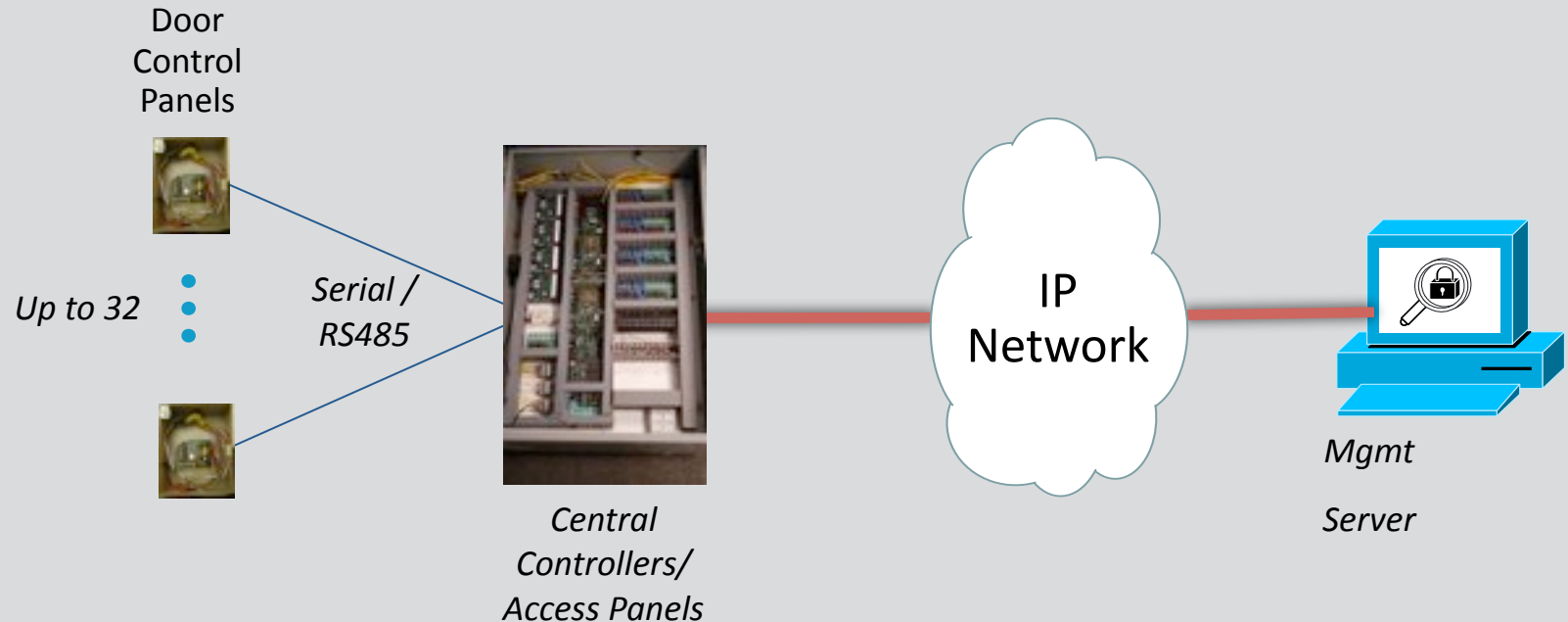




IP ACCESS CONTROL

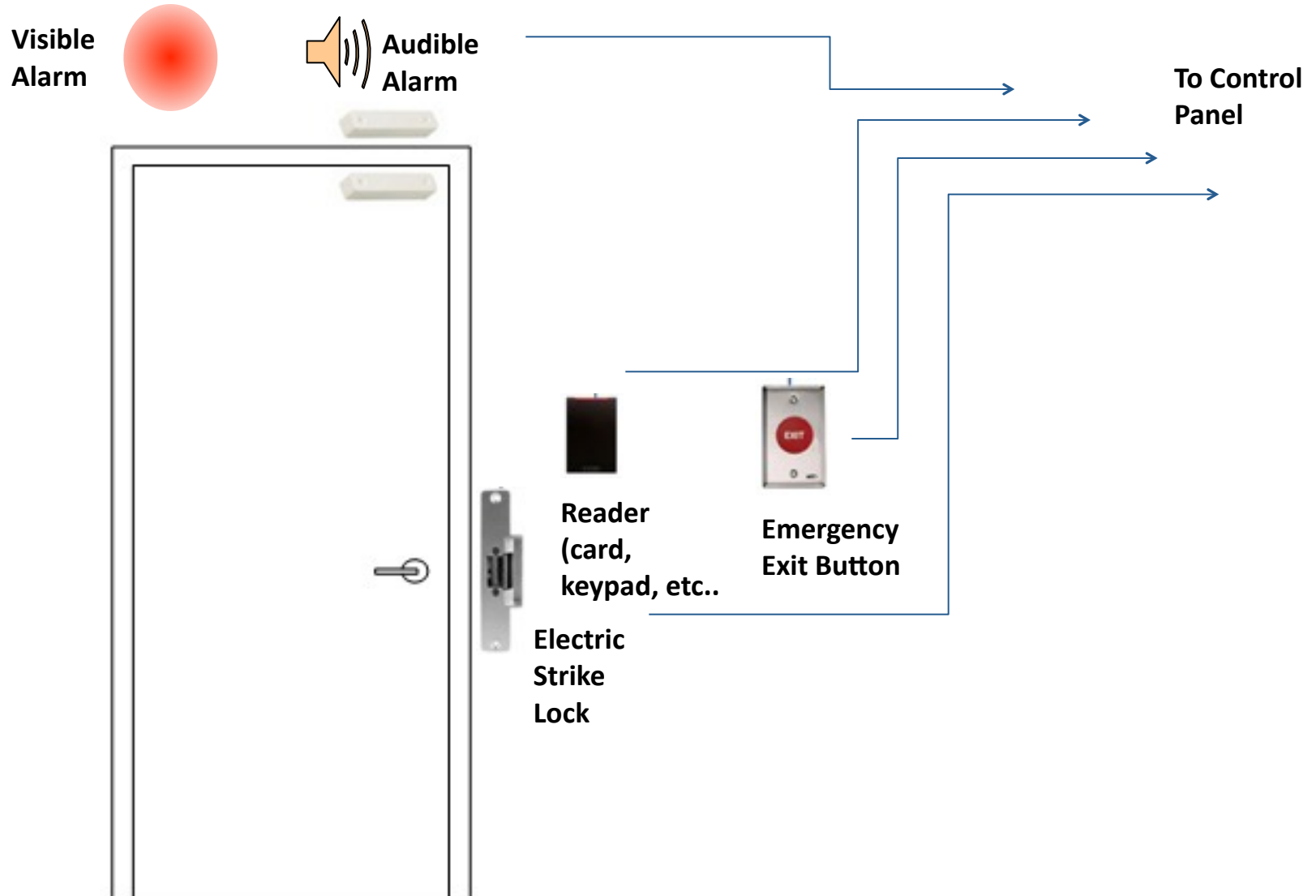


# Electronic Access Control architectures today....



- Complex & expensive to design, deploy and maintain
- Not capable of incremental deployment : Upfront design cycle required
- Separate power circuit required to power door hardware

# A Typical Door..



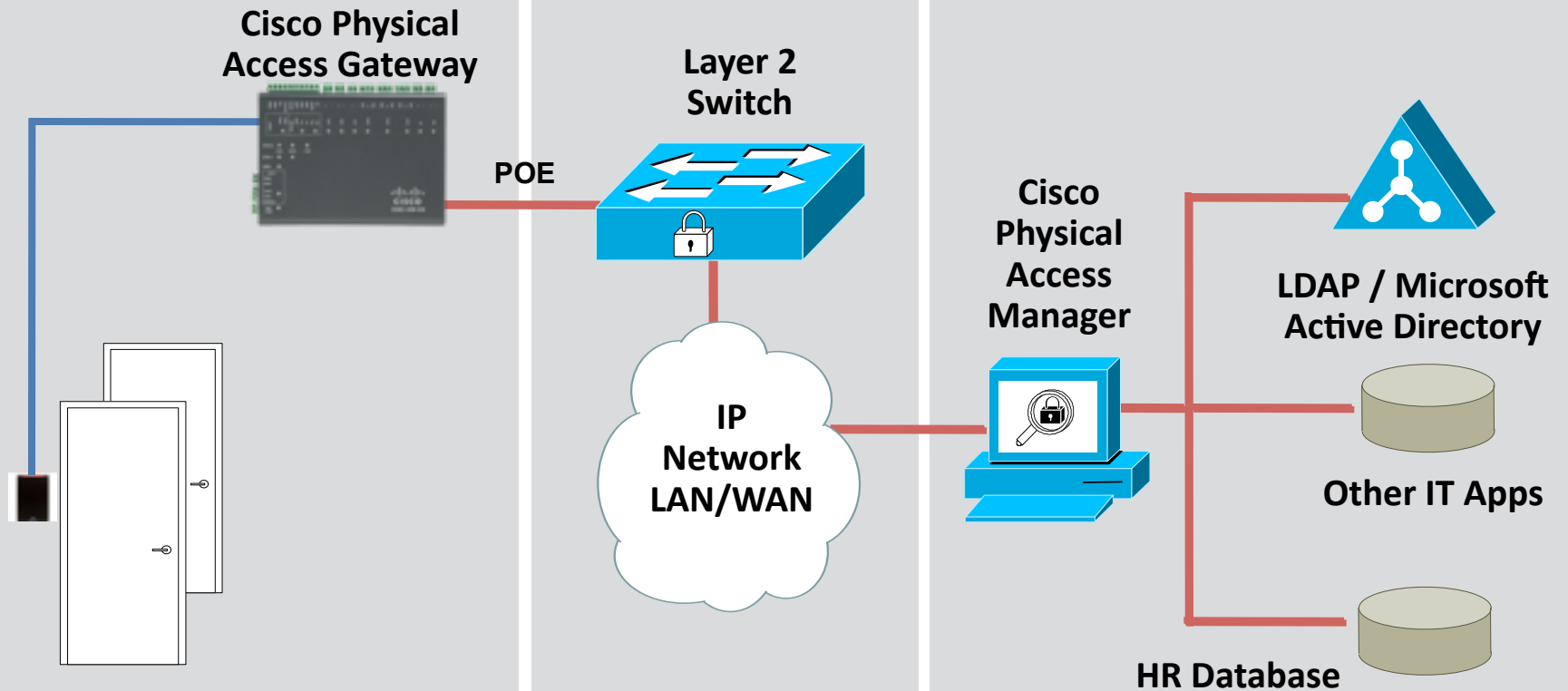
# Cisco Physical Access Control Overview

- ***A Comprehensive Solution*** for Electronic Access Control
- Leverages IP infrastructure
- Integrates with other Physical Security applications



- Hardware:
  - Cisco Access Gateway connects existing door hardware (readers, locks etc.) to the network
  - Additional doors can be managed by connecting expansion modules to the Access Gateway
- Software
  - Cisco Physical Access Manager (Cisco PAM) is a Management Appliance for configuration, monitoring and report generation.

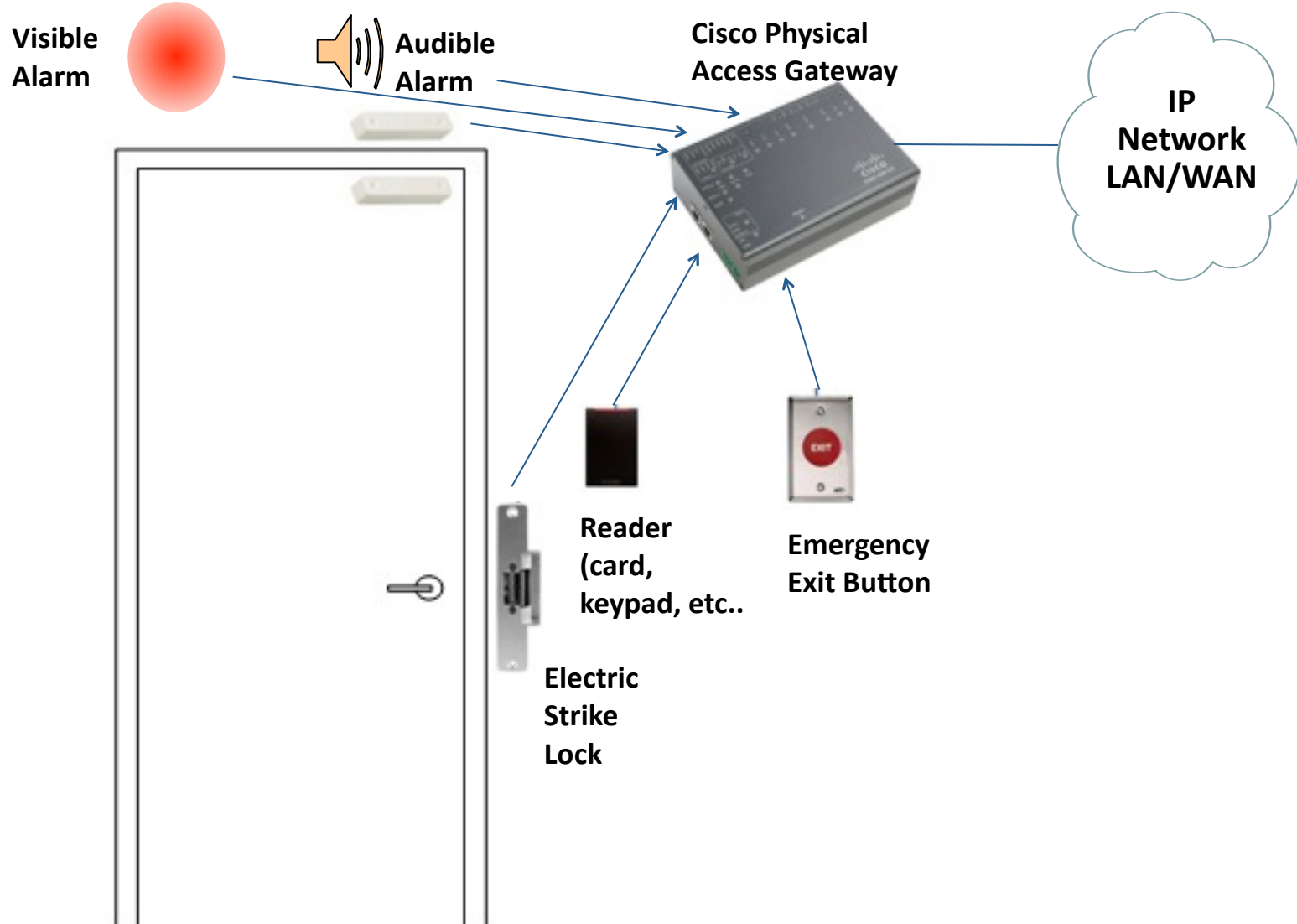
# Deployment Architecture



Scalable Modular Architecture, easily integrated with IT application data

# A Typical Door..

*With Cisco Physical Access Control*



# Hardware Overview

## Cisco Physical Access Gateway



## Reader Module



## Input Module



## Output Module



- Mandatory component. Connects up to 2 doors, and up to 15 additional modules (connected via a 3 wire CAN bus).
- Power: POE or 12V – 24V DC
- 2 Ethernet ports
- 10 pin Weigand Reader port : can be configured as two 5 pin Weigand ports
- 1 RS-485 port
- 3 Outputs (Form C Relays)
- 3 Supervised inputs
- Tamper & PF inputs (can be configured as additional inputs)

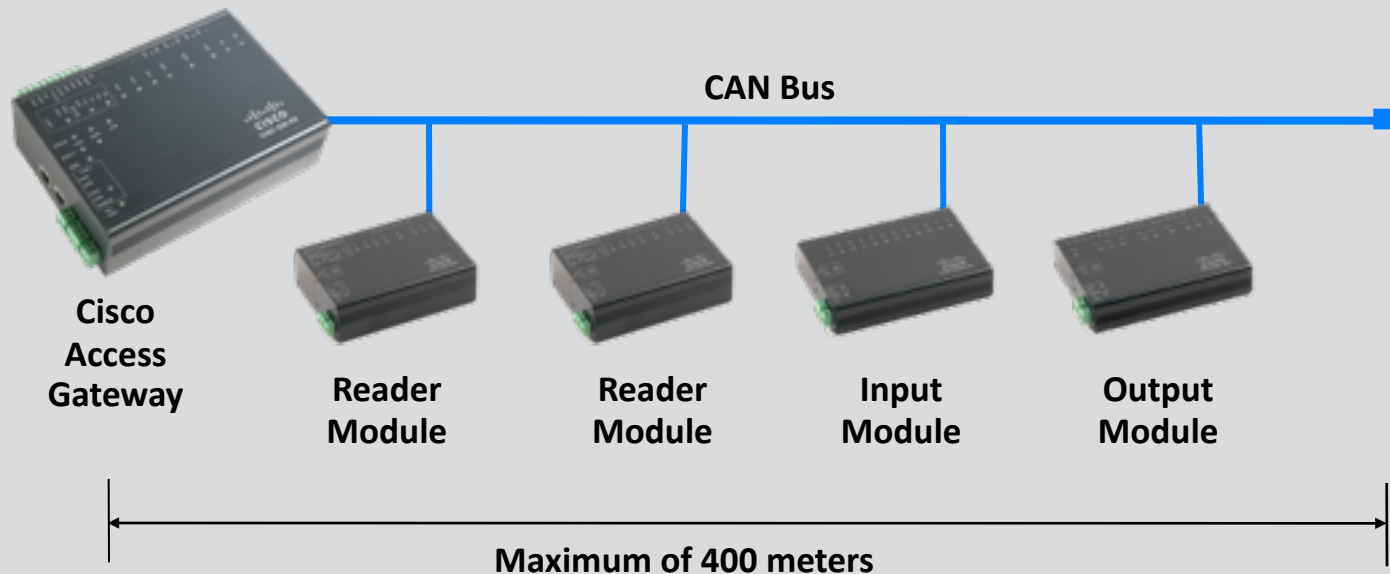
- Requires Access Gateway
- Connects up to 2 doors, to the Cisco Access Gateway via CAN bus.
- Power: 12V – 24V DC
- 10 pin Weigand port : can be configured as two 5 pin Weigand ports
- 1 RS-485 port
- 3 Outputs (Form C Relays)
- 3 Supervised inputs
- Tamper & PF inputs (can be configured to be used as additional inputs)
- CAN Termination switch

- Requires Access Gateway
- Connects up to 10 inputs to the Cisco Access Gateway via a CAN bus.
- Example inputs are: Pushbutton switches, Glass Break sensors, or any contact closure input. circuit
- Power: 12V to 24V DC
- 10 Supervised inputs
- Tamper & PF inputs (can be configured to be used as additional inputs)
- CAN Termination switch

- Requires Access Gateway
- Connects up to 8 outputs to the Cisco Access Gateway via CAN bus..
- Example outputs are: lights, LEDs, or any contact closure output circuit.
- Power: 12V to 24V DC
- 8 Form C (5A, 30V) outputs
- Tamper & PF inputs (can be configured to be used as additional inputs)
- CAN Termination switch



# Expansion Modules



The Cisco Access Gateway is always required, and can control up to 2 doors by itself.

Any combination of additional modules (up to 15) can be connected to the Access Gateway via a 3 Wire Controller Area Network (CAN) Bus.

Additional modules can be a maximum of 1320 Feet from the access gateway.

Modules may be added or removed at run time without affecting operation of the other modules.

# Why Cisco Physical Access Control?

- Leverage your IP infrastructure
  - Use network services (DHCP, NTP etc.) to ease deployment.
  - Use PoE to lower deployment costs.
  - New services possible with the integration of Physical Access with other applications such as IPICS, VSM, IP Phones and Network Security.
- Lower deployment costs and TCO
  - Distributed architecture lowers deployment and operational costs.
  - Pre-provisioning to simplify deployment and configuration
  - No scheduled maintenance required for the hardware

# Cisco Physical Access Manager (Cisco PAM)

1 RU Appliance

Java Thin Client Architecture

Policy Support: Two-Door, Anti-Passback

Report Generator (Canned & Custom)

Badge Design & Enrollment

Microsoft Active Directory integration

Fine grained user rights

Global I/O

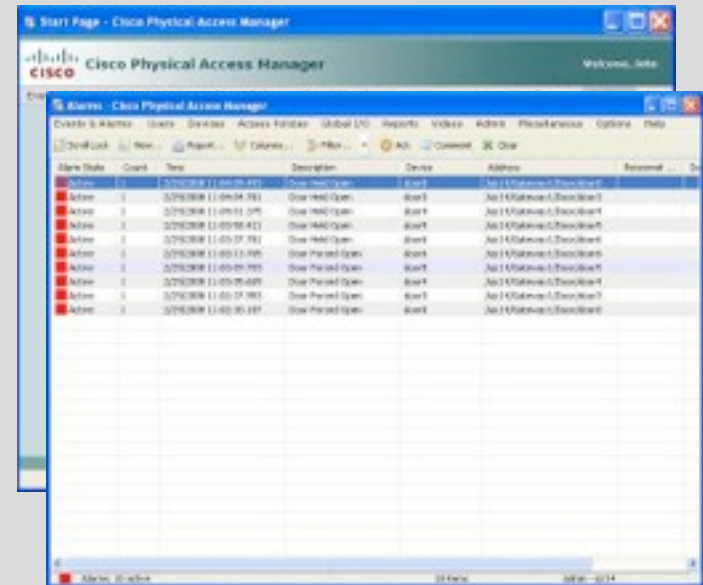
Device Pre-Provisioning

Capacity & Feature Licenses

IT Data integration

Warm Standby High Availability

Audit Trails



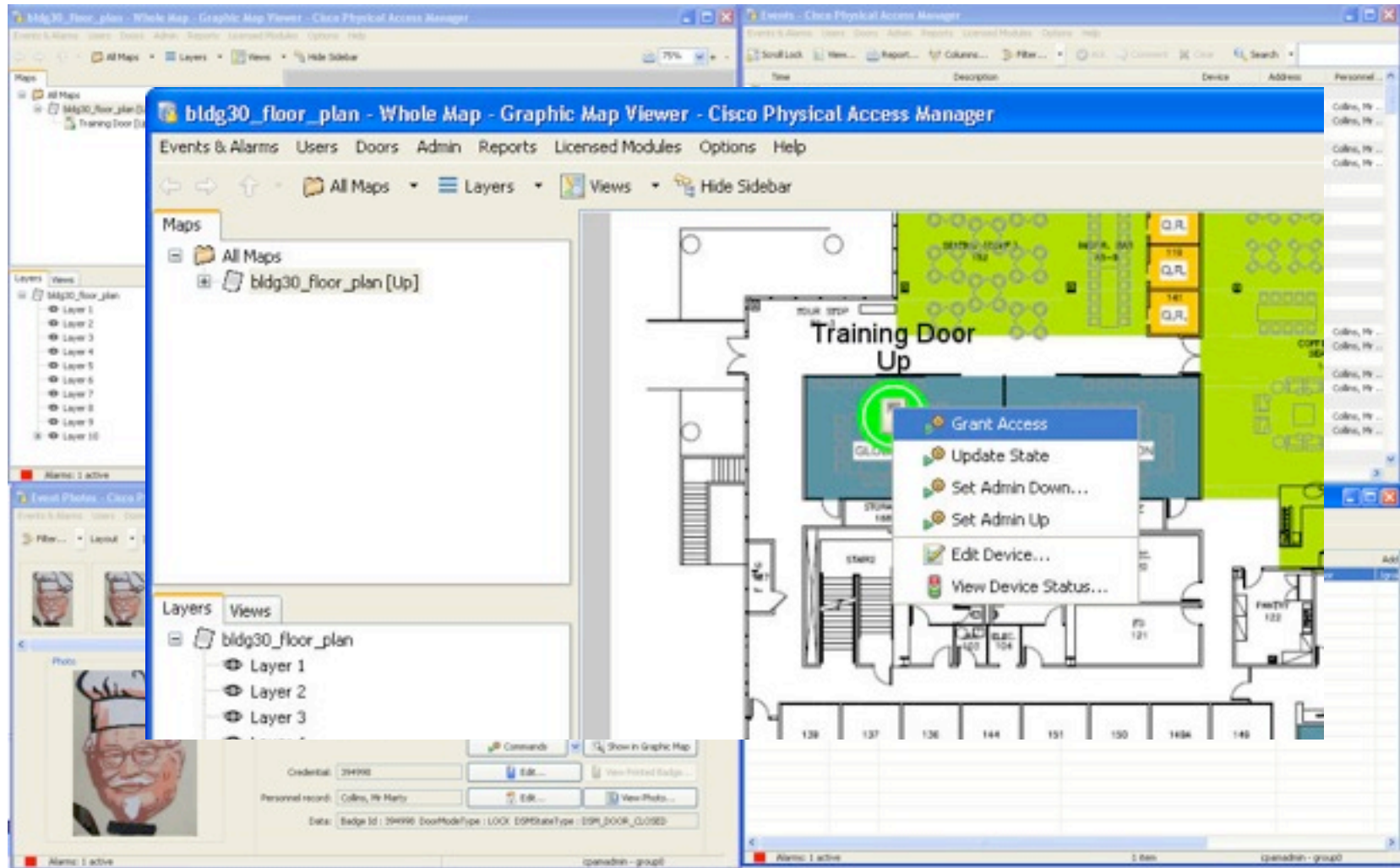
**Cisco PAM**



**Java Thin  
Clients**



# Web Enabled GUI



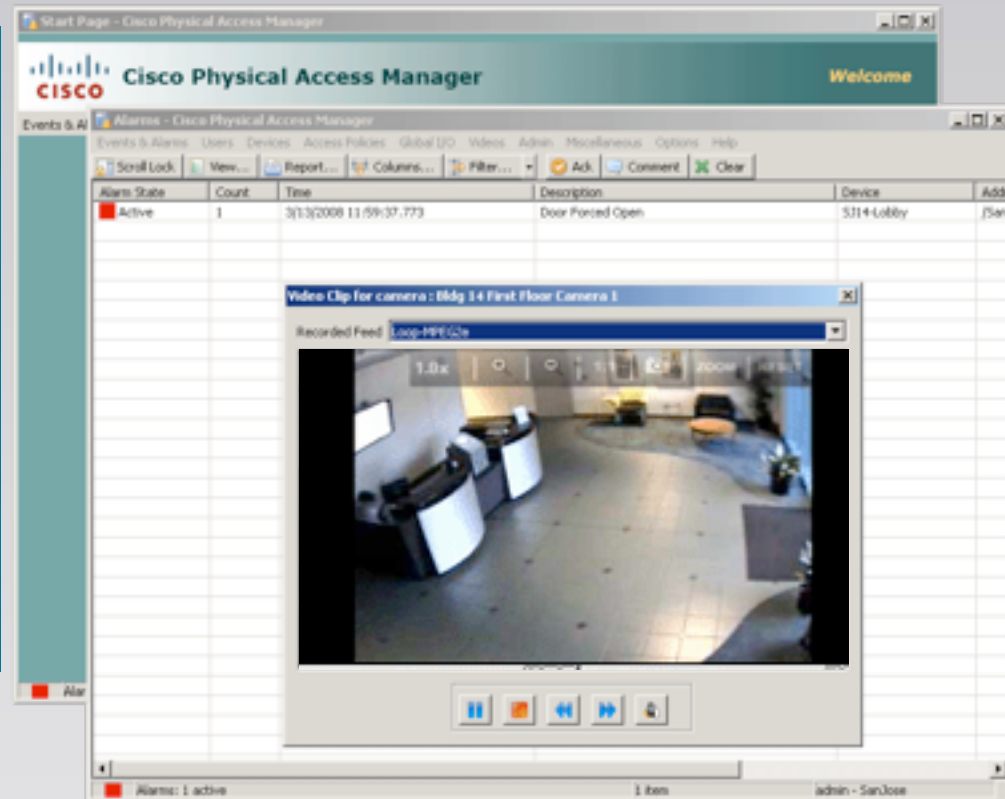
# Cisco Video Surveillance Manager (VSM) integration

Event Video integration with Cisco VSM

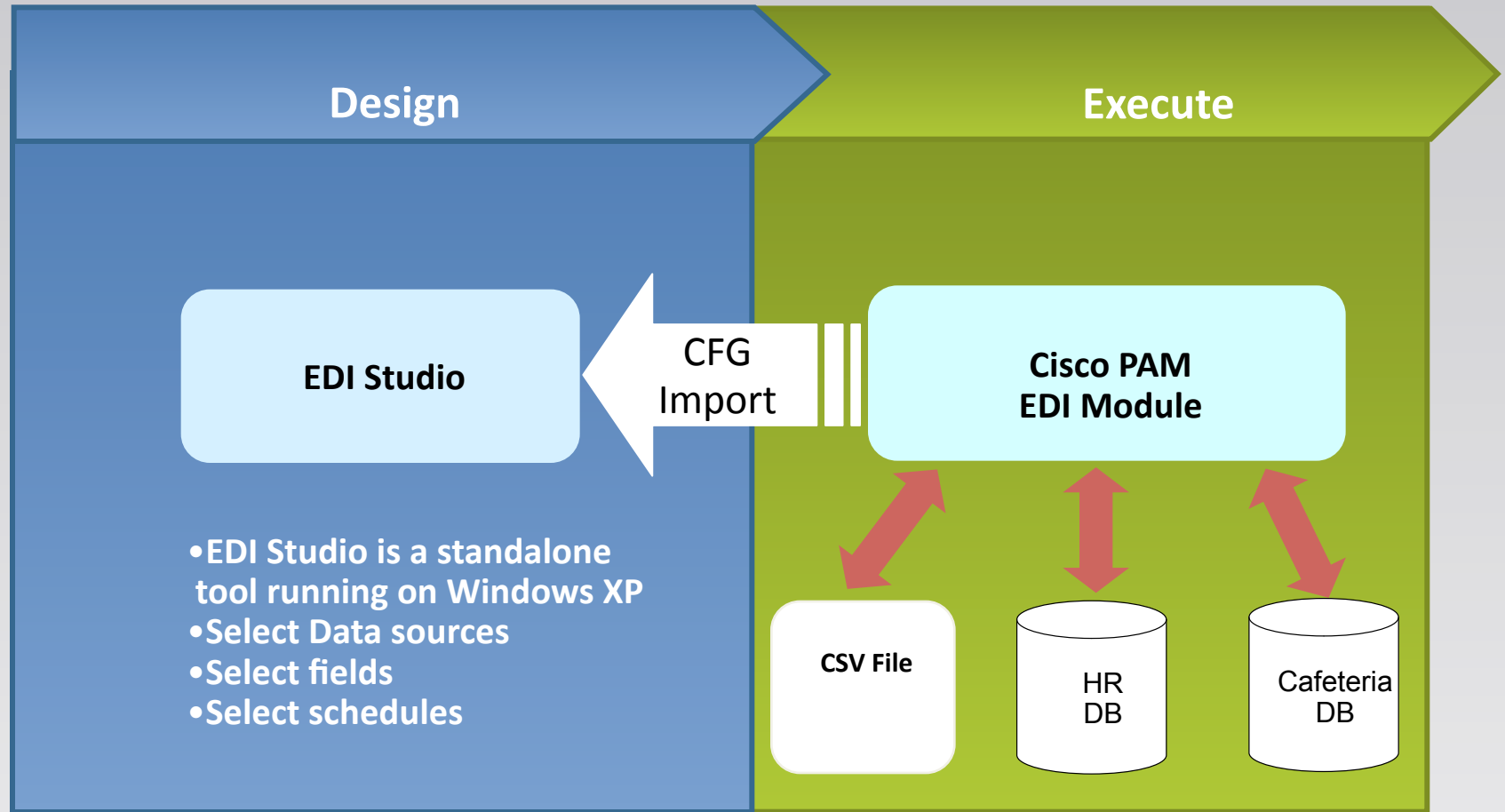
Dynamically acquires camera inventory stored in Cisco VSM. Automatically tracks inventory.

Allows association of cameras to doors.

For every event by the door, recorded and live video can be viewed, PTZ presets can be changed.



# Cisco PAM : Enterprise Data Integration (EDI) Module



**Integrates Cisco PAM data with other databases/IT applications**



# VIDEO ANALYTICS



**CORPORATE OFFICE/  
DATA CENTER**

Alert integration with central monitoring function (data/communications link between branch and office building)

**VAULT/CASH ROOM**

Tailgating into secure area without valid access control event

**BRANCH OPERATIONS**

Queue length in line and drive-thru

**ATM**

Loitering at ATM for extended periods with no transaction started

**OTHER SCENARIOS****1 ATM**

New person enters AOI after transaction has started

**2 External branch security**

Groups of people in parking lot after hours

**3 Teller**

Customer presence verification during teller transaction/open cash drawer

**4 Drive-Thru teller**

Teller signal when vehicle has approached and stopped at drive-thru teller

# Video Analytics: BANKING

ASSET SECURITY/ MONITORING	ATM MONITORING	EXTERNAL PHYSICAL SECURITY	BANK OPERATIONS IMPROVEMENT
Bank vaults and security deposit boxes present special security requirements for monitoring access and protecting the bank customers' valuable assets.	Non-secure ATMs indirectly drive away customers and cause revenue loss. Remote and automated surveillance is essential for the safety and security of customers.	Instead of using CCTV only to conduct investigations after an incident, analytics system provides real-time alerting of activities of interest before an incident occurs.	Existing bank surveillance cameras can provide important operational data, such as queue lengths, measuring peak traffic, and customer wait times.
<p>Identify entry to secure areas or tailgating without valid system verification (via access control integration)</p> <p>People counting/occupancy capabilities for bank vault</p> <p>After-hours human presence detection</p> <p>Object left behind or taken</p> <p>Vandalism/graffiti</p> <p>Cameras blocked/moved during possible robbery</p>	<p>People sleeping or loitering in ATM vestibules</p> <p>ATM (skimmer) insertion</p> <p>People loitering in the proximity of an ATM</p> <p>Person loitering at the ATM with no transaction started (w/ATM integration)</p> <p>Vandalism/graffiti</p> <p>Camera tampering</p>	<p>People approaching bank/building at night</p> <p>Vandalism</p> <p>People loitering in or near bank branch</p> <p>Vehicles loitering around facility perimeter</p> <p>Camera tampering</p>	<p>People counting/traffic throughout the day</p> <p>Queue length, branch traffic, and wait time monitoring</p> <p>Moved camera by teller (camera tampering)</p>

# Maximum Value through **INTEGRATION**

**Bankers** use Video Analytics to detect events for ATM loitering, people counting, data center security, and more. **Intelligent video analytics**, however, is just one layer within an overall banking video surveillance system. But integrate that video analytic output with bank systems and data streams and you create the next generation of **intelligent enterprise solutions** for branch safety and financial risk mitigation

Some solutions for **Banking** that leverage analytic integration for maximum value include:

- ✓ ATM transaction applications to detect human presence with no transaction started (skimmer insertion), or suspicious human behavior after a transaction has started
- ✓ Bank teller systems to visually verify customer presence for certain withdrawal transactions
- ✓ Access control systems to detect “tailgating” or other unauthorized entry into secure areas within a bank, data center, or corporate office
- ✓ Annunciator or alarm system to alert employees of vehicles in drive-through lanes
- ✓ Video management and storage systems to enable alert-driven video delivery, storage and central monitoring



# ANALYTICS: RETAIL

## PARKING LOT

Speeding, loitering in fire lanes, vehicle counting

## LOADING DOCKS AND FIRE EXITS

Left objects and general perimeter security

## POINT-OF-SALE

Fraudulent transactions with POS data integration

## STORE FRONT

People counting; people approaching after hours

For more information, ask about OV: Retail for POS applications

## OTHER SCENARIOS

### ① Aisles and Displays

Left objects in aisles; traffic flow around displays

### ② Returns Line

Entering returns line from within the store

### ③ Merchandise Counters

Crowding or unauthorized access behind counter

# Video Analytics: RETAIL

LOSS PREVENTION	PHYSICAL SECURITY	PUBLIC SAFETY AND LIABILITY	BUSINESS INTELLIGENCE
Video Analytics can be used to watch out for a wide variety of behaviors indicative of customer or employee theft	A retail operation may include a store and warehouse, which requires constant video surveillance to protect inventory and other assets	Public safety is an issue that is top of mind for retailers; including dark parking lots, customers slipping/falling in store aisles:	<b>Event counting</b> generates valuable business data for merchandising and other operational functions
Left packages outside the back exit	General perimeter protection (after hours)	Vehicles speeding through parking lots	High value or promotional item monitoring
Extended loitering within store	Loitering anywhere	Stopped vehicles in fire lanes	Display/shelf space effectiveness (comparison of normal traffic patterns to people who stop in front of a particular product or display)
Person running out of store/sudden exit	Unauthorized entrance through fire doors	Gangs or groups of people forming and/or loitering	People counting (in and out of store; into promotional areas)
Stockroom/warehouse inventory monitoring	Loading dock security	Spills/items left behind in store aisles	Forensics analysis of data to determine trends and patterns of customer behavior
High theft item monitoring	Vandalism	Objects blocking fire exits	
Objects removed from shipping/receiving areas	Vault access (via access control system integration)		
Unauthorized access to counter/display areas	Camera tampering		
	After hours people detection		



# Maximum Value through **INTEGRATION**

**Retailers** use Video Analytics to detect events for security, people counting, left or stolen objects and more. Intelligent video analytics, however, is just one layer within an overall retail video surveillance system. But integrate that video analytic output with in-store systems and data streams and you create the next generation of *intelligent enterprise solutions* for loss prevention and operational business efficiency.

Some solutions for **Retail** that can leverage analytic integration for maximum value include:

- ✓ Retail point-of-sale applications to identify employee shrinkage by visually verifying customer presence during refunds, or verifying manager presence during certain transactions that require manager override
- ✓ Product sales data to compare to human traffic patterns and calculate product conversion rates
- ✓ Access control systems to detect “tailgating” or other unauthorized entry into secure areas within a store, warehouse, office/vault room, etc.
- ✓ Video management and storage systems to enable alert-driven video delivery, storage and central monitoring



**Thank you!**

