

# Critical Infrastructure Guide

Protect your business by quickly responding to potential physical breaches

## The Challenges You Face

Protect your critical infrastructure with layers of physical security systems

Critical infrastructure faces the same security threats as other sectors, except that the consequences can be far more serious for millions of people. At its core, physical security is about keeping your facilities, people and assets safe from real-world threats. It includes physical deterrence, detection of intruders, and responding to those threats in real-time.

---

Hostile Attack

---

Unaccounted Visitors

---

Tailgating

---

Document Theft

---

Server/Data Theft

---

Stolen Identification

---

Vandalism

---

Espionage



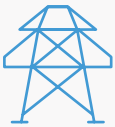
## Impacted Industry Sectors

### Data Centers



Physical security of a data center comprises various kinds of built-in safety and security features to protect the premises and thereby the equipment that stores critical data for multi-tenant applications. Reducing risk in your data center includes prevention, biometric-based access control, intrusion detection and video surveillance which enable you to react to critical events quickly.

### Utilities



There are over 55,000 substations in the U.S. alone, many of which are enticing targets due to the important function they perform and the fact that they are typically unstaffed in remote settings. Traditionally, electrical substation security was focused only on preventing unauthorized access, to stop vandalism and improve safety. But today, security efforts have been redefined to address new threats to protect critical infrastructure.

### Oil & Gas



Reliable and effective physical security in the oil and gas sector is a challenging objective, when situated in remote and often high-risk locations. Geopolitical issues have culminated in the rise of terrorists targeting the physical infrastructure of the oil and gas industry to gain notoriety and control of the valuable resources that these plants process.

### Mining & Quarry Operations



Whether the mined products are diamonds, gold, uranium, or lead, there's a need to protect them from theft or terrorism. Limiting access to visitors and unauthorized persons requires planning, and the use of physical security and video surveillance which can be challenging when operations are often spread over vast areas.

### Government Facilities



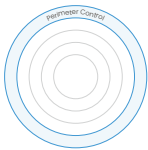
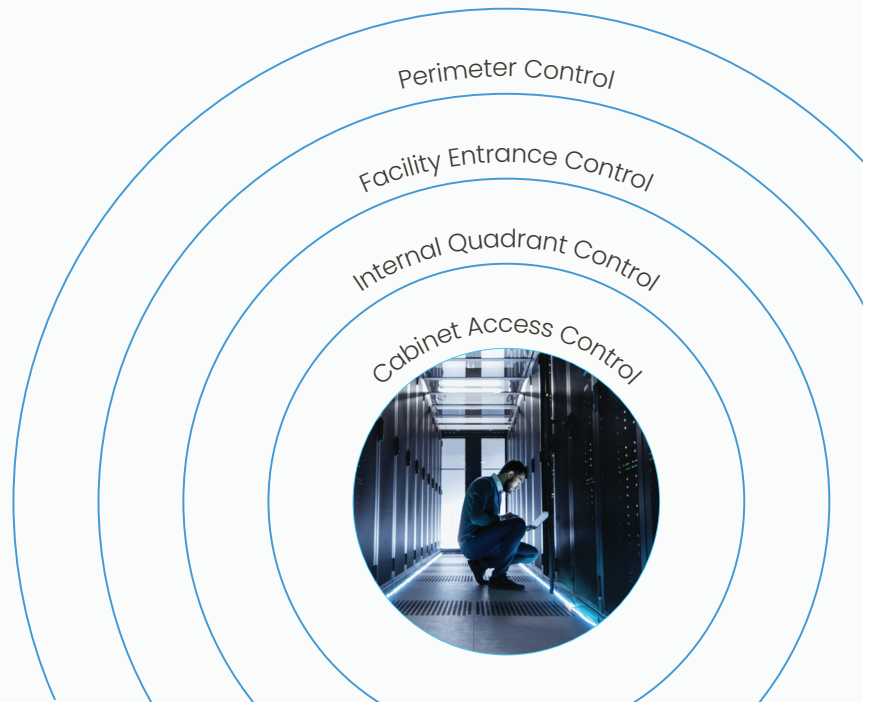
Comprehensive physical security has become critical to protecting a government agency's facilities, property, information, and personnel assets. Integration of video and access control, and the power of analytics are all transforming physical security across local, state and federal government facilities.



# Taking a Layered Approach

A successful security protocol goes beyond a secure front entrance. Implementing smart technologies allows for a more complete and secure facility.

Most companies put all of the security in the front door: surveillance cameras, security guards, and badge access; but they fail to focus on the entire building or facility as a whole.



## Perimeter Security

### Challenges

- Achieve the basic goal of identifying people going in and out of the facility
- Sterile Zone monitoring to identify people jumping fences or crawling
- False alarms that result in significant operational burden on guards who eventually shut off the system

### With Oosto

AI-based proprietary technology that includes a combination of face, body attribute, object and person recognition

- Delivers unmatched accuracy even in low-light environments, extreme angles, and obscured faces
- Provides superior perimeter security with the lowest rate of false alarms
- Achieves 90% increase in security team productivity



## Entrance Control

### Challenges

- Grant access to approved employees and visitors
- Alert if a visitor has over-stayed a permitted time frame
- Reduce COVID-19 exposure risk associated with surface contact

### With Oosto

- Reduce workload and increase security productivity with accurate, automated and customizable alerts
- Receive instant notifications on unauthorized access
- Provide real-time route and location tracking (to prevent visitors from accessing sensitive areas)
- Conclude investigations faster with instant search by individual and/or personal attributes



## Internal Quadrant Control

### Challenges

- Control access to spaces within a building where there are no physical doors or entry points
- Manage access to internal zones based on time and role or group permissions
- Add a dual or triple authentication layer to highly sensitive areas of the facility

### With Oosto

- Create enforceable barriers without erecting permanent structures and get instant alerts when unauthorized people are identified
- Easily set rules for who goes where throughout a space with a granular rules engine that's customizable by time, groups, and location
- Forensics capability enables rapid investigation of any incident



## Cabinet Rack Control

### Challenges

- Cameras are installed over or inside racks but require a human to make sure the correct person is accessing the rack
- Coping with guidelines/practices of who is allowed to open a cabinet at any given time

### With Oosto

- Receive automated alerts when an unauthorized individual attempts to access a cabinet or rack
- Alert on after-hours access
- Provide real-time location information as well as route analysis of unauthorized individuals



For more information, please contact us at: [info@oosto.com](mailto:info@oosto.com)

*Oosto does not offer, sell or make available any of its products or services to customers in the EU for the use of real-time remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement or any of the other prohibited AI practices as outlined in the EU AI Act.*