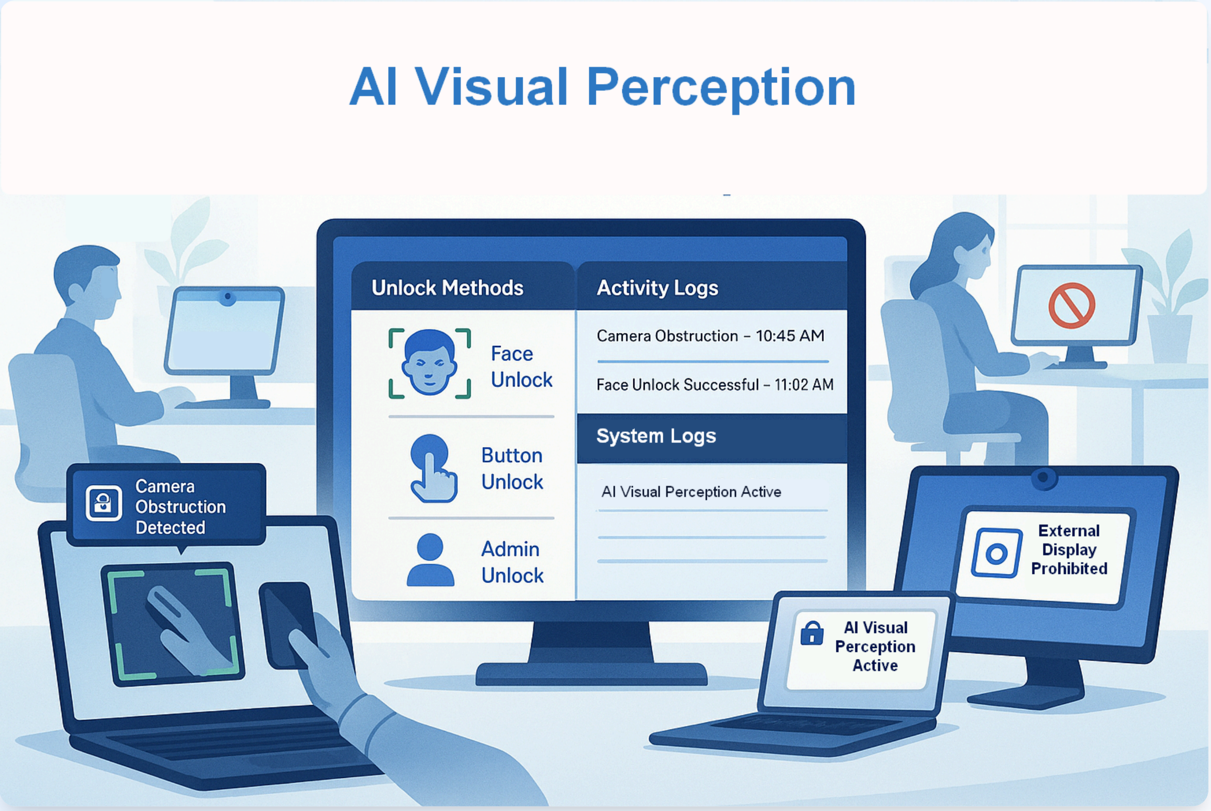
AnySecura

AI Visual Perception

Advanced intelligent monitoring solution for workplace security

Detect · Protect · Alert · Authenticate · Record


AI Visual Perception
Unlock Methods
Face Unlock
Button Unlock
Admin Unlock
Activity Logs
Camera Obstruction – 10:45 AM
Face Unlock Successful – 11:02 AM
System Logs
AI Visual Perception Active
Camera Obstruction Detected
External Display Prohibited
AI Visual Perception Active

Module Overview

AnySecura AI Visual Perception utilizes advanced self-developed AI models to enhance workplace security through intelligent camera monitoring, real-time threat detection, and secure authentication mechanisms, protecting sensitive information from unauthorized access and leakage.

Visual Perception

Through a self-developed AI model, call the computer camera to conduct real-time detection of users' abnormal behaviors. When abnormal behaviors are detected, the computer can be locked, an alarm can be issued, and logs can be recorded.

Camera Obstruction Detection

Automatically detect employees' behavior of covering the camera. When covering the camera is detected, the computer will be locked, an alarm will be issued, and logs will be recorded.

External Display Detection

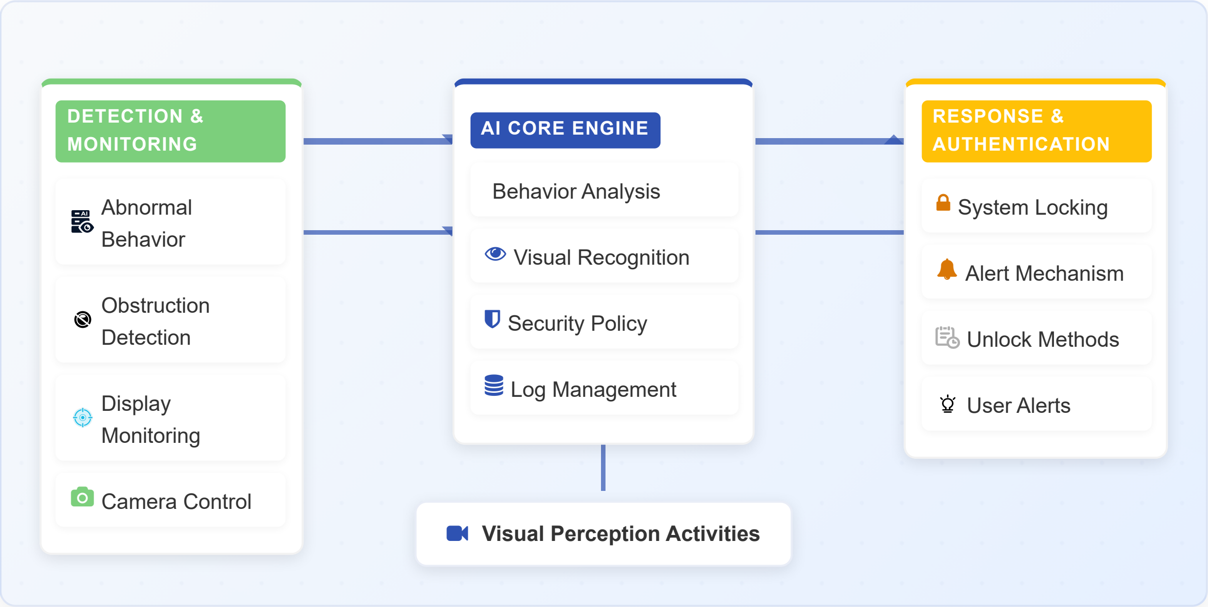
Support real-time detection and prohibition of employees' use of external monitors. When employees use external monitors, a prompt will pop up, and access can be prohibited and logs recorded.

Camera Notification

After enabling the visual perception function, a customizable desktop notification indicating that the camera is on can be displayed on the desktop, reminding employees that the camera is on.

System Unlocking & Shooting Logs

Support multiple unlocking methods including face unlock, button unlock, automatic unlock, application-based unlock, and administrator direct unlock. Comprehensive shooting logs record employee activities including privacy policy viewing, desktop access, mobile phone photography, camera covering, unlock attempts, and shooting function activation.



DETECTION & MONITORING

- Abnormal Behavior
- Obstruction Detection
- Display Monitoring
- Camera Control

AI CORE ENGINE

- Behavior Analysis
- Visual Recognition
- Security Policy
- Log Management

RESPONSE & AUTHENTICATION

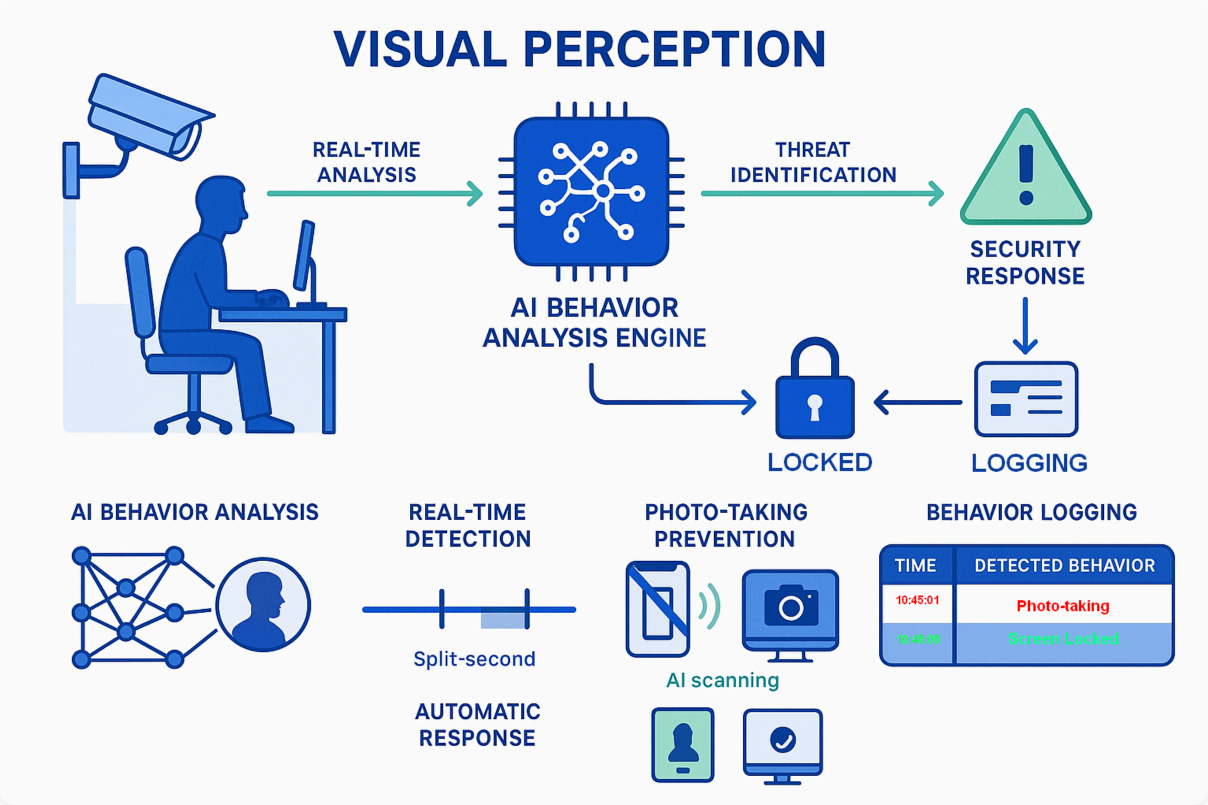
- System Locking
- Alert Mechanism
- Unlock Methods
- User Alerts

Visual Perception Activities

Visual Perception

Advanced AI-powered monitoring that detects abnormal user behaviors in real-time to prevent unauthorized information capture and ensure workplace security.

- **AI Behavior Analysis:** Self-developed AI model that intelligently identifies suspicious activities through computer camera monitoring.
- **Real-time Detection:** Continuous monitoring and analysis of user behavior with instant identification of abnormal activities.
- **Photo-taking Prevention:** Specialized algorithms to detect mobile phone and camera photography aimed at sensitive information.
- **Automatic Response:** Immediate system locking when abnormal behaviors are detected to prevent information leakage.
- **Alert Mechanism:** Instant alarm notifications to security personnel when suspicious activities are identified.
- **Behavior Logging:** Detailed recording of all detected events for audit and investigation purposes.



TIME	DETECTED BEHAVIOR
10:45:01	Photo-taking
10:45:05	Screen Locked

Device Monitoring

Camera Obstruction Detection

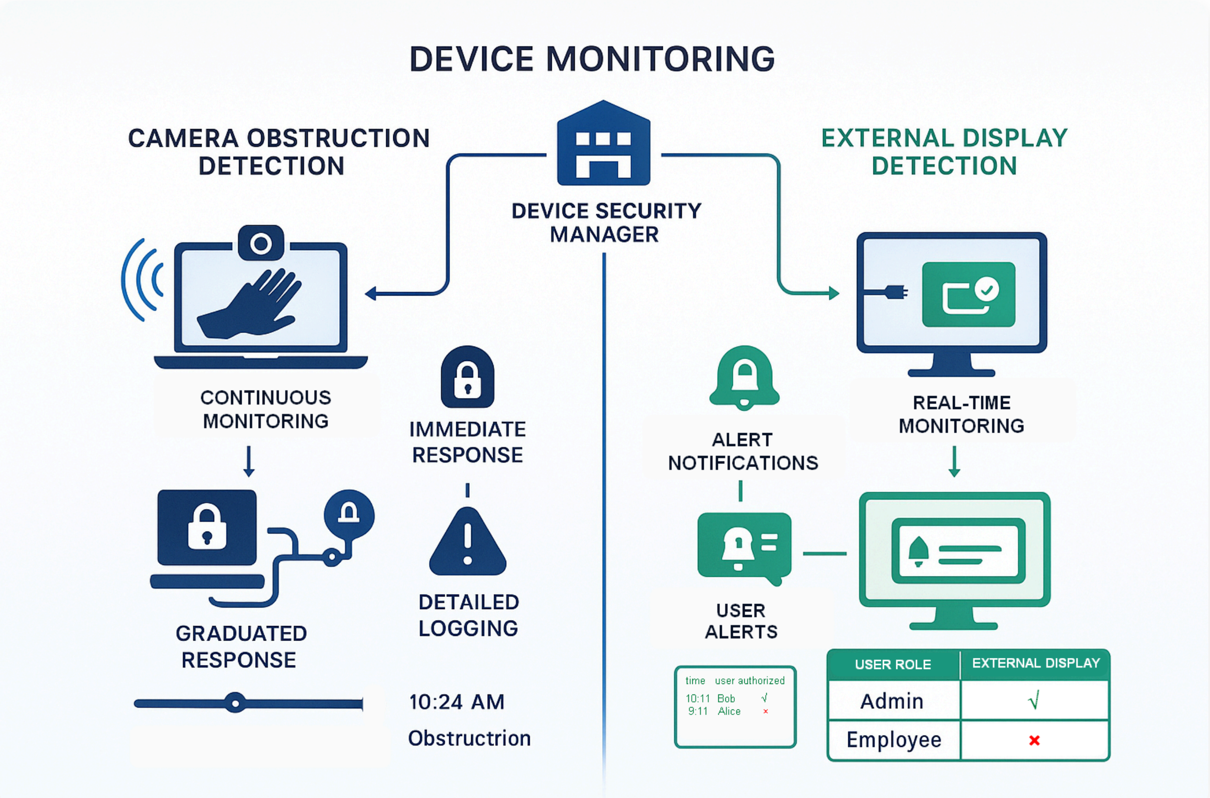
Comprehensive protection against attempts to disable monitoring capabilities through intentional camera blocking.

- **Automatic Detection:** Intelligent algorithms that identify when cameras are covered or obstructed.
- **Immediate Response:** Automatic system locking when camera obstruction is detected.
- **Alert Notifications:** Instant alerts to security administrators about potential tampering.
- **Detailed Logging:** Comprehensive records of all obstruction events with timestamps and user information.
- **Graduated Response:** Configurable response levels based on obstruction duration and frequency.

External Display Detection

Control over external monitor connections to prevent unauthorized information display and leakage.

- **Real-time Monitoring:** Continuous detection of external display connections to protected systems.
- **Prohibition Controls:** Ability to block unauthorized external monitor usage completely.
- **User Alerts:** Pop-up notifications when external displays are connected, warning of policy restrictions.
- **Usage Logging:** Detailed records of all external display connection attempts and activities.
- **Policy Enforcement:** Role-based permissions for external display usage based on job requirements.



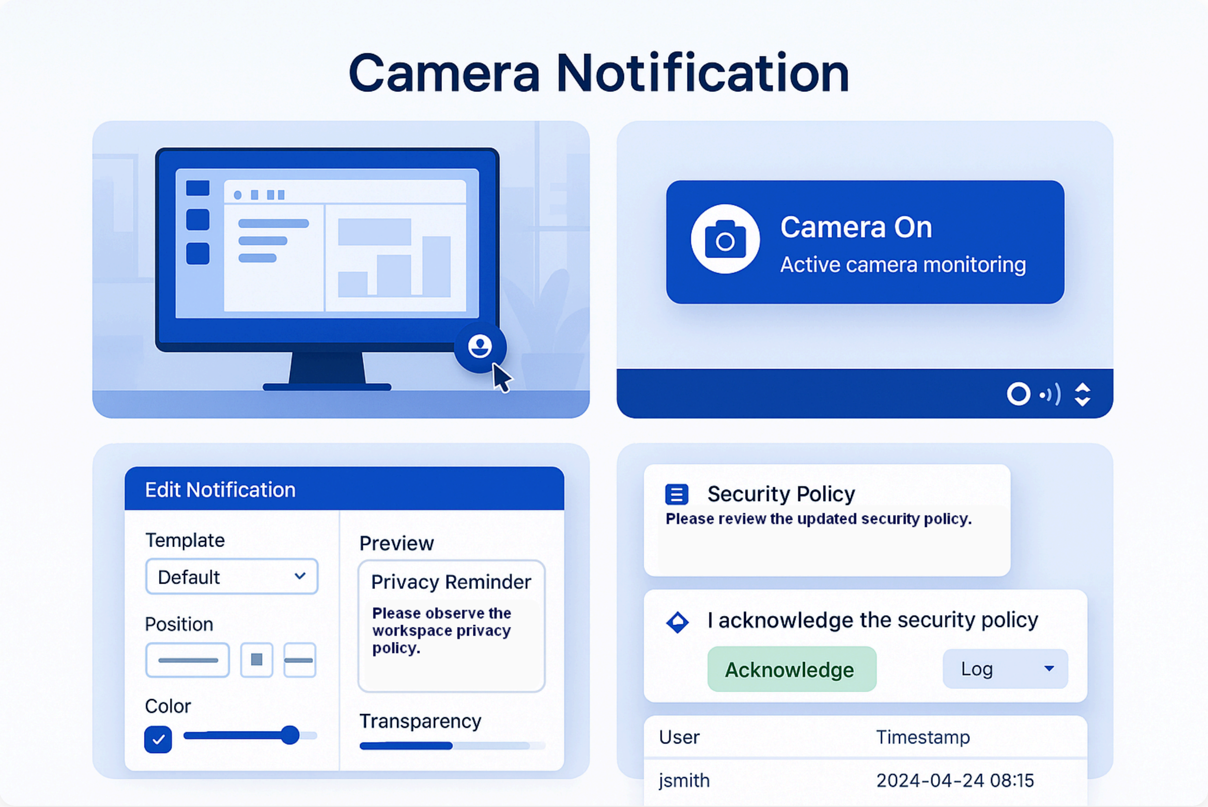
time	user	authorized
10:11	Bob	√
9:11	Alice	×

USER ROLE	EXTERNAL DISPLAY
Admin	√
Employee	×

Camera Notification

Transparent communication about active monitoring to maintain employee trust while ensuring security compliance and proper workplace behavior.

- **Visual Indicators:** Clear desktop notifications showing when the visual perception function is active.
- **Customizable Alerts:** Configurable notification messages, designs, and display durations to meet organizational needs.
- **Privacy Reminders:** Notifications include gentle reminders about appropriate workplace behavior and privacy considerations.
- **Policy Communication:** Direct links to security policies and guidelines within notifications for easy reference.
- **Consistent Display:** Persistent but non-intrusive indicators ensuring employees are always aware of active monitoring.
- **Acceptance Tracking:** Records when employees acknowledge notifications for compliance documentation.



Camera Notification

Camera On
Active camera monitoring

Edit Notification

Template: Default

Preview: Privacy Reminder
Please observe the workspace privacy policy.

Security Policy
Please review the updated security policy.

I acknowledge the security policy

User	Timestamp
jsmith	2024-04-24 08:15

System Unlocking & Logging

System Unlocking Methods

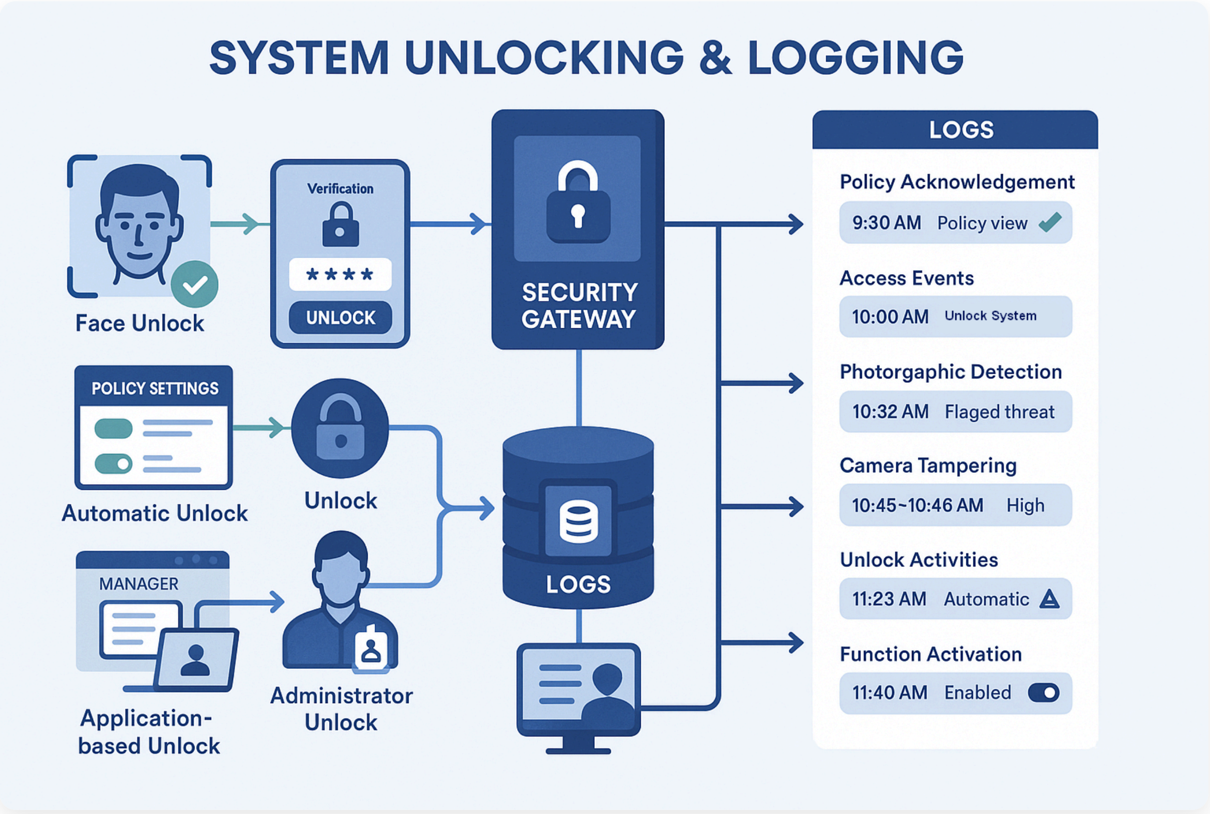
Flexible and secure authentication mechanisms to regain access after security events while maintaining audit capabilities.

- **Face Unlock:** AI-powered facial recognition for convenient and secure system access.
- **Button Unlock:** Manual unlock through designated interface controls after identity verification.
- **Automatic Unlock:** Policy-based automatic access restoration without requiring photo capture.
- **Application-based Unlock:** Formal request process for access restoration with manager approval.
- **Administrator Unlock:** Direct access restoration by authorized security personnel with full audit trail.

Shooting Logs & Activity Records

Comprehensive documentation of all security-related events for compliance, investigation, and policy refinement.

- **Policy Acknowledgment:** Records of employees viewing and acknowledging privacy policies.
- **Access Events:** Detailed logs of all desktop entry and system access activities.
- **Photography Detection:** Records of all detected mobile phone and camera usage.
- **Camera Tampering:** Documentation of all camera covering and obstruction attempts.
- **Unlock Activities:** Complete records of all system unlock attempts, successful or failed.
- **Function Activation:** Logs of all visual perception feature activations and deactivations.



SYSTEM UNLOCKING & LOGGING

Policy Acknowledgement
9:30 AM Policy view ✓

Access Events
10:00 AM Unlock System

Photorgaphic Detection
10:32 AM Flaged threat

Camera Tampering
10:45~10:46 AM High

Unlock Activities
11:23 AM Automatic ⚠

Function Activation
11:40 AM Enabled ●

Application Scenarios

1. Office Anti-Photography

The Challenge

A technology company with sensitive intellectual property faces unauthorized photography of confidential documents and screens in core departments, leading to security breaches.

The Solution

Implementing **Visual Perception** and **System Unlocking**:

1. Enable high-sensitivity visual perception in core departments
2. Configure immediate system locking when photo-taking is detected
3. Use face recognition for secure unlock after security events
4. Maintain detailed logs of all incidents and responses

Results Achieved

- ✓ 95% reduction in unauthorized photography incidents
- ✓ Complete audit trail for investigation and compliance

2. Factory Anti-Sneak Photography

The Challenge

A manufacturing plant with sensitive product designs on public computers in unsupervised production areas faces risks of industrial espionage through unauthorized photography.

The Solution

Leveraging **Visual Perception** and **Camera Obstruction Detection**:

1. Deploy high-sensitivity visual perception for early threat detection
2. Configure immediate screen locking when photography is suspected
3. Implement strict camera obstruction detection with automatic locking
4. Require manager approval for system unlocking after incidents

Results Achieved

- ✓ Eliminated unauthorized photography of sensitive manufacturing data
- ✓ Prevented attempts to disable security through camera tampering

Core Values & Benefits

Enhanced Security

Advanced AI-powered monitoring detects and prevents unauthorized information capture, protecting sensitive data from leakage through photography.

Comprehensive Oversight

Complete visibility into potential security threats with monitoring of camera tampering and external display connections.

Transparent Compliance

Clear notifications about active monitoring maintain employee trust while ensuring compliance with security policies.

Actionable Insights

Detailed logs and analytics provide valuable information for security policy refinement and incident investigation.

Ready to Enhance Your Workplace Security?

Learn More About Solutions

Contact Our Experts

www.anysecura.com

support@anysecura.com