The bridge to possible

Industrial Physical Perimeter Security Solution Brief

April 2024

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at https://www.cisco.com/site/us/en/about/contact-cisco/index.html.

Contents

Secure Your Industrial Perimeter using Cisco Meraki and Industrial IoT

Introduction

The perimeter is the point of demarcation between what is inside a zone, and what is outside. It is often the first line of defense against unauthorized access. Physical perimeter security is that part of a physical security solution that concerns the perimeter of a facility. The industrial sector, particularly those being considered as national critical infrastructure, considers physical perimeter security as an imperative measure in their physical security implementation due to regulatory compliance requirements, the nature of its operation, and the protection of high-value assets. Here are some related standards and their applications to some of the industrial verticals:

- ISO 27002:2022, Control 7.1 Physical Security Perimeters. Control 7.1 in the new ISO 27002:2022 explains the need for organizations to define and set security perimeters and use these parameters to protect areas that contain information and other associated assets. This standard defines the physical perimeter as the physical boundaries of a building or area and controls access to it. It also classifies physical perimeter security as one of the controls in physical security, which provides controls over the entry into facilities and buildings, as well as the movement within them. These controls generally include access control using doors, alarms, fences, and barriers around facilities.
- North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) plan, CIP-014-3. The purpose of this control is to identify and protect transmission stations and transmission substations, and their associated primary control centers. That if these stations and control centers were rendered inoperable or damaged because of a physical attack could result in instability, uncontrolled separation, or cascading within an interconnection.
- Security guidelines for General Aviation Airport Operators and Users. This guidance document was developed jointly by the General Aviation (GA) community and the Transportation Security Administration (TSA). It suggested airport security enhancements around perimeter security to delineate and adequately protect security areas from unauthorized access by using measures such as fencing, walls, electronic boundaries, and other physical and/or natural barriers.

What is Industrial Physical Perimeter Security

Perimeter means outer boundary, and it is often the property line and the first line of defense against unauthorized access. The perimeter is a point of demarcation between what is outside of a zone, and what is inside.

Perimeter Security is a solution that secures the perimeter

Technologies:

- Physical barriers – Fence
- Fence-mounted shock detection cables
- Fence Vibration Sensors
- Infrared
- Radar
- Thermal camera
- Fiber acoustic sensing
- Video analytics
- Combination of Radar, Optical fiber, PTZ camera
- Lidar


Electric Utility


Rail


Water Utility


Smart City


Roadways


Oil & Gas


Ports & Terminal


Factory/Warehouse

Challenges in Industrial Physical Perimeter Security

Industrial sectors like electric grid substations, airports, rail, roadways, ports, terminals, manufacturing facilities, warehouses, oil, and gas lines, and so on, have employed physical perimeter security solutions with various technologies. These technologies include physical fence barriers, fence vibration sensors, fence-mounted shock detection cables, thermal cameras, infrared, radar, fiber acoustic sensing, video analytics, Light Detection and Ranging (LiDAR), or combination of radar, optical fiber, and Pan-Tilt-Zoom (PTZ) cameras. Despite the availability of the technologies, there are some key challenges in implementing physical perimeter security solutions in an industrial environment:

- **Limited coverage:** The industrial sites can be quite large and complex. The area can span several acres or more, and the perimeter of those areas could be miles long. These facilities may consist of multiple buildings, with numerous entry points along the perimeter. It can be source intensive, costly, and difficult to consistently monitor every inch of the perimeter. Blind spots often exist due to structure, terrain, lighting, and other obstacles. Securing large areas requires comprehensive planning and thorough assessment of the existing physical security standard. Traditional physical perimeter security solutions offer limited coverage.
- **Delayed response:** Large industrial sites are normally located in rural areas. This often creates an incorrect assumption by the physical security staff that those facilities have a lower risk of being attacked or breached. Being at remote locations also means less law enforcement to patrol the perimeter and a much slower response to the crime scene. Traditional physical perimeter security solutions suffer delayed response due to the manual processes involved. It could be days or weeks before a physical perimeter security breach is detected.
- **Harsh environments:** Industrial physical perimeter security solutions need to withstand harsh environments. Being deployed at the perimeter of a site or facility, the hardware is generally installed in an outdoor environment. The devices are required to sustain extreme weather conditions in a wider temperature range, resist water and dust, and survive shock and vibration especially when they are deployed near heavy machines and moving assets like railway trackside, terminal ship-to-shore cranes, manufacturing facility, and so on.
- **Lack of network connectivity:** The physical perimeter security solutions that leverage technologies like LiDAR or video surveillance with video analytics require Wide Area Network (WAN) connectivity to bring data back to a control center for monitoring and analysis. Network connectivity is not always available or too costly to build in those rural areas. The physical perimeter security solution requires flexible and secure multi-access WAN technologies.

Benefits

The Cisco industrial physical perimeter security solution delivers converged networking and physical security for industrial environments. This solution helps to unlock more value from the IoT investment when bundling eligible Cisco Industrial Ethernet switches and Cisco Meraki smart cameras.

- **Improve physical perimeter security:** Reduce asset damage and loss with a converged industrial IoT networking and Meraki physical security architecture.
- **Enhance real-time visibility:** Protect people, places, and critical infrastructure easily with Meraki's cloud-managed camera.
- **Increase reliability:** Connect Meraki cameras in any environment, with options for fiber, 4G or 5G cellular, and Cisco Ultra-Reliable Wireless Backhaul for cloud connectivity.

Cisco Industrial Physical Perimeter Security Solution Components

Cisco can help accelerate the modernization of your physical perimeter security and transform your security infrastructure. Employing market-leading Industrial IoT networking and Meraki cloud-managed smart cameras powered by machine learning and computer vision is key. The Cisco industrial physical perimeter security solution is delivered with:

- **Meraki Physical Security Solution:** The Meraki cloud-based physical security solution transforms your safety and physical security best practices with less complexity, fewer manual tasks, and more visibility.
    - Cloud-managed security camera: Intelligent and cloud-managed smart cameras deliver enhanced security and business insights. The smart camera eliminates complex infrastructure by bringing storage and processing to each camera.
    - Cloud-first smart camera video analytics: Using out-of-the-box analytics for people and vehicle detection, securing your industrial perimeter becomes easy, scalable, and cost-effective.
- **Cisco Industrial IoT Networking:** Cisco brings scale and secure end-to-end Industrial IoT network connectivity to empower the security of your industrial perimeter.
    - The Cisco® Catalyst Industrial Ethernet (IE) switching portfolio includes ruggedized, secure, easy-to-use switches built for extending enterprise networks to outdoor and harsh industrial environments. In this solution, Cisco Catalyst IE3200 Rugged Series and Cisco Catalyst IE3300 Rugged Series switches provide power and secure connectivity to the Meraki smart cameras.
    - The Cisco Catalyst industrial routers are a range of ruggedized modular platforms on which you can build a highly secure, reliable, and scalable communications infrastructure. Cisco Catalyst IR1100 Rugged Series routers with a very small form factor, modular, and expandable hardware design deliver dual cellular connectivity as an optional Wide Area Network (WAN) connectivity to this solution.
    - Cisco Ultra-Reliable Wireless Backhaul (Cisco URWB) delivers fiber-like wireless connectivity to extend your network where installing fiber isn't feasible or is too costly. As another optional WAN connectivity, the Cisco IW9165D Heavy Duty Access Point delivers ultra-reliable, high-throughput wireless connectivity, easily deployed with a built-in directional antenna or optional external antennas.

Meraki MV Smart Cameras

The Cisco Meraki MV product line delivers smart cameras for both indoor and outdoor environments. Supplied integration with the cloud-based Meraki Dashboard, these cameras can be deployed and configured in very easy steps. In addition, Meraki smart cameras implement an edge architecture that brings video processing and storage to the camera itself, minimizing the complexity and costly hardware and software required in traditional video surveillance deployments.

In a typical deployment scenario, three cameras are required to cover a point of the perimeter, with one camera each facing left and right direction, then the third camera facing straight ahead. In this solution, three different models are highlighted: the second-generation MV52 and MV72X, and the third-generation camera MV63X. See Table 1 that follows for the product highlights.

Table 1. Cisco Meraki MV Smart Cameras – Product Highlights

Features	MV52	MV72X	MV63X
Lens	Long-range viewing with bullet camera, 12-40mm focal length, f/2.3-16 aperture	Varifocal lens, 3-9mm focal length, f/1.2-2.3 aperture, lens adjustment: tilt: 65°, rotation: +/- 90°, pan: 354°	Fixed lens with mini-dome, 3.3 mm focal length, f/2.0 aperture
Field of View (FoV)	12-37° horizontal, 7-22° vertical	36-112° horizontal, 20-57° vertical, 42-138° diagonal	102° horizontal FoV
Camera Image Sensor	1/1.8" 8.4MP (3840x2160) progressive CMOS Image sensor	1/3" 4MP (2688x1520) progressive CMOS image sensor	1/2.8" 8.41MP (3845x2176) progressive CMOS Image sensor
Nigh vision with IR illumination	50 m (164 ft)	30 m (98 ft)	20 m (66 ft)
Video Recording Resolution	4K (3840x2160) with H.264 Codec encoding, up to 15fps	4MP (2560x1440) with H.264 Smart Codec encoding, up to 24fps	4K (3840x2160) with H.264 Codec encoding, up to 15fps
Audio Recording	N/A	Built-in microphone	Three built-in microphones
Outdoor	IK10+ and IP67	IK10+ and IP67	IK10+ and IP67
Storage	1TB	512GB	1TB
Networking	1 x 10/100/1000BASE-T Ethernet (RJ45) 5.0 GHz 802.11a/n/ac	1 x 10/100/1000BASE-T Ethernet (RJ45 2.4 GHz 802.11b/g/n 5.0 GHz 802.11a/n/ac	1 x 10/100/1000BASE-T Ethernet (RJ45 2.4 GHz 802.11b/g/n 5.0 GHz 802.11a/n/ac
PoE	802.3at PoE	802.3at PoE	802.3at PoE
Temperature	-40°C to 50°C (-40°F to 122°F)	-40°C to 50°C (-40°F to 122°F)	-40°C to 50°C (-40°F to 122°F)
Mounting Options	Wall/Celling, Junction Box, Pole	Wall	Wall, Conduit, Corner, Pole

Meraki MV Analytics – Object Detection

Starting from the second generation, all MV cameras can process the analytics on the camera itself, and then transmit motion metadata to the Meraki cloud by enabling the Motion Search function for a camera. Software on the camera analyzes images multiple times per second and identifies where the objects are located. The camera then tracks the location of these objects over time to understand when they entered, where they went within view, and when they left. The camera rolls up its findings and reports them to the dashboard, where the operator can view the data in a summary form.

Meraki smart cameras use deep learning, a type of machine learning in artificial intelligence research, to drive computer vision object detection. This new capability enables people and vehicle object detection. Cameras can perform real-time object detection, classification, and tracking of people and vehicles to increase safety and provide useful insights into activity. Both object detection and motion metadata are aggregated for analysis on the Meraki Dashboard, under the Analytics tab for each camera.

With APIs enabled on Meraki cameras, the operator can interact with MV object detection analytics to build intelligent business solutions. For instance, by leveraging Representational State Transfer (REST) architecture and Message Queue Telemetry Transport (MQTT) API endpoints from MV Sense API, this solution can provide historical and real-time people and vehicle detection data. When people or vehicles have been detected, operators can invoke Live Link or Snapshot REST API to generate a live Dashboard link or link to a snapshot image of the specified camera. A nearby alarm can be activated when a person or vehicle has been detected. Refer to MV Camera APIs for more information.

Cisco Catalyst Industrial Ethernet Switches

A network switch is required to provide the necessary Power of Ethernet (PoE) power and secure connectivity to the Meraki smart cameras. As deployed at the industrial perimeter, the network switch and cameras are most likely to be installed in an outdoor and unconditioned environment. We recommend the Cisco Catalyst Industrial Ethernet Rugged series switch because of its modular, fanless, and robust industrial design. The MV cameras recommended in this solution are equipped with one RJ45 Gigabit Ethernet port and consume a maximum of 25.5W via 802.3at PoE. To support connectivity to those cameras, Cisco Catalyst IE3200 or Cisco Catalyst IE3300 are recommended in this solution. Both models are built for harsh environments and temperature ranges; fanless and have no moving parts for extended durability; resistant to shock and vibration. Both switches support full Gigabit Ethernet interfaces that provide secure access for Meraki MV cameras and other high-speed applications in the industrial space.

IE3200 series fixed model supports a power budget of up to 240W for PoE/PoE+, shared across 8 ports. The modular IE3300 series supports a power budget of up to 360W to support up to 24x PoE/PoE+ ports or 4x 802.3bt type 4 ports (with 2.5G expansion module) with all GE PoE enabled base. Optionally IE3300 can support up to 480W for the 10G PoE enabled base which is required for connecting to devices like Wi-Fi 6E access points. For deployment of industrial physical perimeter security at an entry point, an IE-3200-8P2S or IE-3300-8P2S is recommended. Both suggested models also support 2x 1GE Small Form-Factor Pluggable (SFP) uplinks which connect to the fiber backbone when it is available.

Cisco Catalyst Industrial Routers and Industrial Wireless

In most deployment scenarios, fiber WAN connectivity is not always available, or it is too costly to build, Cisco industrial physical perimeter security solution offers optional add-on WAN connectivity such as cellular and wireless.

The Cisco Catalyst 1101 Rugged series router is the perfect solution for the cellular WAN option with the most compact and modular design, which makes it an ideal solution for remote asset connectivity across multiple industrial vertical markets. With two LTE modules, the IR1101 enables concurrent connectivity to two cellular networks for WAN redundancy, enhanced data throughputs, load balancing, and differentiated services, making it a highly reliable and high-performance platform. For the location where the 5G service is available, the IR1101 base chassis equipped with a 5G Sub 6Ghz module can provide even higher data speeds.

In rural areas, where cellular coverage is limited, an ultra-reliable wireless backhaul is required to bridge the connectivity between the perimeter monitoring site to the control center where WAN connectivity is available. The Cisco Catalyst IW9165D Heavy Duty Access Point is designed to operate under extreme weather conditions. With its built-in directional antenna design, the Catalyst IW9165D is designed to make wireless backhaul deployment simple. It enables long-range, high-throughput connectivity anywhere fiber is not an option. It can support various fixed wireless infrastructures including point-to-point, point-to-multipoint, and mesh.

Conclusion

The Cisco industrial physical perimeter security solution helps our industrial customers secure their physical perimeters with Cisco Meraki and Cisco Industrial IoT Networking. This solution offers a secure and solid network foundation that not only provides fully-secured access distribution connectivity to the MV smart cameras but also delivers multi-access WAN technology that is flexible for various deployment scenarios. The cutting-edge cloud-managed Meraki MV architecture brings simplicity and data-powered intelligence to accelerate the modernization of the physical security around the industrial perimeter.

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 **https://www.cisco.com/go/offices**.