An AI that prevents employees from taking photos of their monitors

PhotoShield

The Analog Loophole

- Security professionals struggle with closing the gap between the end-point device and the user (the “Analog Loophole”). No matter how much is invested in cyber security technology, data in transit must be displayed on a screen viewed by the user. Valuable data is vulnerable to analog means (i.e., cameras and phones).

- This Analog Loophole poses a bigger problem for enterprises who must demonstrate prudent measures to address the new hybrid work model.

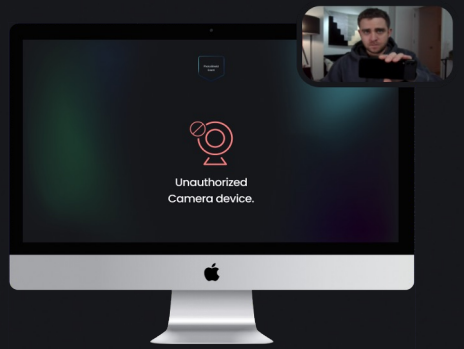
- **Photo Shield solves this problem by preventing users from intentionally or unintentionally disclosing Proprietary, CUI, PII, or Classified information.**

PhotoShield

Stop Employees From Taking Pictures

Photo Shield uses the device's webcam and AI to monitor activity and detect when someone is using a smartphone or digital camera.

Unauthorized Camera Detected



Screen Blocked

PhotoShield

Protection from More Than Just Photos

Photo Shield uses your webcam and AI to monitor activity and take actions automatically to protect your data.

Stop shoulder surfing from exposing data

Detects multiple people in front of the screen

Stop wandering eyes when not at the desk

Detects no person in front of the screen

Stop users from bypassing protections

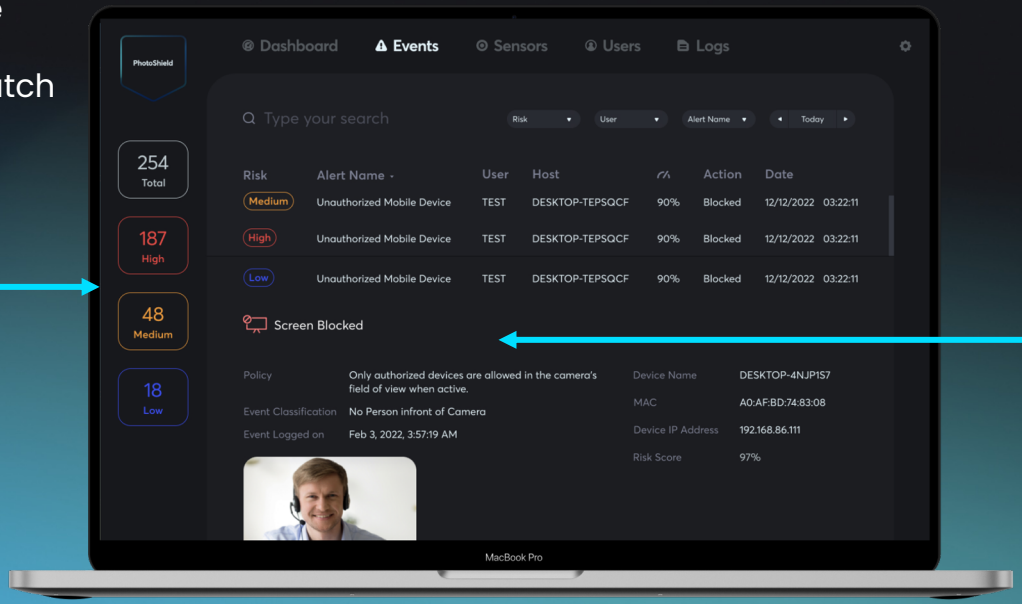
Detects when the camera is being blocked or not functioning

PhotoShield

Set up your own playbook

Control what Photo Shield does when it detects unauthorized activity

Detected “events” are assigned a risk score based on the percentage of its match to the AI algorithm.



Multiple Action Options

- ✓ Block Screen
- ✓ Watermark Screen
- ✓ Warning Notification
- ✓ Lock Device

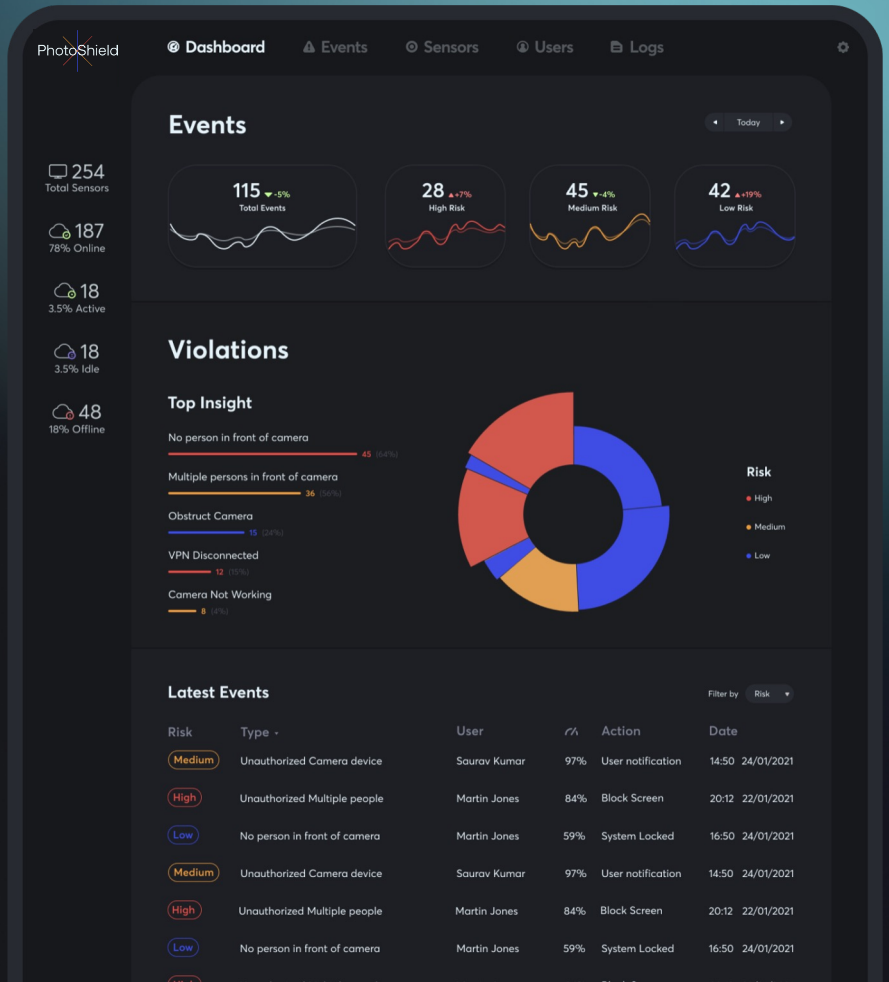
YOU decide what “action” Photo Shield takes when an event happens.

PhotoShield

Centralized Administration and Auditing

Control what Photo Shield does when it detects unauthorized activity

- Monitor and review events<
- See what actions were considered violation “events”
- Setup your playbook on how policies, events, and actions are handled
- Setup and manage users



PhotoShield

Adaptable Technology Platform

Load balancing AI Engine

- The AI engine executes locally on the end-point computer
- Utilizes computers GPU if present
- If there is no GPU, the AI engines native intelligence will optimize CPU usage, performance impact is negligible
- Leverages the Yolo 8.0 advanced AI engine

Flexible server configurations for secure environments

- The management server can be cloud based or locally hosted behind your firewall or in an air-gapped environment
- The agent can also run disconnected from any server if necessary.

Low network bandwidth requirements

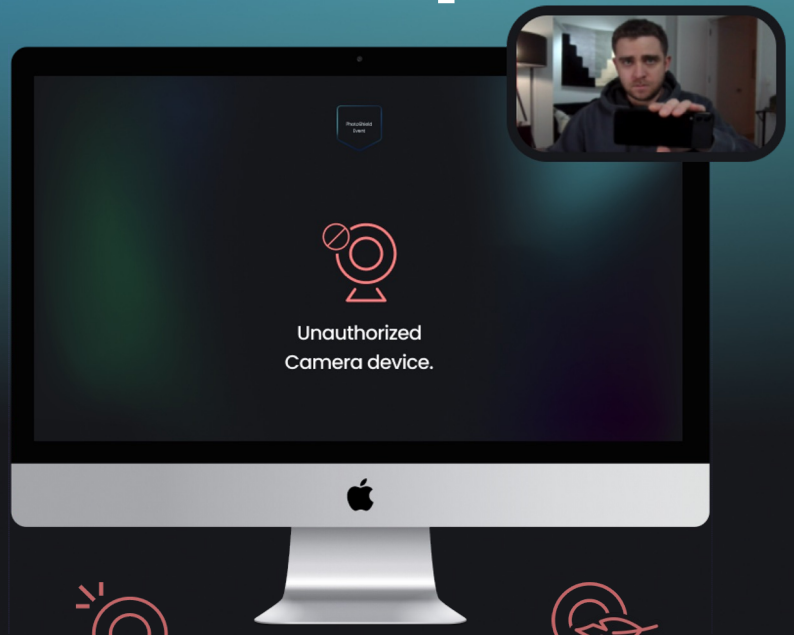
- Detected violation information is the only data sent to the management server
- Network bandwidth requirements are minimal
- Data sent to management server depends on your configuration

Agnostic & Easy Installation

- Runs as an Agent on the user's computer or deployable on Vm's
- The Agent software is deployed via standard solutions such as Microsoft Intune or Ivanti Endpoint Manager
- All required prerequisites are packaged in the MSI

PhotoShield

End-user Experience



Person

Unauthorized Multiple people.

Camera device is not working.

Unauthorized camera obstruction.

Unauthorized Mobile device.

There is a problem.

PhotoShield

Platform Demonstration

PhotoShield

Use-Cases

- Commercial & DIB - Intellectual Property Protection
- Healthcare – Protect PII/HIPAA
- Government- Unintentional Leakage
- Government- Insider Threat
- Government- Counterintelligence

PhotoShield

DISA Strategy Alignment

DISA STRATEGIC PLAN FY2022-2024

LINE OF EFFORT #2: DRIVE FORCE READINESS THROUGH INNOVATION	**Emerging Technology** — Develop a technology roadmap to drive the evolution of current state architectures and services toward next generation capabilities; minimize labor-intensive and time-consuming processes by Artificial Intelligence / Machine Learning solutions to free our workforce to devote their time to higher-value work.
LINE OF EFFORT #3: LEVERAGE DATA AS A CENTER OF GRAVITY	**Advanced Analytics** — Develop advanced analytics and business intelligence to enhance day-to-day decision-making and capabilities for joint all-domain and electromagnetic spectrum operations.
	Cyber Situational Awareness — Create an enterprise defensive cyber operations (DCO) and data monitoring strategy to optimize use of data as a strategic asset.
LINE OF EFFORT #4: HARMONIZE CYBERSECURITY AND THE USER EXPERIENCE	**Continuous Monitoring** — Incorporate DCO continuous monitoring into the accreditation process to move the Department to a continuous authorization to operate (ATO).
	End User Experience — Deliver modernized IT solutions that enhance security protections and increase endpoint performance.

PhotoShield

Enterprise Considerations


Accreditation – ATO – FIPS 140-2/-3 [Sponsorship]


Integration – API Available


Hosting – SaaS – Hybrid – Cloud (Gov or Commercial)


Scalability – 4.3M+ User Capable (Lab Tested)


Training Requirement – Zero User – Limited Admin


Data Rights – Government owns Data – PS owns IP

PhotoShield

Contact

jonhoffman@photoshield.com

(t) +1.703.282.4266