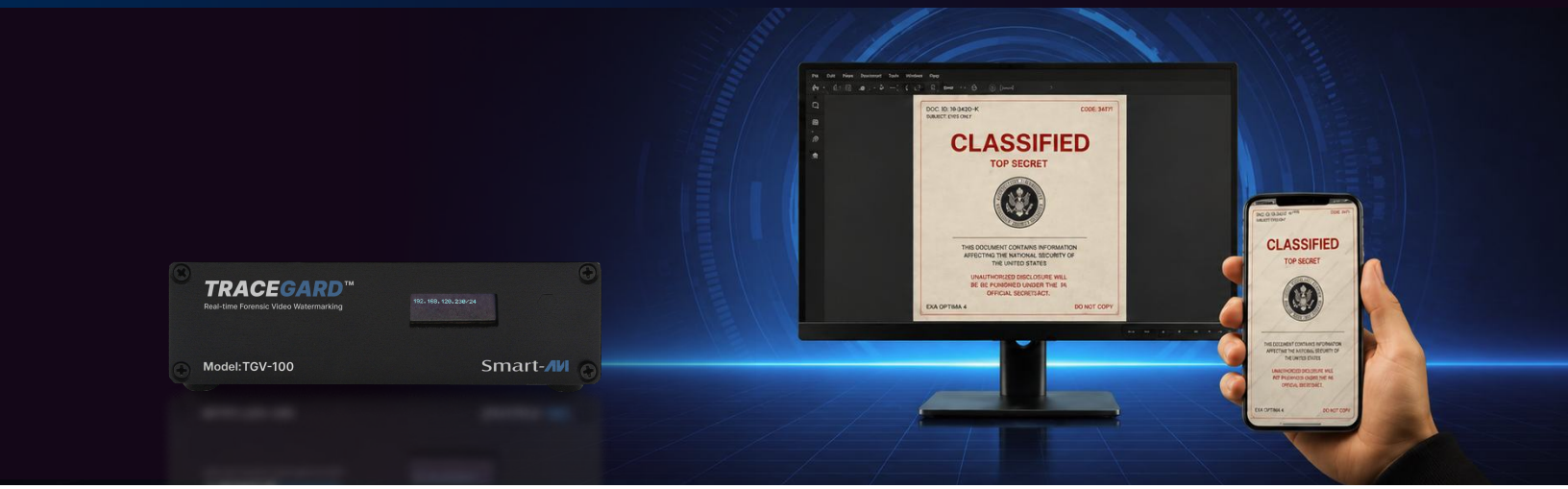
iPGARD™

Designed and Manufactured in the USA




# EVERY SCREEN LEAVES A FINGERPRINT

In secure environments, the hardest leak to stop is the simplest one: a phone pointed at a monitor. Firewalls, DLP and secure KVM protect the data path, but none of them can see a camera. TraceGard closes that gap. Every screen it protects carries an invisible mark that stays in any photo or video taken of it, so a leak points straight back to where it came from.

### HARDWARE-ENFORCED, LIKE EVERY IPGARD PRODUCT

**Works with any computer**
Windows, macOS, Linux, thin clients. No agents to deploy, patch or license.

**Can't be switched off at the PC**
The mark is added after the computer, so local settings and admin rights don't touch it.

**Covers everything on screen**
Documents, dashboards, video, web apps and remote sessions. It protects the screen, not a file type.

# KNOW WHERE EVERY SCREEN CAPTURE CAME FROM

TraceGard adds forensic identification to the live video path, helping organizations investigate photographed, recorded or leaked screen content.

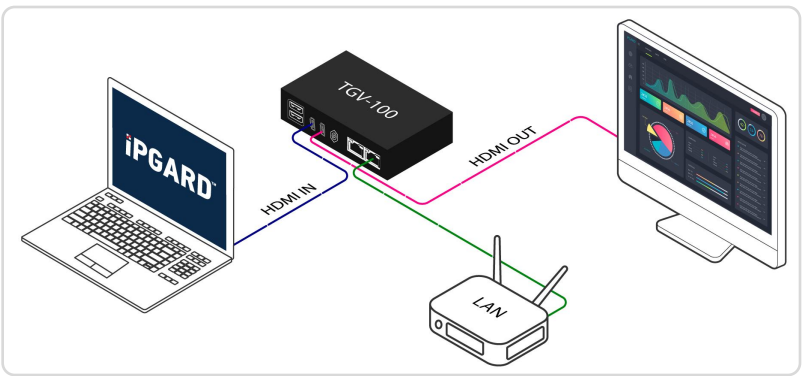
**IDENTIFY**
Associate displayed content with its source.

**TRACE**
Investigate where captured content originated.

**DETER**
Increase accountability for screen photography.

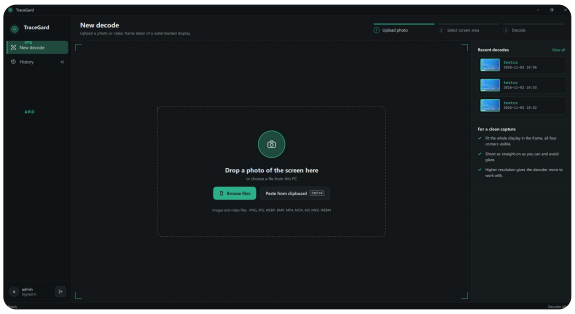
### KEY FEATURES

- **Hardware-based** — independent of the host;
- no endpoint software
- **Real-time** — HDMI in / out, up to 4K@ 60 Hz
- **Front-panel display** — OLED shows IP address
- and status
- **On-board AI engine** — 6 TOPS NPU for video analysis
- **Network-ready** — dual 2.5 GbE for management
- **Deterrence** — traceable screens discourage photography



# TURN A PHONE PHOTO INTO EVIDENCE

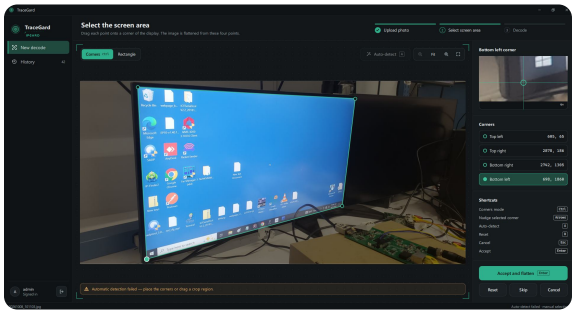
Every TraceGard ships with TraceGard Manager, one application to trace leaked captures and manage every unit on the network. Leaked photos are rarely clean: taken at an angle, under office lighting, then squeezed by a messaging app. TraceGard Manager is built for exactly that.




### STEP 1

**Upload**

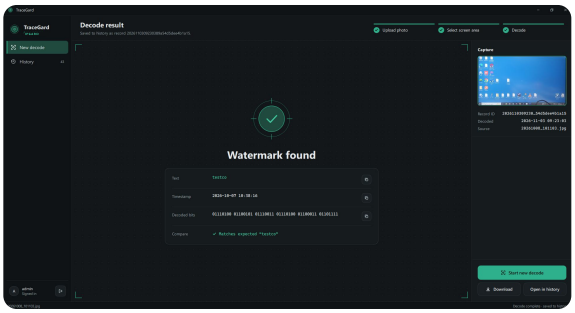
Drag in, browse or paste a photo or video. PNG, JPG, WEBP, BMP, MP4, MOV, AVI, MKV, WEBM.




### STEP 2

**Select screen area**

Auto-detect finds the screen edges. Or drag the four corners yourself. Angled shots can be corrected.




### STEP 3

**Decode**

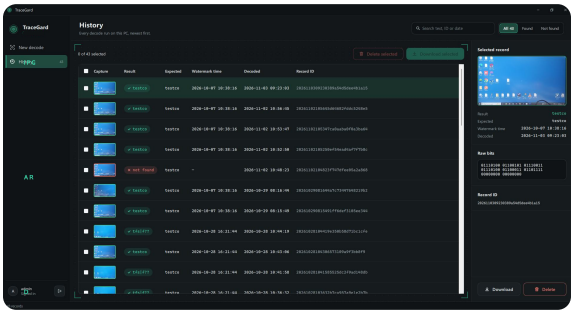
Get "Watermark found", the hidden text and the time. Compare against an expected text. Copy any field.

# MANAGE EVERY UNIT FROM ONE PLACE

The same application finds, configures and maintains every TraceGard unit on your network, so each screen carries the right identifier and an accurate clock.

### HISTORY: EVERY DECODE SAVED

Each decode is saved automatically, newest first, with a unique record ID. Search by text, record ID or date. Filter by found or not found. Download or delete one record or many.



**Network discovery**
Locate TraceGard units by IP address and port.

**Live status at a glance**
Firmware version, watermark text, watermark strength, device time and IP address.

**Custom identifier**
Set the text each unit embeds, so every screen can be traced back to its source.

**Accurate timestamps**
Sync each unit's clock so recovered captures show exactly when content was displayed.

**Adjustable watermark strength**
Balance robustness against on-screen visibility.

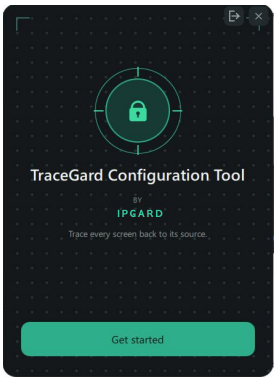
**Remote maintenance**
Change IP settings, reboot, factory reset or update firmware without touching the hardware.

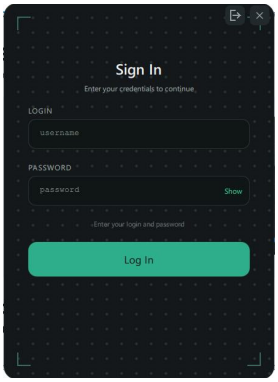
**Batch commands**
Tick the changes you need and apply them in a single send.

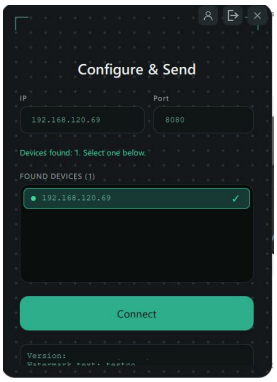
**Secure access**
Protected by user sign-in.




*Device status and commands.*

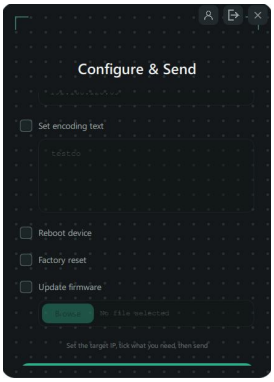









## THE TRACEGARD DEVICE

A small box that sits between your video source and your display. It handles 4K60 video input and output over HDMI. A built-in OLED screen shows the product name, the IP address and the live date and time.  Two 2.5GbE network ports. USB port on the back.







## APPLICATIONS

- **Government & Defense —** secure facilities, classified workstations
- **Finance —** trading floors, deal rooms
- **Healthcare** — patient records on screen
- **R&D & Media** — designs, code, pre-release content

## WHERE TRACEGARD FITS

### LEAK INVESTIGATION

Secure facilities, control rooms: find the exact display and time behind a leaked photo.

### CONFIDENTIALBUSINESS DATA

Finance, R&D, boardrooms: protect information that software can't see once it leaves as a camera photo.

### DETERRENCE

Help discourage unauthorized screen photography.

### SITE OR CUSTOMER ATTRIBUTION

Give each site, customer or room its own watermark text.

## VIDEO

| | |
|---|---|
| **Video input** | 1× HDMI, up to 4K @ 60 Hz |
| **Video output** | 1× HDMI, up to 4K @ 60 Hz |
| **DVI / DisplayPort** | Supported via adapter |
| **Video engine** | Hardware decode / encode, up to 8K |
| **Watermarking** | Real-time, in the live video path |

## PROCESSING

| | |
|---|---|
| **Processor** | 8-core 64-bit, up to 2.4 GHz |
| **Graphics** | Integrated GPU, OpenGL ES 3.2 / Vulkan 1.2 |
| **AI accelerator** | Built-in NPU, up to 6 TOPS |
| **Memory** | LPDDR4X, [8 / 16 / 32 GB] |
| **Storage** | Internal eMMC, [CAPACITY] |

## CONNECTIVITY

| | |
|---|---|
| **Ethernet** | 2× 2.5 GbE (RJ45) |
| **Front panel** | OLED status display (IP address) |
| **USB** | 2× USB-A |
| **Management** | Over the network via LAN, [WEB UI / API] |

## POWER & PHYSICAL

| | |
|---|---|
| **Power input** | 12 V DC |
| **Enclosure** | Black aluminum, desktop |
| **Dimensions** | 8.8” W × 1.0” H × 3.9” D |
| **Weight** | [1.6 lbs] |
| **Model** | TGV-100 |

**From iPGARD**, maker of NIAP-certified secure KVM, matrix and multiviewer solutions, with more than 20 years in AV and KVM. TraceGard extends that protection from the data path to the screen itself.

**See TraceGard trace a leak, live**
Ask iPGARD for a demo with your own photos.

**ipgard.com**
**(888) 994-7427**